Edith Cowan University

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study.

The University does not authorize you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following:

- Copyright owners are entitled to take legal action against persons who infringe their copyright.
- A reproduction of material that is protected by copyright may be a copyright infringement.
- A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.
ABSTRACT

Internet proxy systems such as Squid exchange intelligence relevant to their function as caching proxy servers via a distributed and trusted hierarchy of machines. The required intelligence is broadcast based along the network based upon established trust relationships throughout the connected network via specific port and protocols of exchange. An intrusion detection system that incorporates this functionality for gathering attack intelligence could be a formidable foe even for the wiliest attacker.

This paper will outline a possible model for the deployment of a network/distributed network intrusion detection system utilising technologies and techniques already in existence to provide the supporting infrastructure.

Keywords: security, intrusion, detection, firewall, attack, intelligence

INTRODUCTION

Hackers and other perpetrators have moved and adapted rapidly to leverage the distributed, sharing network paradigm presented by the Internet to wreak havoc at ever-increasing rates and with increasing complexity (Brown, Gunderson, & Evans, 2000; CERT, 1999; Dietrich, Long, & Dittrich, 2000; Fonseca, 2001; Kent, 2000; Neumann, 1999). The changing nature of network based attacks from singular to distributed modes of attack (CERT, 1999; Dietrich et al., 2000) and the use sophisticated tools to launch these attacks underlies the need for the development of a distributed defensive countermeasures. A distributed network model for the sharing and distribution of attack intelligence is one such method that the proposed Network Intrusion Detection Hierarchy (NIDH) will exploit to counteract such attacks.

Most of the tools and countermeasures deployed to defend most modern networked computer systems such as firewalls, virtual private networks, intrusion detection systems have their functionality and modus operandi still in a singular or digital xenophobic security paradigm. Rarely if at all do these systems share attack intelligence between hosts let alone across a trusted distributed network or hierarchy.

Firewalls are very good at denying or filtering access to a network but they are not very good at gathering attack intelligence as they simply block and discard information based on existing rulesets. Most of the existing firewall systems simply store intrusions into a logfile if so configured and rarely is this data then analysed.
Intrusion detection systems are the equivalent of a digital tripwire that detects what is termed an intrusion, breach or attack of a network computer system (McCarty, 1999; Ranum, 1999). The common flaw is that most currently deployed systems have only a single tripwire. The one point of reference for the tripwire is normally the inbound data device a router or ethernet card for gathering intelligence for the intrusion detection system. They also rarely communicate with other systems to exchange attack intelligence.

There are many current attempts at developing systems that use distributed trusted networks to gather attack intelligence. One of the more recent and additions is the Autonomous Agents for Intrusion Detection (AAFID) proposed by (Spafford & Zamboni, 2000) and this goes some way to providing distributed intrusion detection systems through the use of autonomous agents. These agents report attack intelligence back to specified transceivers for processing and is one such model that is trying to address the current problems of system isolation.

There are existing systems that analyse the logfiles from intrusion detection systems, firewalls, and other network countermeasures. Most of these systems are capable of detailed analysis of logfiles that produce extensive and extensible static reports. What is lacking is a mechanism for the dynamic sharing of attack intelligence although several of the existing countermeasure systems already have the ability to communicate the results of analysis via a network socket.

This paper will outline a possible model for the deployment of a network/distributed network intrusion detection system utilising technologies and techniques already in existence to provide the supporting infrastructure. The model will leverage concepts and methods already used by the Squid proxy cache system. The model is not intended to rewrite the rule book but provide infrastructure capable of a rapid response to attacks via the sharing of attack intelligence.

**THE NIDH MODEL**

**Baseline Systems**

The baseline systems for the model should have firewall and intrusion detection capabilities. For the purposes of the explanation of this model we can assume that the system that is described by the author operates above the firewall and intrusion detection systems as depicted in Figure 1.

![Figure 1: NIDH Architecture](image)

The NIDH extracts information from the standard reporting functions on these systems. This information can come from either a direct output stream/socket containing this information. Alternatively, through the tailing of the logfiles that are files created on a disk sub-system as result of directing the output stream to disk for storage. The firewall and the intrusion detection system should be capable of at least identifying the probed or attacked port and providing this information either to the logfile or socket. The NIDH is a stand-alone process that is scalable. For example, the NIDH does not have to be located on the server that runs all of the other services, and in fact, could be a separate machine that summarises this information for a complete network.
Data Analysis

The NIDH should summarise and reduce the amount of data where there is high repetition of an attack type over a short time frame. The use of an automated attack or a brute force attack would typically produce multiple logfile entries from the same attacking host in rapid succession. The following detail in the Logfile 1 exhibit is a snippet from a conventional system logfile demonstrating exactly this scenario.

Feb 2 12:03:04 foden netacl[28347]: deny host=adsl-63/63.202.208.126 service=wu.ftpd
Feb 2 12:03:04 foden netacl[28353]: deny host=adsl-63/63.202.208.126 service=wu.ftpd
Feb 2 12:03:04 foden netacl[28348]: deny host=adsl-63/63.202.208.126 service=wu.ftpd
Feb 2 12:03:04 foden netacl[28354]: deny host=adsl-63/63.202.208.126 service=wu.ftpd
Feb 2 12:03:04 foden netacl[28349]: deny host=adsl-63/63.202.208.126 service=wu.ftpd
Feb 2 12:03:04 foden netacl[28350]: deny host=adsl-63/63.202.208.126 service=wu.ftpd

Logfile 1: A sample attack or probe

The logfile format in Logfile 1 provides vital information about the attack and the attacking host. The following is an explanation of the first line of logfile entry:

- Date & Time of the attack - Feb 2 12:03:04
- Defensive Host - foden
- The process name and number responsible for the action - netacl[28347],
- The action taken - deny
- Attacking Host - host=adsl-63/63.202.208.126 - in the format hostname/IP Address
- Service attacked/probed - service=wu.ftpd - the service number for this is 21

The NIDH should summarise this amount of data to simply one reference of the attack host in IP Address format and the service in service number format being attacked for transmission through the NIDH to other systems. This reduces the amount of data that would be transmitted across the NIDH. It also takes into account and counterattacks the problems presented by the use of automated vulnerability scanners such as Nessus, SATAN, or automated scripts that are used to implement brute force attacks.

Pattern detection where possible should occur as well for instance in the case of a distributed attack. The log example Logfile 2 below has been modified to demonstrate a sample log entry for a distributed attack

Feb 2 12:03:04 foden netacl[28347]: deny host=distributed_1 service=wu.ftpd
Feb 2 12:03:04 foden netacl[28353]: deny host=distributed_2 service=wu.ftpd
Feb 2 12:03:04 foden netacl[28348]: deny host=distributed_3 service=wu.ftpd
Feb 2 12:03:04 foden netacl[28354]: deny host=distributed_4 service=wu.ftpd
Feb 2 12:03:04 foden netacl[28349]: deny host=distributed_5 service=wu.ftpd
Feb 2 12:03:04 foden netacl[28350]: deny host=distributed_6 service=wu.ftpd
Feb 2 12:03:04 foden netacl[28351]: deny host=distributed_7 service=wu.ftpd

Logfile 2: A sample distributed attack

What differs in this case is the attacking host changes distributed_1 to distributed_7 but the attacked service wu.ftpd remains the same over a period of time. It would be highly unlikely that this behaviour or pattern is anything other than an attempted distributed attack on a system on that particular service.
Web of Control - Tripwire Web

Squid file caching systems exchange intelligence relevant to their function as caching proxy servers via a distributed and trusted hierarchy of machines. The required intelligence is broadcast based along the network based upon established trust relationships throughout the connected network via specific port and protocol of exchange.

An intrusion detection system that incorporates this functionality for gathering attack intelligence could be a formidable foe even for the wiliest attacker. The NIDH leverages this idea of a trusted hierarchy of interconnected hosts to be the backbone upon which to transfer attack intelligence between hosts to be utilised by defensive countermeasures installed on these hosts. One of TCP/IP's inherent strengths is its ability to packet switch and route around troublespots in a network in this case a disconnected server. Due to this arrangement, a parent/sibling mesh as per Figure 2 can exist and should one system become inoperable it will not unduly affect others within the mesh.

![Figure 2: Sample NIDH Hierarchy](image)

Each node on the network when arranged such as in Figure 2 having parent and sibling relationships with others becomes a trip-wire mechanism in itself. For example, if Host 3 in this scenario were attacked it would send "attack intelligence" to Host 4 who then sends to Host 5. Packets would also flow to Host 2 who sends to Host 5 and Host 1 respectively. This flow is illustrated in Figure 3

![Figure 3: Packet Exchange Trace for an Attack originating against Host 3](image)

So automatically, the machines that receive the intelligence packets from other NIDH connected Hosts can use this information to better defend themselves. Having received the attack intelligence packet from an upstream Parent Host, the Receiving Host can use the intelligence to protect itself. It could apply firewall routing blocks to deny the requisite services to the Attacker Host IP Address before it even begins to scan or attack that machine. For simplicity the example, given of course is one instance of an attack on one machine the logic of which can apply across the entire interconnected hierarchy.
The trusting of packets that are sent between the servers in the hierarchy can be problematic if a host is compromised and used to attack the hierarchy. The firewalls and IDS on the connected systems should be set such that they only accept packets from the trusted NIDH socket and any other standard ports such as mail or web. This should be done to protect hosts against being attacked by a compromised host that is in the hierarchy. As a system that sends a scan or SYN packet to other than the trusted sockets to the other hosts will be automatically removed from the hierarchy.

The Attack Intelligence Packet

To reduce information redundancy and increase the ability of the mesh to counteract attack, the "intelligence packet" needs some special design considerations. As in Figure 3 if we were just broadcasting to the systems the Attacking Host IP 203.38.0.163 and the service/port 80 that it is attacking then this data would become repeated. In the example given above, it would receive duplicate packets at Host 5 as it would receive this packet from both Host 4 and Host 2. So to reduce this redundancy the packet should contain a Timestamp, Victim Host, Attacking Host plus the attack detail as follows in Table 1

<table>
<thead>
<tr>
<th>Time &amp; Date 1/1/70 format</th>
<th>Victim Host Details Hostname/IP Address</th>
<th>Attacking Host IP Number</th>
<th>Port Attacked</th>
</tr>
</thead>
<tbody>
<tr>
<td>1235663.6</td>
<td>Host 3/10.0.0.3</td>
<td>203.38.0.163</td>
<td>80</td>
</tr>
</tbody>
</table>

Table 1: Sample Attack Intelligence Packets

Hence Host 5 upon receiving the "duplicate" packet could simply drop it or compare the two packets and check the validity of the packet. The packet upon receipt could be passed to the firewall to block/deny access to that IP on that port based upon the firewall control policy of that particular host.

The NIDH packet may seem positively benign and lacking in information when compared to a Common Intrusion Specification Language (CISL) packet (Tung et al., 1999). The (CISL) is a highly detailed and rich language for the purposes describing attacks as part of the Defense Advanced Research Projects Agency (DARPA) run Common Intrusion Detection Framework (CIDF) project (Staniford-Chen, 1998). The intent of NIDH is to provide a fast, reactive defensive mechanism that allows rapid exchange of attack intelligence.

To analogise the difference between the two packets, consider an exchange of fire between two parties. NIDH simply identifies where the shooter and the direction the bullets are coming from. The CISL however tells you who the shooter purports to be, what bullet they are using, from how far away, what gun they are possibly using and so on to a large degree is superfluous information. While CISL and other rich descriptive languages may help in the ex-post analysis the basic underlying tenet is the same. If someone is spraying bullets at you, who cares what type they are if there is an immediate threat of damage, get out of the way.

In addition, to reduce a possible broadcast storm created by small packets of information, the packets could be sent at predetermined intervals between systems in much the same way that Squid uses digests to compare cache contents between systems.

Group Memory or Digest

To make the system more effective, a use of digest/memory devices will be needed. There needs to be a short-term event table, which for the purposes of this model we will call the volatile digest, could be held on each machine in much the same way that a bridge holds a route table. This could be stored in the random access memory of the server as a table.
Long-term memory, could be in the form of a disk written digest which the author will call the permanent digest. This is a similar mechanism to what Squid already uses to tell each cache what is available at its parent cache by regular exchange of digest information. The purpose or intent here is to use this permanent digest for when a server rejoins or joins the network that the server will simply request and receive a copy of the digest from its nearest neighbour system. Having got the permanent digest it would then use the information in this to generate denial routing instructions for the firewall that is running on the system. Hence the system is using the attack intelligence stored in the collective memory of the NIDH to prevent against known attacking or malicious hosts.

Time stamping and check pointing of files should be used to send only the new additions to the digest to other computers in the NIDH. This will help overall in the reduction of traffic across a network, as the files sent will be physically smaller. It will also make it relatively easier for machines in the hierarchy to update their digests, as they will be comparing the small incoming file with the larger resident digest file as opposed to processing two large files.

**Sifting the Malicious from the Non-Malicious**

One of the problems with the proposed NIDH system as with all intrusion detection systems is determining what constitutes an attack. The NIDH system described here is by no means is perfect in this respect. However, it is an improvement on existing systems due to the ability to gather attack intelligence from a variety of dispersed hosts.

Take for example a wily attacker who uses a single scan of a single service as opposed to a brute force attack on all ports that an inexperienced or less overt attacker would typically use. If the wily attacker replicates this attack on other hosts within the NIDH then the certainty that this attack is non-malicious declines rapidly. By utilising the volatile digest features of the NIDH and scanning it for replicated attacking IP numbers on different NIDH servers over a given timeframe, for instance, 24-hours a detection of these stealthy attacks should occur. In the case of any of the intrusive IP numbers matching then the certainty that these detected intrusions are indeed possibly malicious in intent would start to increase in probability. A rating of attack magnitude could be assigned as well for the gathered attack intelligence.

A distributed attack is problematic for most commonly available defensive mechanisms due to the singular, and often disconnected, silicon fortress mentality from which they are designed and implemented. Unlike existing systems, the NIDH by the use of distributed attack intelligence sharing should provide a method of inoculating the other NIDH connected servers against a distributed attack. The servers should have learned about the attacking machines via regular NIDH intelligence exchange.

The sometimes transient nature of attacking hosts either because of semi-permanent hosts using DHCP or the fact that potential attackers may use a variety of machines to attack can prove problematic for this countermeasure design. The proposed digest system may have some persistence problems for "legitimate" users who wish to access the system who may be using "transient IP" services for example dialup users of an ISP. However, this far outweighs the potential risk of a malicious compromise of a system. Non-malicious insiders could be problematic also but a simple trust table that ignores trusted internal IP numbers that is incorporated alongside the digest system will remove this problem.

**Secure Intelligence Exchange**

One of the problems with a system such as the NIDH is the secure exchange between entities in the system of intelligence information. For this system to be effective, it is important that there is some way of verifying the authenticity of the sender and the integrity of the transmitted packet. An obvious way this can be achieved is by the use of a Public Key Infrastructure (PKI) to facilitate encryption of data and also as means of authentication.
A PKI allows these attributes to be enhanced and allows for the ready encryption of data streams as well by using digital certificates. PKI also allows for the revocation of keys allowing removal of rogue or compromised servers.

Of course, the problem with a PKI is the administration and security of the actual PKI itself. One way of overcoming this is by using a network of notaries. Notaries can help administer and notarise new members into the network as well as leveraging existing Certificate Authority systems and providers such as Verisign, Thawte or other providers to further verify identity. The use of encryption and PKI while having processing overheads is necessary to increase the authenticity and integrity of the packet within the distributed network.

CONCLUSION

As pointed out in the introduction, the number and complexity of attacks and probes is on the increase. The use of automated tools, some of which are capable of distributed attacks, can create sophisticated and sustained attacks on hosts with minimal computer knowledge is also increasing. However, most of the counter measures that are in place today are still in a singular defensive paradigm and are poorly equipped to cope with these new distributed, automatic tools.

If we are to effectively reduce the risk mitigated by these increases in intensity, complexity and ubiquity of network probes and attacks. Then the development of a system or systems that share attack intelligence and use distributed means to exchange this intelligence are needed. The old adage “united we stand, divided we fall” should now be, “networked we stand, distributed we fall”. If we are to defeat the distributed, automaton hacker of the new millennium, distributed defensive measures must be developed.
REFERENCES


ABSTRACT

Let $S_0, S_1, S_2, \ldots, S_n$ be a family of $n + 1$ symplecta in a parapolar space that satisfies the following property (g):

For each point $x$ not in a symplecton $S_i$ we have $x^{1/S}$ is a single point.

Let $x_0$ be a point in $S_0$, then, by (g), there is a point $x_1 \in S_1$, with $x_1 = x_0^{1/S_1}$. Define by induction $x_{i+1} = x_i^{1/S_{i+1}}$, $i = 1, 2, \ldots, n$, $x_{n+1} = x_n^{1/S_0}$ (indices of symplecta are taken modulo $n$). To encipher we match $x_0$ to $x_{n+1}$ and to decipher we reverse the process from $x_{n+1}$ to $x_0$ using the corresponding symplecta in a reverse order.

One geometry among others that satisfies property (g) is the half-spin geometry $D_{6,6}(F)$. In this work we construct the half-spin geometry and explain how to make up the cipher system using this geometry. Many properties of this geometry will be derived.

Key words: half-spin geometry, cipher system, Cryptography, parapolar space, Lie incidence geometries, hyperbolic geometry.

INTRODUCTION

This is the age of information technology. One of the means to protect information from invaders is to encipher this information. Many different methods and algorithms have been studied and applied in the past 50 years. Many authors have written tens if not hundreds of paper about information and computer security. The purpose of this paper is to add to the literature in this field. What is special about this paper is the use of geometric means and properties instead of algebraic ones to implement the cipher system. Some of the geometric material contained here can be found in other sources. The geometric properties that we will use can be derived from the algebraic structure. For more information about the half-spin geometries see Shult (1994), or Cooperstein (1997).

BASIC ALGEBRAIC DEFINITIONS AND NOTATIONS

Let $B$ be a symmetric or alternate bilinear form defined on a vector space $V$ over an arbitrary field $F$. For a subspace $W \subset V$ we set

$W^\perp = \{u \in V : B(u, v) = 0, \text{ for all vectors } v \in V \}$. $V^\perp$ is called radical of $V$ with respect to $B$. A bilinear form $B$ on a vector space $V$ is called non-degenerate iff $V^\perp = \{0\}$. Otherwise $B$ is called degenerate.

Two forms $B_1, B_2$ on $V$ are said to be equivalent if there is a one-to-one and onto linear transformation $\psi : V \rightarrow V$ such that $B_1(u, v) = B_2(\psi(u), \psi(v))$. 

Mohammed Suliman El-Atrash

Department of mathematics
Science College
Islamic University of Gaza
P.O. Box 108
Gaza, Palestine
Email: matrash@mail.iugaza.edu

Ciphering Using Half-spin Geometry $D_{6,6}(k)$
A vector \( u \in V \) is called an isotropic vector, if \( B(u, u) = 0 \), and a subspace \( W \) of \( V \) is called totally isotropic (abbreviated TI) subspace of \( V \) if \( B(u, v) = 0 \) for all \( u, v \in W \). If a TI subspace \( W \) of \( V \) is not contained properly in any TI subspace of \( V \), \( W \) is called maximal totally isotropic (abbreviated MTI) subspace of \( V \).

It can be shown (see Bierbrauer (1997)) that all the MTI subspaces have the same dimension it is called Witt index of \( V \) and is denoted by \( \text{ind}(V) \). Two vectors \( u, v \) are called orthogonal if \( B(u, v) = 0 \).

A 2-dimensional vector space with non-degenerate bilinear form \( B \), in which there is an isotropic vector \( u \) is called a hyperbolic plane, otherwise it is called an anisotropic plane.

A vector space \( V \) of dimension \( 2n \) is called hyperbolic if \( V \) is endowed with a symmetric bilinear form of Witt index \( n \), and is called elliptic if Witt index is \( n - 1 \).

The following couple of Theorems explains the structure of vector spaces endowed with bilinear forms, for references see Bierbrauer (1997).

Theorem. Let \( B \) be a non-degenerate symmetric bilinear form on a vector space \( V \) of dimension \( 2n \) over a finite field \( F \). Then \( B \) is a hyperbolic form on \( V \) iff \( V \) has a basis \( \mathbf{A} \), such that \( V = H_1 \perp H_2 \perp \ldots \perp H_n \), where all \( H_i \) are hyperbolic planes, \( i = 1, 2, \ldots, n \) with \( \text{ind}(V) = n \).

It shows that all hyperbolic non-degenerate symmetric bilinear forms on a certain vector space are equivalent. To find one we will revert to following theorem that determines when the scalar product is hyperbolic.

Theorem. Let \( B \) be the Euclidean scalar product on a vector space of dimension \( n = 2r \) over the finite field \( F \) of order \( k \). Then if both \( k \) and \( r \) are odd

(a) \( B \) is a hyperbolic form iff \( k \equiv 1 \pmod{4} \).

(b) \( B \) is an elliptic form iff \( k \equiv 3 \pmod{4} \).

Furthermore, if \( r \) is even integer, or \( q \) is even; \( B \) is always a hyperbolic form.

### BASIC GEOMETRIC DEFINITIONS

Given a set \( I \), a geometry \( \Gamma \) over \( I \) is an ordered triple \( \Gamma = (X, *, D) \), where \( X \) is a set, \( D \) is a partition \( \{X_i\}_{i \in I} \) of \( X \) indexed by \( I \), \( X_i \) are called components, and * is a symmetric and reflexive relation on \( X \) called incidence relation such that:

\[ x * y \text{ implies that either } x \text{ and } y \text{ belong to distinct components of the partition of } X \text{ or } x = y. \]

A point-line geometry \( (P, L) \) is simply a geometry for which \( |I| = 2 \). One of the two types is called points \( P \), and the other type is called lines \( L \). In this paper we will not be concerned about geometries that contains lines that are incident with the same set of points, therefore, without loss of generality we may consider incidence as containment i.e., \( p \in P \) and \( l \in L \), then \( p * l \) if and only if \( p \in l \). In a point-line geometry \( (P, L) \), we say that two points of \( P \) are collinear if and only if they are incident with a common line.

The symbol \( x^+ \) means the set of all points collinear with \( x \), including \( x \) itself. A point line geometry \( \Gamma = (P, L) \) is called singular or (linear) if every pair of points are incident with a unique line.

A subspace of a point-line geometry \( (P, L) \) is a subset \( X \subseteq P \) such that any line which has at least two of its incident points in \( X \) has all of its incident points in \( X \), \( \langle X \rangle \) means the intersection over all subspaces containing \( X \).
In a point-line geometry $\Gamma = (P, L)$, a path of length $n$ is a sequence of \( n + 1 \); \( x_0, x_1, \ldots, x_n \) where, \( x_i, x_{i+1} \) are collinear, \( x_0 \) is called the initial point and \( x_n \) is called the end point. A geodesic from a point \( x \) to a point \( y \) is a path of minimal possible length with initial point \( x \) and end point \( y \). We denote this length by \( d_\Gamma(x, y) \). $\Gamma$ is called connected if for any pair of distinct points \( x, y \) there is a path connecting them.

**BASIC SPACES**

For the following definitions see Cohen (1993).

A gamma space is a point-line geometry such that for every point-line pair \((p, l)\), \( p \) is collinear with either no point, exactly one point, or all points of \( l \), i.e., \( p \perp l \) is empty, consists of a single point, or all points of \( l \).

A polar space is a point-line geometry $\Gamma = (P, L)$ satisfying the Buekenhout-Shult axiom:

For each point-line pair \((p, l)\) with \( p \) not incident with \( l \); \( p \) is collinear with one or all points of \( l \), that is, either \( |p \perp l| = 1 \) or else \( p \supset l \).

We write \( \text{Rad}(\Gamma) \) for the set \( \{ p : p \perp = P \} \), and is called the radical of \( \Gamma \). A polar space \( \Gamma = (P, L) \) is said to be non-degenerate if and only if \( \text{Rad}(\Gamma) = \emptyset \).

A point-line geometry $\Gamma = (P, L)$ is called a parapolar space if and only if it satisfies the following properties:

(a) is a connected gamma space,
(b) for every line \( l \); \( l \perp \) is not a singular subspace,
(c) for every pair of non-collinear points \( x, y \); the set \( x \perp y \perp \) is either empty, a single point, or a non-degenerate polar space of rank at least 2.

Let \( V \) be a vector space of dimension 3 over a finite field \( F = \text{GF}(k) \), where \( k \) is a prime power. The classical example of a projective plane is the geometry we get by taking the points to be the one-dimensional subspaces of the vector space \( V \), and the lines to be all 2-dimensional subspaces of \( V \).

In general, if we take \( V \) to be a vector space of arbitrary dimension \( n \) more than 3 then the geometry we constructed in the last paragraph is called a projective space of singular rank \( n-1 \).

**DEFINITION OF THE HALF-SPIN GEOMETRY \( D_{n,n}(F) \)**

Let \( B \) be a symmetric hyperbolic bilinear form defined on a vector space of dimension \( 2n \). A Polar space of type \( \Omega_{2n}^+(k) \) is the point-line geometry \( (P, L) \), where \( P \) is the set of all isotropic one-dimensional subspaces \( \langle x \rangle \) of \( V \), and \( L \) is the set of all TI 2-dimensional subspaces.

Let \( T_i \) be the set of all TI \( i \)-dimensional subspaces of \( V \), \( 1 \leq i \leq n-2 \). Let \( T_n \) be the class that consists of all maximal TI subspaces of dimension \( n \). It can be shown that (see see Shult (1994)) \( T_n \) is partitioned into two classes denoted by \( M_1 \) and \( M_2 \) subject to the following rule:

Two maximal TI subspaces \( m_1 \) and \( m_2 \) of \( V \) belong to the same class if and only if the dimension of \( m_1 \cap m_2 \) has the same parity as \( n \).

The half-spin geometry \( D_{n,n}(F) \) is defined as the point line geometry \( (P, L) \) whose set of points is one of the classes say \( P = M_1 \) and the set of lines is the set \( L = T_{n-2} \). A point \( m_1 \in M_1 \) is incident with a line \( A \in T_{n-2} \) if and only if \( m_1 \supset A \).
In this work we are concerned only with the half-spin geometry $D_{6,6}(k)$; the reason for this particular case ($n = 6$) will be clear later. See comments below Property 3.

Here we summarize the construction of $D_{6,6}(k)$. We have a symmetric hyperbolic bilinear form $B$ on a vector space of dimension 12 over a finite field $F = \text{GF}(k)$. The classes $M_1, M_2$ consist of maximal TI 6-dimensional subspaces. Two TI 6-subspaces belong to the same class if their intersection is of even dimension. So the dimension of the intersection of $m_1 \cap m_2$ is 0, 2, or 4 for distinct $m_1, m_2$. Thus, the points of $D_{6,6}(k)$ consists of one class ($M_1$, say) of the two classes of MTI 6-spaces, and whose set of lines corresponds to the set of all TI 4-spaces, where, a line $l$ that correspond to a 4-subspace $X$ is incident with the set of all points that corresponds to all MTI 6-spaces that contains $X$.

Symplecta are the objects (subspaces) of the geometry $D_{6,6}(k)$ that correspond to the set of all TI 2-subspaces in $\Omega^+_{2n}(k)$; i.e., a symplecton $S$ that corresponds to a 2-subspace $Y$ is the set of all TI 6-subspaces that contains $Y$. TI 1-subspaces in $\Omega^+_{2n}(k)$ correspond to $D_{5,5}(k)$'s in $D_{6,6}(k)$. TI 3-subspaces in $\Omega^+_{2n}(k)$ correspond to projective subspaces of singular rank 3 in $D_{6,6}(k)$. TI 6-subspaces of the second class $M_2$ in $\Omega^+_{2n}(k)$ correspond to projective subspaces of singular rank 5 in $D_{6,6}(k)$.

We have been using one notation $\perp$ to mean two things; one to mean perpendicularity for subset of vectors with a bilinear form, second to mean collinearity in the geometries. It will cause no confusion.

**PROPERTIES OF $D_{6,6}(k)$**

The relations between some of the varieties of $D_{6,6}(F)$ geometry are mentioned below. Proofs can be deduced from properties of the underlying polar space $\Omega^+_{12}(k)$.

**Property 1.** For a point $p$ and a symplecton $S$, with $p \not\in S$, one of the following cases occurs:

(a) $p \perp S$ is a single point.

(b) $p \perp S$ is a maximal singular subspace of $S$.

**Property 2.** For any two distinct symplecta $S_1, S_2$, one of the following cases can occurs:

(a) $S_1 \cap S_2$ is a line.

(b) $S_1 \cap S_2$ is a maximal singular subspace of both $S_1, S_2$.

(c) $S_1 \cap S_2$ is empty.

**Property 3.** If $S_1 \cap S_2$ is empty then either (i) or (ii) can occur.

(a) for one (and hence every) point $p \in S_1$; $p \perp S_2$ is a maximal singular subspace of $S_2$.

(b) for one (and hence every) point $p \in S_1$; $p \perp S_2$ is a single point, in this case there is a bijection of $S_1$ onto $S_2$. Furthermore, for every $p \in S_2$; $p \perp S_1$ is also a single point. The two symplecta in this case are called parallel.

By property 1, we see that we have only two different cases for any point-symplecton pair $(p, S)$, either $p \perp S$ is a single point, or $p \perp S$ is a maximal singular subspace of $S$. By property 3, it follows that if we take a symplecton $S_1$ parallel to a symplecton $S_2$ then for every point $p$ in $S_1$ we have only one case, that is, $p \perp S_2$ is a single point. This property is the essence of this paper, we will use it to achieve the goal of this paper. Other geometries do not have such property even among half-spin ones.
CONSTRUCTION OF THE CIPHER SYSTEM

Let $S_0, S_1, S_2, \ldots, S_n$ be an $n+1$ parallel symplecta in the half-spin geometry $D_{6,6}(k)$. Let $x_0$ be a point in $S_0$ ($x_0$ will be our plaintext). It follows by property 3 that there is a point $x_1 \in S_1$, with $x_1 = x_0 \cap S_1$. Define inductively $x_i = x_{i-1} \cap S_i$, $1 \leq i \leq n$, $x_{n+1} = x_n \cap S_0$ ($x_{n+1}$ will be our ciphertext). To decipher we go back from $x_{n+1}$ to $x_0$ using the corresponding symplecta in a reverse order.

Clearly, the system is a private key system, in which the sequence of symplecta $S_1, S_2, \ldots, S_n$ must be kept secret as the key of the system. The message space and the ciphertext space is $S_0$. $n$ has to be larger than 1, since in this case the ciphertext is the same as the plaintext.

Next, we will discuss several aspects of this cryptosystem including: implementation of the system, Level of security of the system, complexity of the system.

In Shult (1994), The author showed that for the half-spin geometry $D_{n,n}$ there exists an embedding of it into a projective space $P(V)$ whose underlying vector space $V$ has dimension $2^{n-1}$. Therefore points of the half-spin geometry $D_{6,6}(k)$ are considered as projective points in $P(V)$ whose underlying vector space $V$ has dimension 32. Of course there are many of such embeddings (all are isomorphic).

Once we have a point $x_0$, (that is or contains the ciphertext $m$), that lies in a symplecton $S_0$, the point $x_1$ in $S_1$ that is collinear to $x_0$ can determined in the following way:

It is enough to show how to calculate $x_1$ from $x_0$, $S_0$ and $S_1$. In a similar fashion we calculate the rest of $x_2, x_3, \ldots, x_{n+1}$. We know that both $x_0, x_1$ are MTI 6-spaces. It follows that both can be represented by two $6 \times 12$ matrices $N_0, N_1$ respectively, where rows of $N_i$ represent a basis for $x_i$, $i=0, 1$. We know also that $S_0$ corresponds to a TI 2-space $\{\underline{u}_1, \underline{u}_2\}$, and $S_1$ corresponds to a TI 2-space $\{\underline{w}_1, \underline{w}_2\}$. We may assume without loss of generality that rows of $N_0$ are $\{\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4, \underline{u}_5, \underline{u}_6\}$, and rows of $N_1$ are $\{\underline{w}_1, \underline{w}_2, \underline{w}_3, \underline{w}_4, \underline{w}_5, \underline{w}_6\}$. The line that passing through $x_0, x_1$ corresponds to the TI 4-space $X = \underline{w}_1 \cdot \underline{w}_2 \cap \{\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4, \underline{u}_5, \underline{u}_6\}$. It follows that $x_1$ corresponds to the MTI 6-space $\{\underline{w}_3, \underline{w}_4, \underline{w}_5, \underline{w}_6\}$. To determine $X$, we need to find a four TI 4-spaces $\{\underline{w}_3, \underline{w}_4, \underline{w}_5, \underline{w}_6\}$. This can be achieved by finding a basis of the solution set of the following two equations:

\[
\begin{align*}
    w \cdot \underline{w}_1 &= 0, \\
    w \cdot \underline{w}_2 &= 0,
\end{align*}
\]

\(^*\)

where, $w = x_1 \underline{u}_1 + x_2 \underline{u}_2 + x_3 \underline{u}_3 + x_4 \underline{u}_4 + x_5 \underline{u}_5 + x_6 \underline{u}_6$.

Thus, we are looking for four independent solutions of the two equations (*) in 6 unknowns $x_1, x_2, \ldots, x_6$. Equations (*) can be rewritten as:

\[
\begin{align*}
    x_1 (\underline{u}_1 \cdot \underline{w}_1) + x_2 (\underline{u}_2 \cdot \underline{w}_1) + x_3 (\underline{u}_3 \cdot \underline{w}_1) + x_4 (\underline{u}_4 \cdot \underline{w}_1) + x_5 (\underline{u}_5 \cdot \underline{w}_1) + x_6 (\underline{u}_6 \cdot \underline{w}_1) &= 0, \\
    x_1 (\underline{u}_1 \cdot \underline{w}_2) + x_2 (\underline{u}_2 \cdot \underline{w}_2) + x_3 (\underline{u}_3 \cdot \underline{w}_2) + x_4 (\underline{u}_4 \cdot \underline{w}_2) + x_5 (\underline{u}_5 \cdot \underline{w}_3) + x_6 (\underline{u}_6 \cdot \underline{w}_2) &= 0.
\end{align*}
\]

\(^{**}\)

Coefficients of equations (**) are known

We do have four independent solutions $\{\underline{w}_3, \underline{w}_4, \underline{w}_5, \underline{w}_6\}$ of equations (*), since $\underline{w}_1$, $\underline{w}_2$ are independent (the two symplecta are parallel) and $\{\underline{u}_1, \underline{u}_2, \underline{u}_3, \underline{u}_4, \underline{u}_5, \underline{u}_6\}$ are in fact a MTI 6-space.

It follows that the whole system turned out to be finding out 4 solutions of a system of two equations (**). The solution can be calculated by any method like Gauss elimination method.
As for the complexity of the system, not much should be said about that, since clearly from the computations that this system is as complex as the DES system. To break such system it requires the solution of 2 equations in \( n \) variables of degree 6 which is considered as a hard problem. In fact we can add that the security level of such system is very high, because of the huge key space, and the arbitrariness of \( n, k \).

**SOME NUMERICAL FACTS ABOUT \( D_{6,6}(K) \)**

1. The number of points of the half-spin is \((k + 1)(k^2 + 1)(k^3 + 1)(k^4 + 1)(k^5 + 1)(k^6 + 1)\)
2. There are \((k^4 + 1)(k^5 + 1)(k^6 + 1)\) distinct symplecta that partition the set of points in the whole geometry.
3. The number of points in each symplecta is \((k + 1)(k^2 + 1)(k^3 + 1)\).

**REFERENCES**


Cohen, A. (1993) *Handbook of incidence geometry*


Designing Information Security for Small Businesses: Lessons from a Case Study

Dr. Terence Love

School of Management Information Systems
Edith Cowan University
Perth, Western Australia

ABSTRACT

This paper focuses on the different factors that impact on the design of information security for smaller businesses. A case study is used to identify issues, and costs of information attacks, preventative measures and remedial work. The paper identifies lessons for designing information security solutions for smaller businesses.

Keywords: Information Security, SME, Design, Human Factors

INTRODUCTION

Over the last five years, the use of computing and the Internet has become widely established in small businesses (NOIE, 2000, Australian Bureau of Statistics, 2001). There is increasing uptake by individuals and small businesses of online financial services such as online banking and share trading (NOIE, 2001). These changes, along with the fact that the most common computer operating systems used in small business (Windows 95/98) provide minimal data security (TheCounter.com, 2001, Schneier, 1999b, Schneier, 1999a), imply that information security issues are increasing in this sector. Resolving the information security issues of smaller businesses is important because they are the strongest growing area of the economy, they include the largest number of businesses, and their successful adoption of e-business is seen as a key factor in national economic and social development (NOIE, 2000, NOIE, 2001, Australian Bureau of Statistics, 1999, Australian Bureau of Statistics, 2001). This paper suggests, however, that currently, neither large nor small-scale information security solutions align with the realities of smaller businesses.

Information security and information warfare protection are important to all organisations. The increased role of computers and the Internet in business processes has increased the difficulty of providing information security, and increased opportunities for information warfare attacks (The SANS Institute, 2001). Traditionally, larger organisations have been earlier adopters of computers and computer networking, and have been the locus for aggregation of technical expertise in computing and networking. Together, these factors have shaped research into information security and information warfare, and the creation of information security solutions for large and small businesses (see, for example, The SANS Institute, 2001, Smith, 1997).

Computer and network information security products are, in the main, designed using a technical focus. Information security solutions designed for smaller businesses echo this preoccupation with technical issues, and as a consequence, most information security solutions for smaller businesses are "mini" versions of solutions aimed at larger organisations. For example, mini-firewalls have been developed for the small office/home office (SOHO) market, Internet browsers offer security settings, and a range of do-it-yourself file encryption solutions such as PGP are available.
This case study is aimed at identifying factors to support the design of information security solutions specific to small business through understanding the qualitative human issues and differences in the relative costs of information security problems to small and large businesses. The business owner in the case study estimated that the cost of responding to two successful information attacks on the business’ computer systems was equal to a year’s profit (not including the risks or consequences from important information being illegally used to gain access to bank accounts or other assets, or act against the business). The relative cost to small businesses of responding to an information attack is proportionally bigger than for larger organisations.

OVERVIEW OF THE CASE STUDY

This case study analyses a real incident in which a computer in a small business was infected by a virus, infiltrated, and information transferred to an unknown location on the Internet. A rich picture is developed of the costs and resources associated with addressing information security at the smaller end of the business organisation spectrum. This offers the basis for identifying factors for improving the designs of information security solutions for smaller business organisations. An overview of the incident is as follows:

1. Business is protected by antiviral software.
2. A viral attack breaks through this protection.
3. This viral attack is identified (in part) and steps are taken to recover the situation.
4. It becomes clear it is possible that systems and important financial data have been severely compromised – almost certainly by a secondary attack.
5. All business processes are stopped. Steps are taken to secure the financial arrangements with other organisations.
6. Computer and information security is reviewed, and outcomes are implemented in the computer systems.
7. Computers are tested and business processes rebuilt for the business to resume using its amended computer systems.
8. Ongoing plans made for surveillance on computer behaviour and financial documentation, and research into security issues.

Each of the above stages involved time and resources, and, in some, significant risks that challenge the future viability of the business. Several stages require high levels of technical expertise. For many smaller businesses, understanding about information security protection is strongly shaped by the advertising of information security products for the SOHO market and newagents magazines. A significant issue to emerge is management’s decisions are often strongly dependent on an intuitive analysis of situations, artefacts, systems and risks. These intuitions depend on designers of computers, software and Internet systems providing sufficient clues.

CASE STUDY IN DETAIL

Setting the scene: In this business, the computers are used for financial management, document creation, and image manipulation. Like many micro businesses the organisation is acquiring small-scale e-business functionality: it has its own website, takes orders over the Internet and is an early adopter of Internet banking and share trading services. Information security precautions before the attack consisted of regular backups, good email and file hygiene, carefully chosen passwords, and antiviral software from an international certified company. The anti-viral product was chosen because it updates from the Internet using spare bandwidth. The owner had tried other products and found that manual updating of virus signatures was often neglected. A large number of passwords were in use, and, because of this, were stored in an encrypted password database on this computer. At this stage it was not appreciated that encryption varies, and the level of encryption on this file was negligible. The business used three Windows 98/95 machines with a network printer in a small network whose
structure changed frequently. Each machine acts as a backup for others (the main function of the network) with 100Mb Zip backups stored off site. One computer was connected to the Internet (no Internet sharing). At the time of the attack, the Internet connected machine was physically disconnected from the network.

**Information Warfare Attack:** The attack concluded a hectic exchange of emails with another organisation. The last email contained a viral package. The message was from a trusted source. The title of the attachment was believable. The attachment was recognised as a virus because of the continuous sound of the hard drive transferring data. About two seconds after opening the attachment the power was cut and four seconds later (the APM delay) the computer shut down. It was restarted and a full virus scan undertaken. The scan showed several dozen files infected with a mix of viruses. The other organisation was notified. They confirmed they had not intentionally sent that attachment and later confirmed their machine was infected. Further investigation showed the anti-virus scanner had been reset from 'real time' to 'scheduled' (unclear whether due to the attack or due to an omission from the previous day when real time scanning was turned off temporarily to install software).

**Remedial Action:** The first stage in the remedial process (undertaken as part of the full scan above) was to instruct the anti-viral software to repair the infected files. This it did but leaving a small amount of doubt due to its screen messages being inconsistent. Most of the viruses were not described in the software manufacturer’s virus database. An Internet search was undertaken to find out more about the viruses to understand the scale of security breach. The picture that emerged was complex: the infected email had contained many viruses each with different functionality (Trojans, bombs, backdoors).

In restoring files to bring the machine back to a pristine functional condition, the virus checker was reinstated and set to scan real time. In addition, a repeat full scan was initiated. To the owner’s surprise, an even greater number of virus-infected files were identified, many different from first time round. Eventually, after using the repair function with full scan six times, all files were clear but dozens of systems files had been deleted that the anti-virus product could not repair. The computer would boot and run, but not to specification. The hard disk of the machine was reformatted and software and data were reinstalled. The backup regime meant that almost all the data was secure. The only significant loss was of two weeks of emails and appointments. The Outlook personal folder (85Mb) refused to load, and this necessitated using an archive.

A this point, the concern that information security had been compromised was offset by the awareness the virus was not specifically targeted at this computer, and there was no evidence that viruses had propagated from this machine to colleagues whose addresses were stored on it. Precautionary measures included the removal of all banking information from the computer, and it was decided that for 6 months particular attention would be paid to financial documentation. It was concluded that the failure of protection against the information attack was probably due to real time virus checking being inadvertently disabled, and perhaps the heuristic virus identification process had confused sound files as infected. Details of the incident were sent to the anti-virus software manufacturers because of the failure of the software to clearly identify that it had not removed or neutralized the viruses it had found and a reply awaited.

**The Second Attack:** In the days following the incident, it became clear that things were not right but, at first, this was put down to paranoia. The sizes of downloads and uploads did not correlate with files being transferred; beyond differences expected from telephone line quality or poor server response. In addition, the computer did not behave in exactly the way it was expected. Suspicions increased in intensity when the machine was found dialing whilst unattended. The machine was isolated whilst further research into information security was undertaken, and again the hard drive was reformatted. Around this time, a similar failure by the same antiviral software was identified at another organisation. In this case, ‘real time’ scanning was fully functional: the software appeared to have failed to stop virus infestation.
Research into virus protection led to sites offering free security testing. This indicated a serious security failure due to its network configuration that allowed its drives (and those of any other machines on this network) to be viewed and manipulated remotely. This failure preceded the virus attack.

**Stop the Business:** The business was stopped. An increased understanding of cracking software led to the realisation that the password system and its encrypted storage was not secure. Along with other private information on the computer, this exposed the business and owners bank accounts. Banks were contacted, the situation explained, and advice sought. This process took considerably longer than expected due to lack of expertise by bank staff. The most common response was that nothing needed to be done, but that the bank was not responsible for any losses. Senior managers at banks revealed that they did not have processes for situations where customers’ online security was compromised. The only secure solution was to close all online banking and other arrangements. This was done and new passwords obtained for all other accounts.

After turning off file sharing, and binding the network onto Netbeui and off Tcp/ip, file download sizes normalized and the computer no longer suffered fits of erratic behaviour.

**Review Information Security:** The business was restarted using manual systems and a search undertaken for a better security model. At this stage it was clear that the major risks were banking and other assets, and major costs were the time and effort needed to respond to attacks. A rough calculation indicated the costs of responding to two similar attacks per year would neutralise profit margins. Two main improvements were identified: increasing protection against attacks and reducing the cost of responding to a successful attack. The first implied some form of firewall, protection against unauthorized access to files, and a change of anti-virus software. The second implied reducing time and labour costs to restore the computer system back to good working order.

**Computer Changes:** The solutions identified consisted of moving to Windows 2000 (for its file security, and, more importantly, its self-repairing ability), and installing a firewall and new anti-virus software. Identifying suitable software proved problematic. All of the major software manufacturers of SOHO level firewalls and anti-virus software make similar claims: that they will provide complete protection, and are easy to set up and use. The only significant differences are in the branding image presented, e.g. ‘Cheap, Cheerful and Scary’, ‘Serious and Responsible’, ‘Corporate and Mobile Professional’ and ‘Professional but with Shareware origins’. The preferred solutions were chosen because their manufacturer offered a web-based security test, and because of comments in magazine reviews.

**Testing and Rebuilding Business Processes:** Windows 2000 and new firewall and anti-viral software installed apparently without problems. The system was tested using the manufacturer’s web-based security tests and the newly hardened system came out as fully secure. New business systems were developed to avoid keeping on computer any financial and asset related information that might be used to illegally gain access to businesses assets. The operational software and data was reinstalled and configured. The ‘hardened’ machine was brought into action on the Internet.

**Ongoing Surveillance:** Attention was given to unusual machine behaviour or unusual events on bank and credit card accounts.

**Ongoing Research into Information Security:** Resources were committed to researching computer information security through subscribing to two electronic newsletters.
ANALYSIS

At its simplest, this case study describes a small business organisation caught with inadequate information security protection at all levels. Regardless of the anti-viral protection in place, the business's computer systems were open to identification via share sniffing software. Using this technology, the information attacker had full access over the Internet to the business's hard drive shares and files as soon as the IP address was identified.

The successful virus attack was useful because it drew the business owner's attention to resolving security issues and building stronger protection.

**Lesson 1:** Unless the system had been obviously and successfully challenged it is unlikely improvements would have been made.

The case shows how the usual advice about opening attachments is problematic in small business contexts. Many organisations that a business interacts with have imperfect security systems, and small businesses frequently do business with individuals and organisations of which they know very little. An email order from an unknown customer is not an unusual event, and, accepting occasional losses is preferable to having rules that block business.

**Lesson 2:** Small business arrangements are often insecure because they are co-located (same machine or same insecure network) with systems and information that require high security. Minimising this co-location is important (Smith, 1997).

It is not sufficient to rely on manufacturer's advertising claims as shown by the failure of the original anti-viral software, and by the new firewall. After a few days, the firewall was again tested - it failed. The manufacturer's recommended firewall settings lead to a failed condition by their own security tests. Resetting the firewall ports and services is not well explained in the manual but with technical support from a colleague the firewall was again secured. Even then, the firewall failed Gibson Research (www.grc.com) security tests.

**Lesson 3:** Processes by which small businesses are informed about security software are often flawed because software manufacturers are one of the major sources of information, and their information provision is biased by the need for its marketing and advertising role to act in their favour. Small businesses need to be able to identify appropriate software through ways that are more successful than present.

Banks and other organisations have a significant role in information security for smaller businesses. Currently, banks are trying to maximize profits by reducing transaction costs, and as part of this process are encouraging small businesses to use online banking services. The move online results in significant shifts in security issues for businesses. Physical security solutions are well established and responsibilities well-delineated and accepted. In the move online, financial institutions have effectively transferred more of the share of risks of information sharing onto small business clients because more of the technical aspects of the processing happen at the clients' end of the network. More significantly, banks have reduced their participation in resolving practical aspects of information security. Their responses to a lost chequebook and a lost set of internet banking passwords are different (they know what to do about a lost chequebook) and do not align with the differences in potential for losses to the business (a lost chequebook is less risky to the business).

**Lesson 4:** Improved designs for improved information security solutions for small businesses must include improvements to financial institutions systems in the areas of rights and responsibilities.

For smaller businesses, such as that described above, a substantial economic effect of the information attacks was in terms of costs of recovering the systems. Proportionally, the effort, labour costs and resources needed to recover business processes back to full functionality are much higher in smaller
than in larger companies. This is intrinsic: total costs of ownership are dominated by economies of scale gained through the use of standard operating environments - a situation unlikely in small businesses using a variety of computers.

**Lesson 5:** Designing information security solutions for smaller businesses requires a strong focus on minimizing the cost of keeping the system functioning securely. Hardware prices have reduced to the level that making a complete copy of a software environment on a hard drive (stored perhaps off site) is becoming economically practical. Perhaps the most important issue to emerge in this case study is that the back door Internet access to the business' computers was discovered because of increased sensitivity to unusual events and behaviours. The realisation that security software does not guarantee information security came from detailed exploration of the literature

**Lesson 6:** Surveillance, research and reflection are important aspects of information security, and, hence, supporting them is an important issue in designing solutions for small businesses.

Some weeks after the final system was in place and functioning, it was discovered that all users had access to all files. Windows 2000 is not secure as installed. Over 300 changes are needed to secure its base configuration (Schneier, 1999a). Resetting file permissions was neither intuitive nor straightforward.

**Lesson 7:** In design terms, when users are told that software provides a service then it is necessary to tell them when it is not implemented - especially in relation to security.

**QUANTITATIVE ISSUES**

The direct costs of addressing the information attack were identified by the proprietor. The limitations of memory in these circumstances mean that the costs may understated. The proprietor's estimates are listed below:

<table>
<thead>
<tr>
<th>Task</th>
<th>Time</th>
<th>Cost ($50/hr)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifying attack, researching virus details, redoing virus checks, reformattion computer rebuilding software and data</td>
<td>16 hrs</td>
<td>$800</td>
</tr>
<tr>
<td>Attempting to resolve problems with Outlook file</td>
<td>4 hrs</td>
<td>$200</td>
</tr>
<tr>
<td>Removing banking and other sensitive information – backing up and creating new manual system</td>
<td>3 hrs</td>
<td>$150</td>
</tr>
<tr>
<td>Move the business completely back to manual systems. Reformat the computer.</td>
<td>10 hrs</td>
<td>$500</td>
</tr>
<tr>
<td>Discussions with banks and other financial institutions</td>
<td>6 hrs</td>
<td>$300</td>
</tr>
<tr>
<td>Research into information security and security software issues</td>
<td>12 hrs</td>
<td>$600</td>
</tr>
<tr>
<td>Buying and installing new OS and information security software, rebuilding and reconfiguring system and testing</td>
<td>18 hrs</td>
<td>$900</td>
</tr>
<tr>
<td>Checking website for intrusion</td>
<td>3 hrs</td>
<td>$150</td>
</tr>
<tr>
<td>Reconfiguring firewall software</td>
<td>4 hrs</td>
<td>$200</td>
</tr>
<tr>
<td>Final developments of new business system</td>
<td>8 hrs</td>
<td>$400</td>
</tr>
<tr>
<td>Resolving network issues and implementing file sharing restrictions</td>
<td>9 hrs</td>
<td>$450</td>
</tr>
<tr>
<td>New operating system software, information system software, replacement of programs that wouldn’t work under Win2000, office material</td>
<td>(Approx)</td>
<td>$1100</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>$5750.00</strong></td>
</tr>
</tbody>
</table>
Other costs, more significant than direct costs, include:

- Loss of business with the organisation that sent the virus laden email (and a significant loss of collaborative potential).
- Losses of efficiency from changing business and computer systems to more secure but less streamlined processes
- Losses from time business stopped trading.
- Potential future losses due to misuse of information transferred out of system.
- Costs of ongoing surveillance and information security issues research

CONCLUSIONS

Several conclusions emerge from this case study into a small business recovering from an information system attack. First, the most significant issues are non-technical, regardless of the fact that the attacks and response occur via computer subsystems that are essentially technical. These issues point to several lessons for those designing improved information security solutions for smaller businesses. Taken together, they suggest that designing improved forms of information security software or systems may be more effectively based on disciplines of ergonomics, organisational design and management systems design rather than having a purely technical focus.

REFERENCES


A Random Access Symmetric-Key Encryption System for Network Security

Pengbo Liu \(^1\) and Tan Tiong Hok, Daniel \(^2\)

\(^1\) S2-B3-a06, 
Information Research System Lab 
Nanyang Technological University 
Singapore, 639798 
Email: Liu_pengbo@hotmail.com

\(^2\) Center for Educational Development 
Nanyang Technological University 
Nanyang Avenue 
Singapore 639798 
Email: ethtan@ntu.edu.sg

ABSTRACT

In this paper, a new encryption system framework will be described. The process is called the Random Access Symmetric-key Encryption System (or RASKES). It utilizes simple operations such as XOR, NOT, etc or combinations on variable length of sub-plain-text. The encryption process is based on the combination of random sub-key access, random algorithms access and the variable length of data sub-block encryption. From the output of a PRNG (pseudo-random number generator), a series of tri-values will retrieve elements of the sub-key and algorithms to encrypt a corresponding sub-text. The length of the sub-text is partitioned as the same length of sub-key during encryption.

Keywords: encryption, symmetric key algorithm, session key, PRNG and one time pad

INTRODUCTION

Current designs and approaches of encryption consider algorithms whose strength depends on key length [1]. With the use of high-speed computers, fast performance of the encryption and decryption processes can be achieved. However, no matter how strong an encryption algorithm is, many can be broken by exhaustive search. The present premise for much of today’s algorithm is that the time taken for such a search will not be practical or feasible.

Encryption is the process of disguising a message in such a way to hide its substance. An encrypted message is called cipher text. And the process of turning cipher text back into plaintext is called decryption. Currently much research has gone into the design of highly secure encryption system intended to protect sensitive information. However, no matter how strong these algorithms are, they could always be broken by exhaustive search except a well-known scheme – one time pad.

There are two general types of key-based algorithms: symmetric-key algorithm and public-key algorithm. Symmetric key encryption is a scheme in which the encryption and decryption process shares the same key. These algorithms, also called secret-key algorithms, single-key algorithms, or one-key algorithms, require that the sender and receiver agree on a key before they can communicate securely. As long as the communication needs to remain secret, the key must remain secret. Some famous symmetric key encryption algorithms are DES, FEAL, IDEA and GOST [2].
Public-key algorithms (also called asymmetric algorithms) are designed so that the key used for encryption is different from the key used for decryption. Further more the decryption key cannot be calculated from the encryption key. The scheme is called "public-key" because one of the encryption keys can be made public. A complete stranger can use that public key to encrypt a message, but only the specific person with the corresponding decryption key can decrypt the message using his private key. One of the most popular used public key algorithms is RSA, which have been implemented practically, could be found in great detail in the following website [3].

According to Shannon's information theory, only if the number of possible keys is no less than the number of possible messages, the cipher becomes unbreakable [4]. In other words, the key must be at least as long as the message itself, and no key be reused; then the cryptosystem will achieve perfect secrecy. One time pad is such a scheme. It is a large non-repeating set of truly random key letters, written on individual sheets of paper. They are then glued together into a pad. The sender uses a key letters on the sheet from the pad to encrypt exactly a one plain-text unit of equal length (typically one letter). Each key letter is used exactly once for only one message. The sender completes the encryption the message and then destroys the used pages of the pad. The receiver has an identical pad and uses each key on the pad pages in a reversed fashion to decrypt the message [5].

However, to be put into practical use, there are two weakness of one-time pad: Firstly the key bits in the pad must be random, with the length of the key sequence equal to the length of the message. Secondly, the key sequence could never be used again. Even if a multiple-gigabyte pad is used, if a crypto-analyst has multiple cipher-texts whose key overlap, he can reconstruct the plain-text. He could slide each pair of cipher-text against each other and count the number of matches at each position. Then he can, subsequently break it.

To overcome these disadvantages, a new encryption system is designed, consisting of an Encryption Algorithm Library (or EAL), a pseudo-random number generator (PRNG), a Crypto-Engine, and a plain-text pre-processor. A "one-time pad" will be generated for each plain-text: a sub-key will be uniquely generated by hopping over the span of a long master key through the session key acting as a seed to the PRNG. In addition, variable length of plain-text will be encrypted using its output, coupled with a wide range of algorithms to be used to enhance the security of encryption process.

The following content of this paper has been organized like this: At the beginning the components of RASKES will be discussed in detail. Then it described the decryption process. Finally, the conclusion is given with the simulation results.

RASKES – DESIGN AND PRINCIPLE

The goal of the Random Access Symmetric-key Encryption System (RASKES) is to provide efficient and secured trustful service. It is relatively easy to use. Even for those inexperienced cryptographers, it is not difficult to understand the operating philosophy of RASKES. In that regard, its simplicity creates implicit trust among the users. The architecture presented here is built on the following principles:

Object independence - each object is responsible for managing its own resource requirements such as memory allocation and use of other required objects. For example, an object could use another object's function without handling any low-level details inside. For the algorithms to be added for encryption use - the user does not have to take care of the encoding issues of the other objects.

Intelligent objects - The architecture should know what to do with data and control information passed to objects, including the ability to hand it off to the other objects where required. This leads to a very natural interface in which the user knows the object will do the right thing, without requiring it to be accessed or used in a particular manner.
The new system is based on the symmetric or secret key system. Only one key is used for the encryption and decryption. A master key is used for extracting sub-keys. All the sub-keys are extracted from this master key. Those sub-keys are of variable lengths based on a parameter $L$. Derived from the principle of one-time pad; the length of individual sub-key is the same as the corresponding sub-plaintext. The features of RASKES are as follows:

- Random access to the algorithms in a selectable library
- Random access for master key hopping
- Random length of the data block to be encrypted

A seed will be used to trigger a PRNG. Output from this PRNG is used to extract the sub-key from the master key, and select a range of algorithms from an algorithm library. The master key is a secret file. In the tests, we use 1-255 numbers permutation instead a real key, which produce good results.

Three parameters are generated by a PRNG for a section of sub-plaintext – they are denoted by the tri-values $(P, L, N)$. $P$ represents an offset of a master key. $L$ represents the variable length of the sub-key and sub-plaintext. $N$ represents an index number in the encryption algorithm library. From these parameters, the segmentation of the master key into sub-keys can be determined, as well as the selection of the algorithms from an encryption library for encryption. The algorithms are relatively simple and fast operators like XOR, NOT, etc or their combinations. Hence a wide range of algorithms will be used, the number of which equals to the length of plaintext. This is the property of one time pad.

The components of RASKES is shown in the following figure:

![Figure 1: Components of RASKES](image)
PSEUDO RANDOM NUMBER GENERATOR (PRNG)

A pseudo-random number generator is a program that produces, once its initial state (known as the seed) is chosen, a deterministic and periodic sequence of numbers [6]. Example of PRNG includes the ANSI X9.17 key generation mechanism and the RSAREF 2.0 PRNG [7]. Normally, a PRNG intends to start in an un-guessable state to an attacker, which comes from values collected from physical processes. System implementers and designers will try to ensure that there is sufficient entropy in these inputs. Some good recommendations of resources of randomness could be found in [8][9][10]. Offers cryptanalysis of a number of PRNG.

The PRNG generates a series of predictable sequences of numbers depending on the seed value. In RASKES, these random outputs of PRNG grouped as the encryption parametric tri-values of \((P, L, N)\) for consecutive sub-plain-text encryption/decryption. Each group of \((P, L, N)\) indicates how to section a sub-key and what kind of algorithms to be used for the corresponding sub-plaintext. They have the following conditions:

\[
\begin{align*}
P & \leq N \leq L \leq \text{the size of the full master key (we assume a circular key)} \\
N & \leq \text{the number of columns in the selected encryption algorithm table} \\
L & \leq \text{the number of rows in the selected encryption algorithm table}
\end{align*}
\]

For example, Fig 2 shows the generation of sub-key. This sub-key exists only for a single use for encrypting a selected sub-plain-text. It is generated when the CE (Crypto-engine) gets the parameter of \(P, L, N\), and used only once with the algorithm chosen related to them. Note that operators like NOT, Rotate, ADD... do not need a sub-key.

The sequence of a sub-key may not directly relate to the sequence of a master key. Also sub-keys may overlap; some part of a master key may be used twice or more, while some part of the bytes may not be used at all.

ENCRIPTION ALGORITHM LIBRARY (EAL)

A possible implementation of the EAL may consist of many tables (see Fig 3), which can be publicly stored in some server or privately known only to a closed group of users. Inside the individual tables, there are relatively simple revertible algorithms, like XOR, NOR, ADD...

Instead of using more complicated ones like DES, RSA...simple ones can be used for their speed. On the other hand it does not imply that the encryption data is not secured. Conversely, the level of security is increased because a greater number of algorithms will be used to generate cipher-text. According to the principle of one-time pad, each byte of plaintext will be encrypted by one algorithm.

The algorithms selection is determined by a PRNG. As a PRNG might return a 32-bit value, it will be dedicated up to 8 bits for algorithm selection. We may prefer the items come from the internal state of PRNG. Furthermore, the use of different algorithms will possibly lead to different timing and power usage. [11][12]. We recommended that using a PRNG to fill the algorithm table. When all the algorithms are of equal possibility, we can assume the algorithm table is auto-balanced.
In EAL, a row represents an index number of the EAL; a column represents an algorithm to encrypt one byte of sub-plain-text. For example, choosing table ID1, and index No. 01, maximum 14 bytes of plain-text could be encrypted with the first byte using algorithm A5, the second byte using A3... and so on.

From Fig 3, it can be seen the size of individual algorithm table is different. Before the encryption process, one of the communication parties selects the table’s ID from user interface. The selected ID of encryption table is then transmitted through a secured communication channel to the other communication party. This will be used in decryption process. The output of PRNG also varies based on the ID of algorithm table.

<table>
<thead>
<tr>
<th>LID1</th>
<th>PU</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B</td>
</tr>
<tr>
<td>256</td>
<td>A1</td>
</tr>
<tr>
<td></td>
<td>A2</td>
</tr>
<tr>
<td></td>
<td>A3</td>
</tr>
<tr>
<td></td>
<td>A4</td>
</tr>
<tr>
<td></td>
<td>A5</td>
</tr>
<tr>
<td></td>
<td>A6</td>
</tr>
<tr>
<td>255</td>
<td>A4</td>
</tr>
<tr>
<td></td>
<td>A1</td>
</tr>
<tr>
<td></td>
<td>A2</td>
</tr>
<tr>
<td></td>
<td>A8</td>
</tr>
<tr>
<td></td>
<td>A7</td>
</tr>
<tr>
<td></td>
<td>A1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LID1</th>
<th>PU</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B</td>
</tr>
<tr>
<td>0</td>
<td>A1</td>
</tr>
<tr>
<td></td>
<td>A1</td>
</tr>
<tr>
<td>3</td>
<td>A9</td>
</tr>
<tr>
<td></td>
<td>A5</td>
</tr>
<tr>
<td></td>
<td>A1</td>
</tr>
<tr>
<td></td>
<td>A1</td>
</tr>
<tr>
<td></td>
<td>A2</td>
</tr>
<tr>
<td>0</td>
<td>A8</td>
</tr>
<tr>
<td></td>
<td>A7</td>
</tr>
<tr>
<td></td>
<td>A2</td>
</tr>
<tr>
<td></td>
<td>A4</td>
</tr>
<tr>
<td></td>
<td>A1</td>
</tr>
<tr>
<td>01</td>
<td>A6</td>
</tr>
<tr>
<td></td>
<td>A11</td>
</tr>
<tr>
<td></td>
<td>A4</td>
</tr>
<tr>
<td></td>
<td>A1</td>
</tr>
<tr>
<td></td>
<td>A13</td>
</tr>
<tr>
<td></td>
<td>A12</td>
</tr>
<tr>
<td>00</td>
<td>01</td>
</tr>
<tr>
<td>......</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>14</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LID1</th>
<th>PU</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>B</td>
</tr>
<tr>
<td>0</td>
<td>A9</td>
</tr>
<tr>
<td></td>
<td>A1</td>
</tr>
<tr>
<td></td>
<td>A2</td>
</tr>
<tr>
<td></td>
<td>A8</td>
</tr>
<tr>
<td></td>
<td>A7</td>
</tr>
<tr>
<td></td>
<td>A2</td>
</tr>
<tr>
<td></td>
<td>A4</td>
</tr>
<tr>
<td></td>
<td>A1</td>
</tr>
<tr>
<td></td>
<td>A3</td>
</tr>
<tr>
<td>0</td>
<td>A4</td>
</tr>
<tr>
<td></td>
<td>A1</td>
</tr>
<tr>
<td></td>
<td>A12</td>
</tr>
<tr>
<td></td>
<td>A1</td>
</tr>
<tr>
<td></td>
<td>A6</td>
</tr>
<tr>
<td>00</td>
<td>01</td>
</tr>
<tr>
<td>......</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>21</td>
</tr>
</tbody>
</table>

A1 - Ax: encryption algorithm identifiers
LID1 - LIDx: encryption algorithm library identifiers
PUB: publicly known
PRI: privately known

Figure 3: Public and Private tables in EAL

A plain-text is segmented into blocks of variable length data, which could be 8 byte or a bigger size according to the parameters from PRNG. Those encryption algorithms used are randomly chosen.

**CRYPTO-ENGINE (CE)**

This CE generates a random keypad according to the PRNG tri-values. On the other hand, it stored all the chosen algorithms. When a keypad and algorithms are ready it encrypts the plaintext. The length of a keypad and the number of algorithms used are equal to the length of plaintext. This is the basic principle of One-time pad. When generating a keypad, it calculates its length. PRNG will stop to generate (p, l, n) when a keypad reaches the same length of a plaintext.
DECRYPTION

As we have mentioned before, RASKES is a symmetric key encryption system. The same key is used for encryption and decryption. To decrypt the cipher text, the receiver has to generate the same key value. Therefore, we need to consider how to distribute the key. We recommend using a public key algorithm, when the two parties authenticate each other, they can share the master key.

The seed, master key and the ID number of EAL will be distributed through some secure channel after the communication parties authenticated one other. The EAL could be found in a public known server. Supposing the sender and the receiver know which PRNG is used to generate the encryption tri-values. From the seed, the same PRNG series will be generated; hence the sub-key and random algorithms could be retrieved. The plain-text series could thus be rebuilt.

To decrypt the cipher-text, the parameters have to be exactly the same as those used for encryption. For one PRNG with the same seeding values, the same encryption parametric values can be expected. Tests in the designed software show that the decryption speed is similar to the encryption speed. And the original data was recovered correctly.

SIMULATION RESULTS AND SECURITY CONSIDERATION

RASKES is implemented in a PIII 550 MHz computer with a memory of 128MB using C++. Assuming the mode of operation is there is no cipher feedback. The key value we used is finite of 0-255 number permutations. The algorithms used are all reversible, including:

- XOR
- NOT
- Rotate left 0-7 bits
- Rotate right 0-7 bits
- Reverse bit
- Any combinations of one or two above algorithms

Because RASKES generate a keypad before encryption started, encryption speed is the same no matter what size of an algorithm table is used. Encryption and decryption performance is shown is the following figure. From this figure, the encryption speed is around 11.5Mb/sec, decryption speed is around 12Mb/sec.

![Figure 4: Performance of encryption and decryption](image-url)
Security of RASKES could be considered through the following three factors:

- Sub-key hopping
- Algorithm hopping
- Variable size of encryption block

For the typical symmetric encryption available today, the same key is used for both encryption and decryption. The encryption key used in RASKES comes from hopping within the space of a master key. This master key must be shared or made available among the communication parties. It could be some known files (e.g. system file, HTML page content, a multimedia file, widely used text), or user defined data. One requirement of the master key is that it should be long enough for segmentations. The sub-key used for each block of plaintext is generated based on the outputs of PRNG P and L --- P denotes the offset position from bit 0 position, where as L denotes the segment length. Since the random output of PRNG have good properties, it would be difficult to guess on sequence of the segment a sub-key. The use of different PRNG is an option of the CE functions. In other words, the CE might incorporate multiple PRNG engines. In such a case, the choice of the particular engine must also be prearranged between the principals.

The algorithms used for encryption are selected by the PRNG output N. The number of algorithms used is equal to the number of bytes of data segments from the plaintext. It means that each plaintext segment will be encrypted by different algorithms-sub-key combination. This product will enhance the level of security of RASKES.

RASKES is a block cipher since it operates on blocks of data. However the length of blocks varies, being determined by the output of the PRNG L. The minimum size of one block is one byte, and the maximum size equals to full columns of a selected encryption algorithm table. For example, an algorithm table of 8 columns can be used to encrypt up to variable length of 8 bytes of sub plaintext. This is another factor in increasing the security of encryption.

Any one who wants to break the cipher need to know how the plaintext has been segmented, what encryption algorithms from which library have been used, and how to create the session key from a master key. All of these secrets are hidden in the PRNG. Hence a statistically strong PRNG is needed. On the other hand, the large internal state of EAL could also make exhaustive search extremely challenging. From this point of view, the system has all the advantages of “one time pad”, while the user do not have to worry about reusing algorithms or a master key.

CONCLUSION

In this paper, a new architecture of encryption framework named RASKES was designed and successfully implemented using C++. It is a symmetric key block cipher with variable length of sub-plaintext processing. The random output of a PRNG will enable the extraction of sub keys hopping from a specified algorithm table. The plaintext is then sectioned into variable sub-data segment lengths. This cipher offers a similar level of security as the proved algorithm one-time pad with enhancement. It is recommended to put into commercial to test its strength and weakness.
REFERENCE


A Business Information Infrastructure

V Stagg¹ and M Warren²

¹School of Computing and Mathematics
Deakin University. Australia
Email: vstagg@deakin.edu.au

²School of Computing and Mathematics
Deakin University. Australia
Email: mwarren@deakin.edu.au

ABSTRACT

Information Infrastructures are becoming necessary and vital elements for nations worldwide. Significant efforts are required to provide infrastructure protection, increase cooperation between sectors, and identify points of responsibility. These issues of infrastructure protection, especially from Information Warfare threats, cannot be sufficiently dealt with using the current infrastructure model. By extending the existing model through identification of vertical sectors for a defence-in-depth approach, and the horizontal elements with a defence-by-breadth approach, subsets of a National Information Infrastructure, such as the proposed Business Information Infrastructure, may provide for greater security and protection.

Keywords: Business Information Infrastructure, Information Warfare, Information Security.

INTRODUCTION

Global, National, Critical, and Defensive Information Infrastructures have become necessary and vital elements for nations worldwide. These infrastructures are an eclectic mix of open and closed networks, private and public systems, the Internet and government, military, and civilian organizations (Anderson, 1998; Aberg, 2000). They are important vehicles for the generation of national wealth throughout developed societies; they increasingly influence the power and capability of nations (Westwood, 1996), cause radical changes in international finance and commerce (Cordesman, 2000), and are powerful stimulants to the creation of content, ubiquitous communication, and access to new markets (NRC, 1996).

A problem with many infrastructures is that they are too big, continually growing, regularly reconfigured and reengineered, and lack suitable staff and resources to administer and secure them (Brock Jr, 2000). As the integration of technology into everyday life increases, the reliance on the integrity, availability, and reliability of these infrastructures grows accordingly (Luiijf, 1999). Due to this heterogeneous nature of infrastructures and their involvement in a nation’s economy, another issue of concern is the lack of a significant or focal point of authority for infrastructure control (PCCIP, 1997b). Infrastructure protection is the responsibility of the government, military, private, and public organizations (Waltz, 1998), and must take into account the various departments and agencies involved, along with their mission and responsibility requirements (Cordesman, 2000).
When determining the need for infrastructure protection we need to consider the following issues:

- Threats are more severe than in the past
- Vulnerabilities more common and exploitable than in the past
- Consequences are higher than in the past

Current infrastructure developments focus on top-down approaches, which are often unwieldy, difficult to manage, averse to cooperation, and lacking in coordination. In an effort to improve infrastructure protection, increase cooperation between sectors, and identify points of responsibility (Samson, 2000) this paper presents an approach that considers the vertical and horizontal levels of infrastructure, identifying particular infrastructure subsets, and introduces the concept of a Business Information Infrastructure.

**NATIONAL INFORMATION INFRASTRUCTURE**

The National Information Infrastructure (NII) has been defined as a system of high-speed telecommunications networks, databases, and advanced computer systems that make electronic information widely available and accessible (OMB, 1995). The NII has also been described as an inchoate, multidimensional phenomenon, a turbulent and controversial mix of public policy, corporate strategies, hardware and software that shapes the way consumers and citizens use information and communications (Wilson, 1997).

An NII is considered to be the physical and virtual backbone of an information society (Cobb, 1998). It is an evolving entity comprised of all public and private information services, operating as a complex, dynamic system that together with other NII's forms the Global Information Infrastructure (NRC, 1996). The United States Presidential Critical Infrastructure Protection Commission (PCCIP), created in 1996, identified five sectors of infrastructure elements based on the characteristics of the following industries (PCCIP, 1997a):

- Information and Communications
- Banking and Finance
- Energy, including power, oil, and gas
- Physical Distribution
- Vital Human Services

Many elements within the NII, as well as those used to protect and defend it, come from public and private sectors, particularly Commercial Off The Shelf (COTS) software and hardware (Campen et al., 1996). The growing trend of government and military organizations to procure commercial products, along with the need for system interoperability, will see a greater amalgamation of government, military, and civilian infrastructures (Garigue, 1995).

A number of parallel infrastructures already coexist within the NII and include the Defence Information Infrastructure (DII), whose function is to globally link military functions such as mission support, command and control, and intelligence computers through a variety of methods (JCS, 1996). A Critical Information Infrastructure (CII), also considered as a Minimum Essential Information Infrastructure, considers the essential elements of a nation, and implements special hardening, redundancy, recovery, and other protection mechanisms (Anderson et al., 1999; Nash and Piggott, 1999). Figure 1 shows the current infrastructure level hierarchy.
Numerous problems exist in the protection of NII's. Aside from the obvious technical, legal, and financial aspects involved, there are also numerous misunderstandings between business and government over what protecting the NII entails (Caloyannides, 2000). An interesting dichotomy arises with businesses wishing to avoid and prevent attacks, whilst governments want to detect, trail, and then prosecute the attackers. This raises numerous liability, information sharing, and vulnerability issues that have been plaguing infrastructure protection since day one. The issue of governments becoming increasingly removed from ownership of critical infrastructure elements limits their ability to protect them, requiring sector-by-sector solutions (Willemssen, 2000).

The finance sector has long understood the necessity of preserving customer confidence and the integrity of business information. The awareness of information security, implementation of policy, and protective measures is especially strong within this sector (Mitchell et al., 1999). The concern within other sectors is that many organizations do not yet realise the sheer scale of the steadily growing threats they face. The approaches they take to protective measures are often closed, secretive, and compartmentalised in nature, and do not take into consideration the impact their systems have on other elements of infrastructure (Cordesman, 2000). The consequences of an attack may increase where system redundancy has been degraded due to commercial cost cutting, reduction of maintenance schedules, centralisation of critical nodes, and the use of COTS (Cobb, 1998). The reality of the threats faced can be seen in the rise of computer security incidents reported by CERT (http://www.cert.org) from just six in 1988 to over 15,000 for the first half of 2001!

**INFORMATION WARFARE**

Information Warfare is still a relatively new issue, not clearly understood in the commercial sector, yet more than just hype or a buzzword (Gershmanoff, 2000). Originating from the military sector, a certain amount of disparity exists between the various definitions and concepts of Information Warfare developed amongst various military and defence departments (Gray et al., 1997). Derived from various sources, Information Warfare can be considered as actions taken to affect a competitor’s information, information systems, and information-based processes whilst protecting one’s own information, information systems, and information-based processes. These actions may be directed at an individual, a corporation or multinational body, and may occur during peacetime or conflict between nations or societies (Arquilla and Ronfeldt, 1993; Schwartau, 1994; JCS, 1998).
When considering the Information Warfare threat spectrum to an infrastructure, we need to determine the potential adversaries, their motives, and their objectives. Such adversaries could include nation states, criminals, terrorists, hackers, hacktivists, spies, ideological and cultural adversaries, insiders, and competing organizations (Brand, 2000; Luijff, 2000). By identifying the objectives and motives of attackers, it is possible to qualify the potential effort, skill, and expense the attacker is willing to invest in exploiting a vulnerability (Anderson, 1998).

There are important distinctions between nuisance/hacker attacks and Information Warfare attacks against infrastructures. These include the attacker being able to predict the consequences of the attack, the fact that these consequences will measurably increase the likelihood of the attackers objectives being attained, and that these attack options compare favourably with alternatives that may achieve the same results (Anderson et al., 1999). These distinctions imply an inherently more coordinated, planned, and strategic method is applied with clear objectives and aims in mind. Information Warfare threats to infrastructures are gradually being considered greater than traditional military threats (AGD, 1998).

Attacks against infrastructures are relatively new, shifting the threat focus from low-level attacks on individual, system-level elements to high-level system-wide attacks (Anderson, 1998). These types of network-centric attacks can be considered a version of Information Warfare known as Infrastructure Warfare (Alberts, 1999). A report by the Defense Science Board (DSB, 1996) stressed that to understand the Information Warfare process, and identify Information Warfare attacks, will require a determined effort to collect, consolidate, and synthesize information from various infrastructure elements.

Information Warfare is still a new and evolving issue and presents significant challenges to those responsible for developing policy regarding the protection of the NII (Ryan and Ryan, 1996). In 2000 a Forrester report found that 89% of companies surveyed saw Information Warfare as a possible risk, with 6% saying they had first-hand experience of such an attack (Prince et al., 2000). Whilst organizations may not be able to defend against large-scale attacks against the NII, they are more likely to successfully defend against attacks on smaller more constrained infrastructures.

**A BUSINESS INFORMATION INFRASTRUCTURE**

The NII can be seen as a diverse and eclectic mix of systems, networks, people, and processes that often cut across work-practices, departments, functions, and organizational borders (Braa and Rolland, 2000). As Figure 1 shows, the Critical and Defensive Infrastructures are interconnected and interoperable in such a way that they constitute most of what makes up the NII (AGD, 1998). With the growing trend for organizations, public and private, to integrate and utilise information and communications technologies into their operations, there is a significant rise in the reliance on the dependability and reliability of the NII.

The issues of infrastructure protection, Information Warfare threats, attacks, and responsibilities are becoming harder to deal with for those organizations that are part of, or connected with, the current infrastructure model. Infrastructure protection cannot simply be addressed by compartmentalised solutions that have derived from methods and practices out of touch, and out of date, with today's sophisticated and complex technologies. Whilst each sector, as defined by the PCCIP, has its own requirements for security and protection, there is a certain amount of interplay between each sector, along with a common core component of infrastructure elements (Ware, 1999; Mitre, 2001) seen in Figure 2.
With the growing number of non-critical and non-military elements becoming part of the NII, the “problem area” of Figure 2, additional measures will be required to strengthen and secure the existing model. By defining subsets of the NII, based on the sectors defined by the PCCIP, those elements deemed non-critical can incorporate security measures and mechanisms to integrate into the relevant infrastructure sector. With a focus on the Information and Communications sector, Figure 3 outlines a subset defined as a Business Information Infrastructure (BII).

1 “Non-critical business” includes elements such as medium-to-large businesses, large corporations, and other institutions that may be indirectly related to critical elements of infrastructure, be adversely affected by infrastructure attack, or have significant involvement in information and communications technology.
The three main categories of the BII will be based on the focal elements of Information Warfare: information, information systems, and information-based processes. This will help categorise the infrastructure elements and enable clear and decisive methods of protection based against potential Information Warfare threats. By recognising the important horizontal and vertical relationships that exist within the NII model, along with the interplay that occurs between all sectors (Porter, 1990; Ware, 1999) security can be increased not only in depth, but also by breadth (NATO, 1997; Ackerman, 2001; Kewley and Lowry, 2001).

By identifying the elements that make up the BII we can identify crucial support functions that flow vertically (control and cooperation), horizontally (strategy, structure, and rivalry), or both ways (Viitamo, 2001). The efforts in protecting the horizontal elements can consist of methods, policies, and procedures relevant to that sector; many of these will already be in place. The vertical levels can be strengthened with applicable security measures, such as strong encryption, secure channels, redundancy, and recovery systems for the Information and Communications sector. This mix of a defence-in-depth and defence-by-breadth approach will allow for suitable security procedures to be implemented at a horizontal layer, which can then be strengthened with stronger vertical layer security measures. Of course just adding extra defence mechanisms does not guarantee a safer system, but defence-by-breadth is just as important as defence-in-depth (Kewley and Lowry, 2001).

At the BII level many of the entities involved will have strict rules and procedures in place for information collection, management, distribution, retention, and deletion. These procedures can provide a viable framework for Information Technology Information Sharing and Analysis Centers (ISAC) to work within (USDOC, 2001). A common hurdle to ISAC’s is the unwillingness of organizations to share sensitive information with others (Brock Jr, 2000), especially on a large scale. The BII would be able to filter the information from the horizontal elements to develop statistics and analysis that could then be shared among the vertical sectors. The information would enable organizations to develop a better understanding of the threats facing their particular infrastructures and be better prepared to defend them. This information could be combined with other infrastructure subsets, along with federal resources, to better protect the NII (Willemssen, 2000).

**CONCLUSION**

One of the significant differences between offence and defence is that defence is required to ensure against all threats and vulnerabilities, while a successful offence need only exploit one of these (Anderson et al., 1999). This situation is further exacerbated by the continual growth in performance and power of information and communications technologies, the availability and accessibility of information and tools (Stagg and Warren, 2000), and the relative low costs that enable almost anyone to launch an attack against an infrastructure (Luijff, 1999). On the other hand, the cost to detect, repair, recover, respond, research, and retaliate against such attacks is significantly higher (West-Brown and Kossakowski, 1999).

It is important to realise the growth of infrastructures presents shared risks, which in turn creates shared responsibilities for protection (West-Brown and Kossakowski, 1999). Organizations must work together to safeguard their infrastructure networks, which will further help strengthen the NII. A mass attack on an NII resulting in the total shutdown of systems is not likely without a high level of planning, coordination, skilled personnel, and funds (Cobb, 1997). The possibility of attack on elements of the NII is much more feasible with minimal outlay of technology, funds, and personnel required.

The BII model presented offers an additional layer of security to the NII and incorporates many elements deemed non-critical but inherently part of the NII. The BII also provides an opportunity for improving cooperation and coordination between sectors, as well as the sharing of information. By applying sector-by-sector solutions, along with a defence-in-depth and defence-by-breadth approach to security, the dependability and reliability of the NII can be greatly improved.
REFERENCES


Information Operations – A Swedish View

L. Nicander
Secretary of The Cabinet WG on IO-D/CIP
National Office of IO/CIP-studies
Swedish National Defence College
Email: LarsNicander@csi.com

ABSTRACT

This paper touches upon Swedish views of how to organize traditional domestic responsibilities to better catch up with emerging IT-related threats. This paper stresses the need for developed forms of public-private co-operation. It also discusses new ways of handling crises and conflicts, as well as of enforcing sanctions in the international arena.

Keywords: Information Operations, Information Assurance, Critical Infrastructure Protection

INTRODUCTION

This article will cover three aspects of developments in Sweden concerning Information Warfare (IW) and Information Operations (IO). Firstly, the paper examines how the concept of IW/IO was understood. Secondly, the paper examines how the governmental process developed with studies, proposals, agency comments, cabinet bills and parliamentary decisions. Thirdly, the paper examines the emphasized need for international co-operation.

The personal views expressed in this paper do not necessarily reflect the views of the Swedish Government.

CONCEPT AND DEFINITIONS

The Swedish view takes its start from a top-down, national security perspective, rather than from a bottom-up infosec perspective. This perspective suggests a holistic approach to information operations. It also suggests that the Swedish government view the implications of information operations as an important matter in which they are willing to take an active part.

In its thorough Defence Bill from November 1999 (Swedish Ministry of Defence 1999a), the Cabinet described the matter as follows:

The threat against the information society has become increasingly important at the same time as systems and functions important to the society are becoming more dependent on information technology. The question of society's vulnerability in this respect has a strong bearing on security policy.

The boundary line between information warfare and general information security is by its very nature indistinct. There are, however, some marked differences. The first is a matter of perspective. Information warfare is based on a security policy perspective and embraces more than IT or cybersecurity. The contents and effects of the information (intelligence and psychological operations), viewed as a military instrument or from a strategic/economic viewpoint, are essential components of...
this cross-sector concept. Information security begins with individual computers, networks and firewalls and continues up through the sectors. The highest form of information security, with the associated policy and organisational structures, is generally known as Information Assurance, which constitutes the primary defensive component of information warfare.

The other differences relate to the players concerned. While an information attack focuses on individuals and companies, information warfare has states or state-supported organisations as its focus.

Accordingly, Swedish substantive definitions adhere to the taxonomy defined by the US (JP 3-13, Joint Chiefs of Staff (US), 1998), and later also adopted by NATO, where Information Operations (IO) is the comprehensive term. IO could be offensive or defensive and incorporates more than IT-related matters, for example intelligence, perception management, operational art, etc, within a strategic context. In this Bill the old term Information Warfare still was used, but has since been changed to Information Operations.

Information Assurance (IA) is the IT-related foundation within the term IO. IA could be seen as the highest level for the bottom-up perspective where organisations and policy have been added to the traditional infosec toolbox. Some voices have called IA “infosec with a budget”.

With this top-down perspective and the long-standing Swedish tradition of a Total Defence concept – where all-important functions in society are included in the event of crisis/war - it is more logical to talk about the wider term Defensive Information Operations (IO-D) than just Information Assurance. I am thinking here especially about functions as counter-psyops and counter-deception.

How do governments fully detect information attacks where the use of computer virus, logical bombs and electromagnetic weapons are orchestrated with disinformation on the net as well as with planted morphed video sequences in the TV-newscasts? Anyone who has seen the movies “Forrest Gump” or “Wag the Dog” knows what the new technology can do. For example, if Saddam Hussein planted a morphed video in an Arabic media showing Israelis burning down Mecca, this would of course affect the audiences in a certain direction. People tend to believe what they see.

Many non-Swedes are for example very astonished over the existence of a very tiny agency called The National Board of Psychological Defence. During peacetime this agency just has planning and research functions, and publishes academic reports every year on the interdependence and couplings between people, government and media in different major crises – the Estonia-ferry-disaster, the radioactive fall-out from Chernobyl etc. In the case of a crisis and in wartime, the agency grows and becomes more operational, but still in those situations this is not a “big brother”-agency. The cardinal rule is not to tell or promote any untrue messages. The agency has many media representatives in its peacetime board, and many more in its mobilized organisation.

With this as a background the Swedish government in 1996 decided to establish a Cabinet Working Group (WG). The WG was tasked to develop a greater understanding of the implications of IO/IW and to make sure that the government is properly advised in the matter of IO/IW.

THE PROPOSALS FROM THE CABINET WG ON IW-D

In 1996, the Cabinet appointed a working group within the Cabinet Office to look into threats and protection concerning Information Warfare, but also to give proposals about new forms of responsibilities within the government. A representative from the Ministry of Defence chaired the WG, and the Swedish National Defence College (SNDC) was tasked to support the WG with a secretary and its secretariat. The other eight representatives came from the Ministry of Industry, Trade and Communications, the National Criminal Investigative Department, the Swedish Security Service,
the Armed Forces HQ (Ops and Intel), the National Board of Psychological Defence and two representatives from the Defence Research Establishment.
In June 2000 the Cabinet changed the name and created a new mandate for the “WG on Defensive Information Operations”. The WG also more than doubled its size with many new representatives from other Cabinet Departments (Foreign Affairs, Treasury, Justice) and agencies (Post and Telecom Agency, Defence Radio Institute, the Financial Inspection, the Defence Materiel Administration, the Swedish Agency for Civil Emergency Planning, etc.). Still the chair remains with MoD and the secretariat with NDC.

PROPOSALS

The WG on IW-D has finalised two reports to the Cabinet. The first one came in August 1997 with more general conclusions on the character of IW-methods. It also had some policy recommendations, such as the need for looking at the functionality of the economy in a national security context (Cabinet Working-Group on Defensive Information Warfare, 1997).

The second classified report was sent to the MoD in May 1998, and an unclassified version was published in June the same year (Cabinet Working-Group on Defensive Information Warfare, 1998).
This report focused more on the national management structure concerning IW-D responsibilities. The questions addressed were:

- “Who is in charge?”
- “Who to call in the event of a serious cyber attack?”
- “Who can have the overview to recommend the best allocation of the last tax funds for Information Assurance purposes within the Government?” and
- “Who has the authority to rapidly (weeks/months) reallocate government funding for the purpose of reducing serious vulnerabilities in information systems and networks?”

Report No. 2 was issued with ten distinct proposals.

- A co-ordination group at senior level in the Cabinet Office and Ministries will be created to solve, primarily, IW(IO)-related issues that are of an administrative nature. The group, or parts of it, ought also to be able to constitute a part of a national crisis-handling resource.
- A national IW(IO) co-ordination body will be created as a separate division within ÖCB.
- A GovCERT will be organised under the management of the PTS and with the support of the RPS.
- The establishment of a so-called statistics unit will take place in dialogue with the NSD (The Private Sector’s Security Delegation).
- An obligation to report will be introduced for IT-related incidents within the state administration.
- The mandate of the Swedish Armed Forces with regard to the Communications Security Group for the Total Defence (under the administration of TSA), will be extended also to comprise civilian information systems that are of significance for the Total Defence.
- An active IT-check function for the government administration will be established with the Swedish Armed Forces HQ as a base.
- Constitutional amendments in computer and data-related legislation must be initiated immediately.
- A group for analysis of perception/disinformation methods on Internet should be set up at The National Board of Psychological Defense.
- New forms of co-operation, dissemination, training etc in the area of intelligence will be developed with regard to IW(IO) information.
MANAGEMENT STRUCTURE

The management structure is graphically described in Figure 1.

![Management Structure Diagram]

- **RKP**: National Criminal Investigation Department
- **SÄPO**: Swedish Security Service
- **SPF**: The National Board of Psychological Defence
- **FM/HKV**: The Swedish Armed Forces (Headquarters)
- **TSA**: The National Communications Security Group
- **RRV**: The Swedish National Audit Office
- **FRA**: National Defence Radio Institute
- **OCB**: The Swedish Agency for Civil Emergency Planning
- **PTS**: National Post and Telecom Agency
- **FI**: The Financial Supervisory Authority of Sweden
- **GovCERT**: Government Computer Emergency Response Team

**Figure 1: The Management Structure**

A COMPARISON OF SWEDISH AND THE US IN IO-D/CIP APPROACHES

There are some differences compared with the management model endorsed by the US Government. First is the strong emphasis on the new IO-D semi-independent co-ordinating body within the Swedish Agency for Civil Emergency Planning (OCB). This body is the equivalent to the Critical Infrastructure Assurance Office (CIAO) with its planning responsibilities, but it also comprises the threat and intelligence functions that in the US belong to the National Infrastructure Protection Center. Secondly, the Swedish GovCERT could be seen as a “stripped” NIPC, with just the warning and tracing roles. In the report’s proposal this function has been put under the auspices of the Post- and Telecommunications Agency, due to its legal mandate over civilian networks. Law enforcement officers are detached to the GovCERT. In the US it is the other way round with the NIPC within the FBI.

A significant advantage for Sweden compared to many other countries is the way public-private cooperation can be handled, due to the existence of a one-stop-shop for the government to co-operate with the private sector – The Private Sector’s Security Delegation. The least common nominator in this case for politicians and industrialists to join forces against emerging IT-threats, could be been described in the motto “Sweden should be a safe and secure marketplace!”
This means that in Sweden we have taken a holistic approach. By actively involving a wide spectrum of national and international organisations, we are attempting to solve the IO problem.

THE POLITICAL PROCESS

When the Cabinet in its Defence Bill (Swedish Ministry of Defence, 1999b) in March 1999 presented its view to the Parliament, it direct or indirect approved eight of the ten proposals. The two first issues in the list above – a National Co-ordination body and a Cabinet Co-ordination Group – were forwarded to a special assigned Commissioner on Vulnerabilities and Security in Society for further investigation. The Commissioner was tasked to give recommendations in May 2001 on new cross-sector responsibilities for severe strains in society during peacetime.

The issue of responsibilities is somewhat complex in Sweden due to the constitution with a 350-year-old heritage of small Cabinet Departments and strong, independent agencies. This goes back to the 17th century, when our king Gustavus Adolphus II was out in Europe for long campaigns during the Thirty Years’ War. He wanted a stable government that could run domestic business without his immediate presence. The agencies are formally subordinated only to collective Cabinet decisions (at least five ministers present) - not to the minister concerned or the Cabinet Department. This governmental system – with its strict sector boundaries, great authority for the Director-Generals, weak ministerial authority and no formal interagency co-ordination body - is not so well suited to take care of the new cross-sector threats in the Information Age.

In September 1999 the Defence Commission – comprised of parliamentarians on a MoD-assignment – published a white paper (Swedish Ministry of Defence, 1999c) with proposed guidelines on National Security and Defence for the next five years. This paper addressed IO-issues in the round – from the urgent need for restructured domestic co-operation between joint military and civilian parts of the Total Defence concept, to the need for international co-operation. The white paper concluded that the question of vulnerabilities in Swedish society was “of great importance to security policy”.

In November 1999 MoD presented another bill to the Parliament (Swedish Ministry of Defence, 1999a), which included almost all the recommendations from the Defence Commission. On the need for a GovCERT, the Cabinet developed its view as follows.

In the Cabinet (MoD) Bill 1998/99:74 “Restructured Defence for a Changed World”, the Cabinet has also addressed the establishment of a special Computer Emergency Response Team (CERT), a so-called GovCERT, with the primary task of monitoring the Government’s administrative computer systems. The purpose of the GovCERT is to be able to distinguish between non-systematic amateur attacks on the one hand and expert systematic attacks on the other. Attacks in the first category are generally not national in character and attention is therefore concentrated on the latter category.

This GovCERT is intended to function both as a monitoring centre for normal operations and a source of expert advice in the event of failures or major anomalies in the functioning of the network, as well as performing so-called response functions that include tracing the source of a cyber-attack in (almost) real time. In the longer term it should be possible for bodies with private CERT functions (e.g. telecom operators, Internet providers, banking associations etc.) to conclude collaborative agreements with GovCERT. The Cabinet is at present processing the issue about IT-incident handling. The cyber-revolution is essentially a global phenomenon. Communications, computer systems, the development of new products, etc, all have an international dimension and are directed by the market.

When the standing Committee on Defence within the Parliament (Swedish Parliament, 2000) addressed this November MoD-bill, it stressed these issues further. For example, it urged the Cabinet to act more vigorously to remove bureaucratic departmentalisation and to promote faster schemes for exercises similar to the “US Eligible Receiver 97”.

2nd Australian Information Warfare and Security Conference 2001 Page 186
This means that the need for a bureaucratic change concerning protection against the IO-based threats in Sweden has broad support from the political levels – more than from the bureaucratic levels. The next cross-roads will be in November 2001 and in May 2002, when the Parliament finally have to decide on creating a national co-ordination agency 1 July 2002 integrated with other national Crisis Management mechanisms. This will be a result from two Cabinet bills in September 2001 and March 2002, which aims at encompassing actionable views on the recommendations made both by the special commissioner and from the Defence Commission mentioned above. Those recommendations are in all relevant aspects in line with the proposals from the Cabinet WG.

INTERNATIONAL CO-OPERATION

After the Report No. 2 (Cabinet Working-Group on Defensive Information Warfare, 1998) was presented, the focus for the Cabinet WG on IW-D/IO-D was shifted somewhat from the domestic management dimension to the international dimensions.

NEED FOR REGIMES AND "ROE" FOR LEA TO BE ABLE TO TRACE BACK IN NEAR REAL-TIME

One issue on the defensive side of international co-operation is the need for improving the possibilities of making “trace-backs” in near real time. If an attack on a Swedish information system originates in another country, it could take several days for the subject of the attack, e.g. a telecom operator, to learn more on the whereabouts of the perpetrator. They have to contact the Swedish police, who in turn would make contact with the police in the country from which the attack has come and request assistance from the telecom operators concerned in that country. It is therefore important for Sweden to provide active support for international agreements and regulations designed to facilitate rapid tracing across national borders. In the latter case, the relevant G-8 committee has produced recommendations in this direction and the Council of Europe has also endorsed these.

At the 53rd meeting of the United Nations General Assembly in December 1998, a resolution (UNGA 53/70) proposed by Russia was – after some modifications from US and other countries - unanimously adopted to the effect that the threat to civil information systems, for example from terrorists and criminal groups, should be heeded by the international community and cross-border measures implemented. In the continuing discussion of this topic prior to following year’s General Assembly, the need for bilateral as well as multilateral (UN, Interpol) contacts has emerged.

SMART SANCTIONS?

Is the glass half empty or half full? Is offensive use of the “IO-toolbox” always illegal or unethical? Or with the words of Admiral Ellis, CJTF Noble Anvil in Kosovo 1999: “Properly executed IO could have halved the length of the Campaign.”

International Law is a heritage from the Napoleonic Wars in the 19th century, which, interpreted very strictly, could permit huge bombing raids with many civilian casualties as long as there is a legitimate military target in focus, but may not permit the cutting of a telephone wire!

The political view formed by the Swedish Cabinet in November 1999 (Swedish Ministry of Defence, 1999a) and approved by the Parliament in May 2000 stressed the need for a revision of International Law in this respect.
The use of cyber-weapons to attack information systems does not constitute violence in terms of international law but it may nevertheless contravene international law. At the same time it should be possible to make use of such weapons within the provision of the UN Charter (Article 41) – given an appropriate UN Resolution and consequent legal mandate – in order to uphold sanctions or for other conflict prevention measures even though this has hitherto not happened. A more flexible arsenal of non-violent measures of this type would be in line with traditional Swedish policy in this field.

This means that the need for international co-operation is obvious. First, there are no borders in Cyberspace and governments must be able to cope with criminals and terrorists in cross-border IT-activities. Secondly, here could also be an opportunity to strengthen the international community with new means to enforce “smart sanctions” against rogue states. (See also the article on this theme in Survival, Autumn 2000 by Grove, Goodman and Lukasik)

CONCLUDING REMARKS

We have so far just had a glimpse of all the challenges and opportunities that will affect national security in the Information Age.

The essence of Information Operations is Asymmetrical Warfare, and the thoughts of the Chinese strategist Sun Zu (500 B.C.) have been reinforced in Cyberspace. Aggressors, terrorists, advanced criminals and hackers will always try to exploit societal vulnerabilities at their weakest point. The way most western societies are organised today - with strict boundaries between domestic civil law-enforcement sector on one side, and a military and security-policy oriented sector on the other - is an Achilles Heel in the Information Age. That is why the ultimate challenge, in my view, is to break the bureaucratic “stove-pipes” - both domestically and in the context of international co-operation. The tragedy on 11 September in New York and Washington D.C. will stress this perspective even harder.

The same problem exists in a smaller scale within many military services and organisations, where the word “joint” often is only given “lip service” and where outdated boundaries still persist in the minds of too many officers.

Education and awareness arising on this fundamental issue is therefore a cornerstone in the developing curriculum within the IO/IW-field at The Swedish National Defence College, as it was in the first real advanced curriculum in the US National Defence University in 1995.
REFERENCES

Cabinet Working-Group on Defensive Information Warfare (1997)  
Report No 1 - Measures And Protection Against Information Warfare [On-line]  
www.fhs.mil.se/utb/operativa/opi/ikk_eng.htm

Cabinet Working-Group on Defensive Information Warfare (1998)  
Report No 2 - Measures And Protection Against Information Warfare - a proposal for division of responsibilities etc [On-line]  
www.fhs.mil.se/utb/operativa/opi/ikk_eng.htm


Swedish Ministry of Defence (1999a) The New Defence, Bill to Parliament (99/00:30) [On-line]  
www.fhs.mil.se/utb/operativa/opi/ikk_eng.htm (excerpt, unofficial translation)

www.fhs.mil.se/utb/operativa/opi/ikk_eng.htm (excerpt, unofficial translation)

www.fhs.mil.se/utb/operativa/opi/ikk_eng.htm (excerpt, unofficial translation)

www.fhs.mil.se/utb/operativa/opi/ikk_eng.htm (excerpt, unofficial translation)
The Role of Security Standards in Electronic Business (eB)

J. Steve Fall

School of Management Information Systems,
Edith Cowan University, Perth, Western Australia
Email: s.fall@ecu.edu.au

ABSTRACT

Companies are now very aware of the dangers and costs of security intrusion. Today, there is a plethora of security products on the market. However, security is not ensured simply by the installation of firewalls or intrusion detection software. It has become increasingly clear that IT security is not an issue which products alone will solve. Security measures must extend to all areas of business and awareness should be integrated into a company's internal policy and procedures. Within the electronic business (eB) arena it is also important for companies to obtain some assurance that their business partners' systems are also suitably secure.

This paper examines the contribution that IT security standards, particularly the ISO 17799 security management standard and the CC/ISO 15048 product evaluation standard, can make to providing an organisation with an adequate level of IT security. The paper argues that compliance with either of the two standards alone is unlikely to provide an organisation with a level of security that is appropriate for today's eB environment. The paper concludes that if both standards are used together, within a coherent and well designed IT infrastructure, a suitable level of security is more likely to result.

Keywords: Security Standards, Electronic Business, ISO17799, CC, ISO15048, TOGAF.

INTRODUCTION

The Purpose of this Study and Summary of Conclusions

The purpose of this study is to find preliminary answers the following research questions.

1. What is the scope of IT security within the electronic business (eB) environment?
2. What major international standards address the issue of IT security?
3. Will compliance to any one of these standards provide an organisation, that engages in eB, with an adequate level of IT security?

The study concludes that compliance with either of the major standards investigated (ISO 17799 and CC/ISO 15048) alone is unlikely to provide an organisation with a level of security that is appropriate for today's eB environment. However, if both standards are used together, within a coherent and well designed IT infrastructure, a suitable level of security is more likely to result.
The Methodology Used in this Study

The first activity in the study was to carry out an academic literature search. The second activity was to carry out a practitioner and standards web site 'literature' search. The information resulting from these searches was supplemented by the author’s own ‘tacit’ knowledge. The final activity was to analyse and interpret the material obtained from the earlier stages. The general research techniques and paradigm used for this study can be loosely mapped to Tesch's 'hermeneutic interpretation' (Tesch, 1990) within Burrel and Morgan's 'Interpretive' paradigm (Burrel and Morgan, 1979).

Contents of this Paper

The rest of this paper is composed of three sections followed by the references and appendices. The first section outlines the scope of IT security for eB (electronic business). The second section gives an overview of the ISO 17799 security management standard, together with its weaknesses, followed by an overview of the Common Criteria product security evaluation standard and related schemes. This section also includes a brief explanation of the Open Group Architectural Framework methodology and how it can be relevant to IT security. The last section contain the Conclusions.

SCOPE OF IT SECURITY FOR ELECTRONIC BUSINESS (EB)

Since the late 1990’s a number of practitioner eB (electronic business) models (Lacy, 2000, Delphi Group, 2000) and academic eB models (Prahalad & Ramaswamy, 2000; Venkatraman & Henderson, 1998) have been published that describe how an organisation's eB may evolve. An important common thread running through all these evolutionary models is that network usage will expand both in terms of scope (nature of use and application) and reach (variety and number of users and nodes). This clearly has major implications for security because organisations need to allow external controlled access to some of their information assets whilst protecting others. Additionally, the security vulnerabilities of one’s business partners and one’s network service provider can become your vulnerabilities.

According to Gaskell the classic view of IT security was that 80% of the threat was due to internal personnel but ‘in the realm of ecommerce it can be seen that the largest threat comes from external sources’. (Gaskell, 2001, p.2). Today, within the context of eB security greater attention is being paid to external human threat agents such as financially motivated competitors or criminals, benevolent hackers, malevolent hackers, and 'politically' motivated hacktivists.

Companies are now very aware of the dangers and costs of security intrusion. Today there is a plethora of security products on the market. There are also several well-known security standards including the Common Criteria (ISO/IEC 15408), described later in this paper, that are aimed at assessing the quality of security products. However, security is not ensured simply by the installation of firewalls or intrusion detection software. It has become increasingly clear that IT security is not an issue which products alone will solve. Security measures must extend to all areas of business and should be integrated into a company’s external policy as well as internal policy and procedures. Within the eB arena, it is also important for companies to obtain some assurance that their business partners are also security conscious.
IT SECURITY STANDARDS

In this section the following IT security standards are examined.

- The Common Criteria (CC)
- The OpenGroup Architectural Framework (TOGAF)

ISO 17799 (Part 1)

The ISO/IEC 17799 ‘Information Security Management - Part 1: Code of practice for information security’ standard, was published by the International Standards Organisation (ISO) in December 2000. It is based upon the ‘BS 7799 Part 1, A Code of Practice for Information Security Management’. BS 7799 Parts 1 and 2 (which deals with accreditation) has also already been accepted as a national standard in several countries, including Australia and New Zealand (AS/NZS 4444), Switzerland, Holland, and Sweden.

The security framework provided by the standard is designed to:

- provide common best practice guidance to enable an organisation to implement appropriate information security.
- facilitate inter-company trading, especially using eB, by providing confidence in the security of shared information by providing a means by which businesses will be able to verify that their business partners’ security provisions are adequate and unlikely to be the source of potential security pitfalls.

ISO 17799 Part 1 is a very useful tool for businesses to assess their own security. However, it is less useful for verifying that business partners’ security provisions are adequate. This weakness could be overcome if Part 2 of the standard, which deals with the external accreditation of organisations claiming to have implemented the Part 1 guidelines, gets implemented.

ISO 17799 Part 1 is organised into ten major sections, each covering a different topic or area:

- Security policy
- Security organization
- Assets classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- System Access control
- Systems development and maintenance
- Business Continuity management
- Compliance

In the UK (and other countries that have already implemented Part 2 as a national standard) BS 7799 Part 2 provides a process in which a company can have itself evaluated or audited against the control measures described in Part 1. If the company passes the audit it gets a Certificate of Compliance, valid for 3 years. This certificate then certifies that the company conforms to the level of information security prescribed by BS 7799 Part 1.
It is reported that companies who have successfully gone through this certification process, are now using their BS 7799 Certificate of Compliance to demand information security assurances from their eB partners on the grounds that:

"I had my information security evaluated, and I can prove that I conform to the BS 7799 baseline. Before I allow you into my IT systems, I demand at least the same level of information security from you, which you must prove by getting a BS 7799 Certificate of Compliance yourself."

(Von Solms, 2000, p. 618)

WEAKNESSES OF ISO 17799

ISO 17799 has been criticised for specifying its recommended controls at a conceptual level instead of at a more detailed technical level. It has also been criticised on the grounds that the controls it does include are insufficiently comprehensive for contemporary eB (Gaskell, 2001).

Four exemplars of Gaskell’s specific criticisms, aimed at the Australian version of the standard – AS/NZS4444, follow:

1. **System Acceptance**
   Section 8.2.2 (System Acceptance) presents some criteria for the acceptance of new products or systems. … This section could be enhanced by identifying the benefit of third party evaluation of a product’s security claims or by defining standards requirements for the development process.

2. **Electronic Commerce**
   Specifically section 8.7.3 on ecommerce security does not specify any control options. It just raises 9 questions (sections 8.7.3.a-i). This section does refer the reader to Section 9.4.7 which discusses network access control. Section 9.4.7 does not say much besides that network access control will be required. … It is clear that AS/NZS4444 cannot provide assurance to consumers or clients of a ecommerce organisation that the client’s data is adequately protected. Neither can it assure information is protected to a certain level of technical quality.

3. **Quality of Cryptography**
   The most important aspect of secure key generation is that the cryptographic keys are unpredictable. … Section 10.3.5.1 of part 1 of the standard deals with “Key Management”. It does not mention randomness in the discussion on key generation. The location, seeding and pseudo random number algorithms are key parts of the cryptographic mechanisms and security of ecommerce.

4. **Authentication Quality**
   A major area of concern with AS/NZS4444 is its handling of user authentication. Section 9.2.3 of part 1 directly addresses passwords, but passwords are only one form of authentication – albeit a very common one… Elsewhere the standard does acknowledge that biometrics and token based systems are available – but that is all it does acknowledge. There are no requirements for the quality or resilience of authentication mechanisms, other than “risk assessment”.

(Gaskell, 2001, p.4)
Gaskell points out that an initial motive for the development of AS/NZS4444 (BS7799) was that certification of good security practices would facilitate the safe inter-connection of systems for organisations involved in information sharing. He goes on to say that although the standard requires that the controls used by an organisation are ‘appropriate’ for that organisation’s needs the standard does not define the term ‘appropriate’. Additionally he points out that what may be appropriate for one organisation may not be appropriate for other organisations to whom they may be interconnecting.

This is one significant reason that AS/NZS4444 is not appropriate for ecommerce security. The term “appropriate” is not defined. This is a similar problem to defining “secure”, as secure is not a binary condition.

(Gaskell, 2001) (p. 3)

Gaskell does concede that AS/NZS4444 can be protected from criticism by its reliance on a risk assessment for any situation where the control measures in its catalogue are insufficient but points out that thorough risk assessments are quite expensive and that “a standard is typically intended to reduce costs by defining the acceptable specifications with out resort to expensive analysis”.

However, although these criticisms are justified, it should be born in mind that ISO 17799 is basically a security management standard as opposed to a technical standard. The standard is better viewed as aiming to prescribe what needs to be done not exactly how it should be done.

All of the above weaknesses of the standard can be overcome if it is supplemented by the procurement of appropriately certified CC/ISO 15408 products and systems within and a well designed IT architecture as described in the following sections of this paper.

THE COMMON CRITERIA (CC)/ ISO/IEC 15408

The CC is an IT product and systems evaluation standard which has was also adopted and published, in December 1999, as the multi-part ISO/IEC 15408 standard ‘Information technology - Security techniques - Evaluation criteria for IT’ (ISO/IEC/15408-1, 1999). The standard covers how the security requirements of IT products and systems should be determined, specified and tested so that they can be certified as meeting defined security levels.

Prior to 1999 the two most widely internationally accepted criteria used in security evaluation of IT products were the American TCSEC (Trusted Computer System Evaluation Criteria) and European ITSEC (Information Technology Security Evaluation Criteria) standards. The CC was the result of combined efforts of the American and European standards authorities to align and combine TCSEC and ITSEC.

Section 2 of the CC (currently version 2.1) catalogues the functional descriptions of the security requirements of a variety of product classes and their constituent product families and components. Classes include systems such as DBMS, firewalls, operating systems and PC access control systems that each have their own groups, or families, of security requirements (e.g. user identification and authentication). Section 3 of the CC uses these different types of functional security requirement to catalogue ‘Protection Profiles’ (or PP’s) which can be used as a generic basis for the evaluation of different types of products and systems. A protection profile is an implementation-independent statement of security requirements for a family of IT security products. The protection profile for RDBMSs contains requirements for Discretionary Access Control, Identification and Authentication, Object Reuse, Secure Data Exchange, and Audit and Accountability. (IACS, 2001, p. 32). When evaluating a specific product (or Target of Evaluation in CC terminology) each protection profile component can be translated to a number of ‘Security Targets’ (ST’s) which, taken together, create the specification of the security requirements to be used as the basis for the evaluation for that particular
In practice, a security target is a document that specifies the security functionality of a product and the assurance level against which it is evaluated as well as a description of the environment in which it will operate. Product evaluators are required to report upon how well, and to what level, the products they evaluate meet these specific security targets.

The CC also provides a rating system so that products and systems can be rated according to a set of assurance levels, called ‘Evaluation Assurance Levels’. These EAL’s range from EAL0 to EAL7, with EAL7 being the highest level. The CC’s EAL range has been designed to be roughly equivalent to the older US TCSEC and European ITSEC rating scales as shown in Table 1 below.

<table>
<thead>
<tr>
<th>Common Criteria</th>
<th>EAL1</th>
<th>EAL2</th>
<th>EAL3</th>
<th>EAL4</th>
<th>EAL5</th>
<th>EAL6</th>
<th>EAL7</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITSEC</td>
<td></td>
<td>E1</td>
<td>E2</td>
<td>E3</td>
<td>E4</td>
<td>E5</td>
<td>E6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>E7</td>
</tr>
</tbody>
</table>

Table 1: Equivalence of ITSEC and CC Quality Assurance Rating Levels
Adapted from (IACS, 2001, p. 6)

Each jurisdiction normally has its own certification authority and/or programme. For example, Australia has its Australian Information Security Evaluation Programme which was set up by the Defence Signals Directorate in 1995 (DSD, 2001). Other national authorities and programmes include the National Information Assurance Partnership in the US (NIAP, 2001), the Infosec Assurance and Certification Services programme run by the Communications-Electronics Security Group in the UK (IACS, 2001). There are similar schemes in Canada (CSE, 2001), France (SGDN, 2001), and Germany (BSI, 2001) and several other countries. The national certification authority normally delegates the formal product evaluation to independent testing laboratories appointed by the authority. These independent testing laboratories normally have to meet rigorous security and ISO/IEC 17025 quality standards.

Product certificates are awarded following extensive testing of the product’s IT security features to ensure that those features meet an agreed security target (ST). Results of a successful evaluation are published in a Certification Report (CR). This normally contains additional information and advice on how the certified product should be used and any restrictions that may apply in its configuration or use on specific platforms. Security targets and certification reports are available from the developers and, in can be downloaded from certification authorities’ web sites. (DSD, 2001; IACS, 2001).

However, prospective purchasers of certified products need to examine both the security targets and the certification reports in order to ensure that the product meets their specific security requirements. Assuming that organisations actually do determine their requirements and compare them to the security target and certification reports then procurement of appropriately CC certified products and systems would overcome all of ‘weaknesses’ of ISO 17799 identified in the preceding section – except for the problem of determining what an appropriate level is!

In summary, the CC provides a basis for evaluation of security properties of IT products and systems. The CC permits comparability between the results of independent security evaluations by providing a common set of requirements for the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. The evaluation process establishes a level of confidence that the security functions of such products and systems and the assurance measures applied to them meet these requirements.

The CC provides benefits to both developers/vendors and to consumers. For developers/vendors they provide a standardised set of product security requirements to follow in designing and building a product. CC compliance also helps vendors sell their products! Developers whose products are certified against the CC enjoy the benefits of an internationally recognised Certificate as most national...
certification authorities have mutual agreements whereby they accept each other’s certifications. For consumers, CC evaluations and certification helps them determine whether the product meets their security requirements or, at least, will allow them to know what their risks are.

THE OPEN GROUP ARCHITECTURAL FRAMEWORK (TOGAF)

TOGAF is not a ‘security standard’ as such. It is a methodology and supporting tools for defining an open IT architecture that includes the architecture’s IT security services. It is described in a collection of electronic documents and online databases published by The Open Group and available on its public web server (The Open Group, 2000). The development of TOGAF started in 1995 and was originally based on the Technical Architecture Framework for Information Management (TAFIM), developed by the US Department of Defense.

TOGAF consists of two main parts:

1. The Architecture Development Method, is a seven-phase methodology designed to allow organisations to derive an organisation-specific IT architecture that addresses their specific business requirements.

2. The Foundation Architecture is an architecture of generic services and functions that provides a generic foundation on which more specific architectures and architectural components can be built.

The Architectural Development Method (ADM) first provides a method of obtaining information about the benefits and constraints of the existing implementation, together with requirements for change. It then provides a way of combining these two to create a 'target architecture' (or set of architectures).

The TOGAF Foundation Architecture, which is a generic architecture, is used as a template in the third of the TOGAF ADM phases- Create Target Architecture. The output from this phase is a specific target architecture that meets the business requirements of the organisation. The Foundation Architecture has two main components:

- the Technical Reference Model and
- the Standards Information Base.

The Technical Reference Model can be used to help determine the architectural building blocks that will be required in the target architecture. The Standards Information Base can then be used to define the specific services and components required in the products that will need to be purchased in order to populate or implement the developed target architecture.
Fig. 1 shows a diagrammatic representation of the model and taxonomy of generic services provided by the TOGAF Technical Reference Model.

![Diagram of TOGAF's Technical Reference Model and taxonomy of generic platform services](image)

**Figure 1: TOGAF's Technical Reference Model and taxonomy of generic platform services**

(Adapted from The Open Group, 2000)

The Technical Reference Model identifies a set of services for each general service category. For example, the Technical Reference Model’s ‘Security Services’ are composed of the following nine services.

1. Identification and authentication services
2. System entry control services
3. Audit services
4. Access control services
5. Non-repudiation services
6. Security management services
7. Trusted recovery services
8. Encryption services
9. Trusted communication services

Each service can then be related to an on-line Standards Information Base (SIB) entry. The SIB is a (dynamic) database of industry standards for populating a target architecture. The SIB provides the technical architect with a set of tools for defining the standards that a target ITA will prescribe, and for checking the availability in the market place of products guaranteed to conform to those standards.

It is important to note that the 'Qualities' area in the diagram indicates that the architect also needs to identify the quality of service level (QoS) the organisation requires for each required service. Different architectural components may need to provide different QoS and from a security perspective different levels of security service may need to be provided for different architectural building blocks, applications and other assets. If the organisation were to use CC evaluated products the required QoS could be specified as a particular CC Evaluation Assurance Level (EAL).
Although this approach does not provide an automatic answer to what the “appropriate level” of security is for a particular asset in a particular organisation it does provide guidelines on how to go about answering the question. Despite Gaskell’s previously cited assertion that “a standard is typically intended to reduce costs by defining the acceptable specifications without resort to expensive analysis” it is unlikely that any security standard or methodology will be able to identify a universally appropriate (and cost-justifiable) level of security. For most, if not all, organisations some type of risk assessment will be required.

**CONCLUSIONS**

This paper attempts to demonstrate that compliance to either a product technical evaluation standard (the CC or ISO 15408) or a security management framework standard (ISO 17799) alone is unlikely to provide an organisation with a level of security that is appropriate for today’s e-B environment. In this concluding section we will go on to argue, by means of a prison service analogy, that if both standards are used within a coherent and well designed IT infrastructure a suitable level of security is much more likely to result.

**The Need for Product Certification Standards**

It is clear that just purchasing IT products that have CC security certifications will not provide an organisation with an adequate level of IT security any more than purchasing secure locks and secure cell doors that do not fit together will create a secure prison.

**The Need for a Coherent IT Architecture**

If the organisation first creates a well designed and coherent IT architecture, which specifies the quality of service required from each security building block, it can then procure appropriate security products to populate that architecture in an integrated and coherent manner. From an architectural and security viewpoint products that meet BOTH the architectural requirements AND possess the appropriate CC Evaluation Assurance Level certifications can be deemed appropriate. This is analogous to constructing a secure prison building.

**The Need for an Overall Security Policy and Procedure Framework**

Even if an organisation creates a coherent and secure IT infrastructure and populates it with certified products and systems it does not guarantee that its IT assets and information assets will be suitably secure any more than having a well designed and constructed prison will guarantee that prisoners cannot escape.

The IT applications must make appropriate use of the secure IT infrastructure and both must be properly used, managed and controlled in order protect the organisation’s IT assets and information assets.

Analogously, a well-designed and constructed prison must be properly managed and run in order to provide an appropriate level of security. The architecture of the prison or quality of the locks on the cell doors will have little affect on the overall security of the prison if the warders do not know how to, or cannot be bothered, to use them properly. The prison service needs rules and the inmates, visitors and staff need to know what these rules are and why they exist. Also, compliance with the rules must be enforced.
The prison service analogy captures another very important similarity between IT security in the business world and security in the civic world - i.e. 'politics' plays a critical role in the success or failure of both. In order to succeed, IT security must reflect the needs of the organisation AND senior management must be persuaded that it does so. It is unlikely that any significant corporate IT security initiatives would successfully emerge without appropriate top management encouragement and backing.

Formal IT governance practices are therefore required. The purposes of these practices is to ensure that the senior management of the organisation exercise effective control of, and responsibility for, all aspects of the IT operation. However, it is becoming critical for organisations, particularly those that are becoming increasingly dependent on IT, to include an IT security strategy as a central pillar of their overall IT governance strategy. It is equally important that the security strategy must be implemented by specific security policies and procedures that must be regularly audited for both compliance and continuing appropriateness.

Compliance with ISO 17799 will go a long way to providing the required policy, governance and procedural security framework.

In summary, effective and appropriate IT security depends upon:

- sound security policies that are translated into
- well designed organisational and IS/IT architectures that are subsequently populated with
- products, procedures and people that are fit for their purpose

AND

- regular compliance, effectiveness and appropriateness audits.

Adherence to any single standard is unlikely to provide all of these.

REFERENCES


Miles to go before Secure Online Shopping: Certification Authorities and Australian Retailers

Girija Krishnaswamy¹ and Dora Marinova²

¹ School of Management Information Systems
Edith Cowan University, Australia,
E-mail: g.krishnaswamy@ecu.edu.au;

² Institute of Sustainability and Technology Policy
Murdoch University, Australia,
E-mail: marinova@central.murdoch.edu.au

ABSTRACT

Security concerns have been pointed out as one of the most significant barriers for the business aspects of the diffusion of internet technologies and e-commerce in particular. Trusted third party Certification Authorities (CAs) can play a major role in creating an environment of trust. They provide the underlying infrastructure for digital signatures and provide authentication, message integrity and non-repudiation security measures. This study looks at the role played by CAs in the Australian retail sector. The methodology used here is an evaluation of web sites of Australian retailers linked to the yellow pages (www.yellowpages.com.au) of capital cities in Australia. The findings reveal the extent of use of CAs by Australian retailers in instilling consumer confidence in e-commerce payment systems.

Keywords: Electronic Commerce, Authentication, Certification Authorities

INTRODUCTION

Of the several components involved in e-commerce transactions, security is of prime concern for both businesses and consumers. While the protection of the credit card information transmitted electronically is of concern to the consumers, the liabilities involved and the reputation of the business in the event of transaction particulars being stolen and misused by someone is the concern of those receiving orders on the net. In other words, the diffusion of electronic business primarily depends on securing electronic transactions. This is all the more relevant in a volatile economy exposed to LPG (liberalization, privatization and globalization) where even security providing businesses like insurance (as in the case of HIH), and communication business (for example, One Tel) crumble down, spreading the seeds of insecurity in the community. Insecurity on the internet is further augmented by the sabotage of what is perceived to be secure sites like Microsoft or US federal sites.

Electronic commerce could broadly be categorized into B2B (business to business), B2G (business to government) and B2C (business to customers). Since the volume of transactions involved in B2C and the number and the range of players involved are more than that of the other two categories, and public at large are exposed to risk in this segment, attention is focussed here on security provisions provided in B2C web sites in the Australian context. This study looks into the extent of adoption of security technologies by web sites operated in the com.au domain by the retailers and the interregional and sectoral differences in adoption of security provisions. At the same time, evidence will also be presented on the initiatives of the federal government in creating secure environments for B2B commerce within the Commonwealth.
RISKS IN E-COMMERCE

In order to understand the technological solutions to the risks inherent in e-commerce, we ought to look into the risks involved and the security concerns documented. In the interest of both businesses and consumers, technological solutions for risk minimization are highly essential.

While e-commerce risks are varied, insecurity revolves mostly around data - unauthorized disclosure and data alteration. During the course of transmission of unencrypted data, hackers could intercept the transmission to obtain consumer's sensitive information. This data on user names, credit card numbers and payment particulars could all be altered en route. Spoofing and unauthorized actions are other major vulnerabilities to which businesses are exposed in their web existence. The low cost of website creation and the ease of copying web pages make it easy to create illegitimate sites that appears to have originated from established businesses.

The general security concerns centre around the perceived risks described above. Authentication, through which consumers would be able to assure themselves that they are in fact doing business with the right organization that they intend to do business with, will eliminate the risk of spoofing. To avoid the risk of unauthorized disclosure, the confidentiality of the sensitive consumer information, including transaction data must be kept private and secure. The communication between the consumer and the merchant in transit, need to be protected from alteration by third parties, through data integrity. Another concern of both business and the consumer is the chance of the other party denying the transacted communication. For an excellent discussion on e-commerce risks, see Fink (1998).

Thus the standards for ensuring confidence in e-commerce transactions from a practical, legal and technological perspective is to ensure trust among the business and community at large. The confidence that their transactions are only with the intended party, they will be protected in transit, the other party would be legally binding, they will have financial recourse should something go wrong, would ensure in the smooth transition of commerce to the internet.

SECURE TECHNOLOGIES

The solutions for risks posed by technology come from technology itself. A broad understanding of electronic payment systems and the state of art of security enabling technologies would help us map the role of Certification Authorities (CAs) in Australia.

E-commerce systems are founded on electronic payment systems. Broadly defined, electronic payment is a financial exchange that takes place online between buyers and sellers (Commonwealth of Australia, 2000a). Some of the recent trends in both the established and the emerging electronic payment systems are Smart cards, SSL and TLS, SET, Financial EDI, Cybercash, Electronic coins and Micro-payments. However, credit cards are being used increasingly in B2C e-commerce considering its popularity in brick and mortar shopping.

As early as in 1994, Netscape identified the need for ensuring security of transactions on the net. Secure Sockets Layer (SSL), the protocol developed by Netscape enables a web browser and a web server to communicate securely. SSL is the universal standard for authenticating web sites to web browser users and for encrypting communications between browser users and web servers. This protocol requires the web server to have a digital certificate installed on it in order for an SSL connection to be made. SSL is built into all major browsers and hence businesses by installing digital certificates or Server IDs enable SSL capabilities to implement server authentication, client authentication, and data encryption. It relies on a web of trust created by a Public Key Infrastructure (PKI) which in itself is a system of digital certificates, certification authorities, and other registration authorities that verify and authenticate the validity of the parties involved in an e-commerce transaction. Whatever the methods or technologies are used to achieve authentication and security of transactions, a crucial factor is trust. Cryptography solves communication security problems, but
creates key management problems. PKI streamlines key management, but creates trust management problems (Josang, et al, 2000).

Digital Certificates for the web site or Server IDs, are the electronic equivalents of a business license. Server IDs can be issued by a trusted third party, called a CA. Installed on the web server of the business, a server ID enables the consumers to verify the site's authenticity and to securely communicate with it. A server ID assures consumers of the web site's legitimacy and ensures that confidential information such as credit card numbers transmitted online is secure.

Binding online contracts between businesses and consumers can be accomplished by the use of public key cryptography to create a digital signature which is a digital code that can be attached to an electronically transmitted message to uniquely identify the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. To be effective, digital signatures must be unforgeable. Asymmetric encryption techniques use two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. They are extremely secure and relatively simple to use. The difficulty with public-key systems is that one need to know the recipient's public key to encrypt a message for him or her. One would either verify the key fingerprint directly with that person, or by checking the key in a certificate issued by a trusted CA. When decoding a digital certificate, the components of the certificate and the public key would be revealed. Only the holder of a private key could decode a message someone else had encrypted with the corresponding public key. Also a user could sign a message with a private key, and the signature could only be verified with the corresponding public key. This two-way mechanism allows authentication of an individual or an organization, non-repudiation of messages and secure data transmission.

THE ROLE OF CAS

The CA is a trusted third-party organization or company that issues digital certificates to create digital signatures and public-private key pairs. A digital certificate is a general term for a signed document containing two critical pieces of information about the entity, whether it is a business or a consumer. In the case of a business, the first piece of information is the "Distinguished Name", which is a set of values that describes the country, state or province, city or town, organization, division within that organization and the web server domain name. The second piece of information is the "Public Key".

When consumers connect to a secure web server, they are asking the server to authenticate itself. This authentication is a process involving public keys, private keys and a digital certificate. The digital certificate tells the consumer that an independent third party has verified that the server belongs to the business it claims to belong to. A valid certificate means that the consumer can have confidence that he/she is sending sensitive personal information to the right place.

The role of the CA in this process is to guarantee that the individual or the organisation granted the unique certificate is, in fact, who the individual or the organisation claims to be. The CAs are a critical component in e-commerce because they provide a way of verifying the reliability of the electronic communication and guarantee the identity of the parties exchanging information.
ADOPTION OF INTERNET TECHNOLOGIES BY AUSTRALIAN RETAILERS

In November 1999, Australian Centre for Retail Studies, Monash University, came out with a report on e-commerce in retailing based on a large-scale survey of the Australian retail industry. The use of and perspectives of Australian retailers on e-commerce were analyzed and detailed in this report (Monash University, 1999). Of the percentage of retailers identifying e-commerce as #1 or #2 agenda item in the survey, retailers in photography and related aspects came out first (25%), followed by liquor (19.0%). The retailers involved in books and news, though only 8.3%, was more than the average positive response of 6.7%.

After more than one and a half years of publication of the report, it would be fascinating to analyze the nature and extent of adoption of internet technologies among Australian retailers in a few major sectors. Retailers in Australia like elsewhere, have the option either to set up a site on their own or link themselves to virtual shopping malls like http://au.store.yahoo.com. When the retailers set up a shop with shopping malls, the malls provide security. However, when they set up a web site on their own, they have to take care of all aspects of the web sites, including that of security. Since the shopping malls are a category by itself, we decided to focus our enquiry into the nature and extent of internet adoption and the secure transactions provisions provided for, in the retailer's web sites. To understand how the existing brick and mortar retailers are adopting internet technologies, we narrowed down our enquiry to Australian retailers in 4 major products – photographic equipments, books, compact discs and liquor stores.

The http://www.yellowpages.com.au/, the internet yellow pages published on the net by Pacific Access has categories of retailers, searchable state-wise. Though primarily intended to furnish telephone numbers and addresses, the site also provides links to web sites of the retailers. It was assumed that the retailers having web presence would advertise their sites through yellow pages, despite the fact that not all retailers with web sites would use this facility. While the search was essentially focused on yellow pages, we cross checked category entries and searched for random sites both in www.au.yahoo.com and its Australian City links. We found that there are very few additional entries of e-retailers from the yahoo results. The following table gives the number of retailers across different regions over different retail categories. It also provides the number of retailers with web presence and online secure transactions.

### Photographic Equipment & Suppliers - Retail & Repairs

<table>
<thead>
<tr>
<th>State</th>
<th>Total Retailers</th>
<th>Web presence (% of retailers)</th>
<th>Online transactions (% of web presence)</th>
<th>Secure transactions (% of online transactions)</th>
<th>Dead links (% of web presence)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT</td>
<td>9</td>
<td>2 (22%)</td>
<td>1 (50%)</td>
<td>1 (100%)</td>
<td>-</td>
</tr>
<tr>
<td>NSW</td>
<td>311</td>
<td>8 (3%)</td>
<td>2 (25%)</td>
<td>1 (50%)</td>
<td>2 (25%)</td>
</tr>
<tr>
<td>NT</td>
<td>16</td>
<td>1 (6%)</td>
<td>1 (100%)</td>
<td>1 (100%)</td>
<td>-</td>
</tr>
<tr>
<td>QLD</td>
<td>154</td>
<td>3 (2%)</td>
<td>1 (34%)</td>
<td>1 (100%)</td>
<td>-</td>
</tr>
<tr>
<td>SA</td>
<td>44</td>
<td>3 (7%)</td>
<td>2 (67%)</td>
<td>2 (100%)</td>
<td>-</td>
</tr>
<tr>
<td>TAS</td>
<td>22</td>
<td>1 (5%)</td>
<td>1 (100%)</td>
<td>1 (100%)</td>
<td>-</td>
</tr>
<tr>
<td>VIC</td>
<td>242</td>
<td>5 (2%)</td>
<td>1 (20%)</td>
<td>1 (100%)</td>
<td>-</td>
</tr>
<tr>
<td>WA</td>
<td>89</td>
<td>5 (6%)</td>
<td>2 (40%)</td>
<td>2 (100%)</td>
<td>-</td>
</tr>
<tr>
<td>Total</td>
<td>887</td>
<td>28 (3%)</td>
<td>11 (39%)</td>
<td>10 (90%)</td>
<td>2 (7%)</td>
</tr>
<tr>
<td>Books - Retailers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total retailers</td>
<td>Web presence (% of retailers)</td>
<td>Online transactions (% of web presence)</td>
<td>Secure transactions (% of online transactions)</td>
<td>Dead links (% of web presence)</td>
<td></td>
</tr>
<tr>
<td>ACT</td>
<td>68</td>
<td>3 (4%)</td>
<td>1 (34%)</td>
<td>1 (100%)</td>
<td>1 (34%)</td>
</tr>
<tr>
<td>NSW</td>
<td>903</td>
<td>10 (1%)</td>
<td>6 (60%)</td>
<td>5 (84%)</td>
<td>3 (30%)</td>
</tr>
<tr>
<td>NT</td>
<td>29</td>
<td>2 (6%)</td>
<td>1 (50%)</td>
<td>-</td>
<td>1 (50%)</td>
</tr>
<tr>
<td>QLD</td>
<td>418</td>
<td>5 (1%)</td>
<td>3 (60%)</td>
<td>1 (34%)</td>
<td>1 (20%)</td>
</tr>
<tr>
<td>SA</td>
<td>172</td>
<td>2 (1%)</td>
<td>1 (50%)</td>
<td>1 (100%)</td>
<td>1 (50%)</td>
</tr>
<tr>
<td>TAS</td>
<td>72</td>
<td>4 (6%)</td>
<td>1 (25%)</td>
<td>1 (100%)</td>
<td>1 (25%)</td>
</tr>
<tr>
<td>VIC</td>
<td>612</td>
<td>9 (1%)</td>
<td>3 (34%)</td>
<td>2 (67%)</td>
<td>-</td>
</tr>
<tr>
<td>WA</td>
<td>192</td>
<td>6 (3%)</td>
<td>1 (17%)</td>
<td>-</td>
<td>2 (34%)</td>
</tr>
<tr>
<td>Total</td>
<td>2466</td>
<td>41 (2%)</td>
<td>17 (41%)</td>
<td>11 (65%)</td>
<td>10 (24%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compact Discs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total retailers</td>
</tr>
<tr>
<td>ACT</td>
</tr>
<tr>
<td>NSW</td>
</tr>
<tr>
<td>NT</td>
</tr>
<tr>
<td>SA</td>
</tr>
<tr>
<td>TAS</td>
</tr>
<tr>
<td>VIC</td>
</tr>
<tr>
<td>WA</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Liquor Stores - retail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total retailers</td>
</tr>
<tr>
<td>ACT</td>
</tr>
<tr>
<td>NSW</td>
</tr>
<tr>
<td>NT</td>
</tr>
<tr>
<td>QLD</td>
</tr>
<tr>
<td>SA</td>
</tr>
<tr>
<td>VIC</td>
</tr>
<tr>
<td>WA</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

Table 1: Internet presence of Australian retailers for selected industries, by State, as at 13 June 2001
From Table 1 above, it is obvious that the adoption of internet technologies by the Australian retailers having physical retail stores is negligibly low, namely 3% and less. Similar results were found in a study by Krishnaswamy (2000). Even when the retailers have set up web sites, they are more intended to be brochure sites, with some sites with mail order and email order provisions. Of the sites with real time online transactions (which in itself are very few), most of the sites have SSL technologies to ensure confidentiality and safe transmission of private data. There are very few sites with certification authority logos displayed on their sites, despite the projection that "retailing is likely to be impacted by e-commerce more than most other sectors of the economy because of the position which retailers occupy as the interface between product suppliers and end customers" (Monash University, 1999). Though security-enabling technologies are available, businesses are adopting them slowly. Only a detailed analysis of the online retailers listed in different search engines would reveal the extent of adoption of Internet technologies and the role of CAs.

DISCUSSION AND CONCLUSION

What would be the underlying factors for the low adoption of online certification by the Australian retailers? Could this be because the focus is more on B2B and B2G segments? For example, in May 2000, Commonwealth of Australia published a best practice model for business for building consumer sovereignty in electronic commerce. The model provides guidance to industry and consumers on the elements of an effective self-regulatory framework. While adoption of the model would help to ensure that consumers are adequately protected and have confidence in making online transactions, throughout the document, the federal government is reluctant to spell out the role of certification authorities (Commonwealth of Australia, 2000b). There seems to a priority in government policy towards B2B as is reflected in the Ministerial foreword to E-commerce Security when it is 'clear' for the Minister "that B2B e-commerce is already substantial, and is likely to grow exponentially in the next few years, dwarfing business to consumer e-commerce" (emphasis added). A review of the Australian B2B e-commerce initiatives within the Commonwealth gives us a holistic perspective on security concerns. We shall support our argument with a few government initiatives.

Gatekeeper is the Commonwealth Government's strategy for the issue and management of digital certificates. Gatekeeper, under the Office of the Government Information Technology (OGIT) incorporates a rigorous accreditation process, which ensures that service providers comply with and maintain appropriate Commonwealth policies and practices. Accreditation criteria include privacy and security, and it ensures interoperability between accredited service providers (Commonwealth of Australia, 1998). To date, the Australian Taxation Office, Baltimore Certificates Australia Pty Ltd and the Health eSignature Authority and eSign Australia Limited have achieved full Gatekeeper accreditation. Currently, another seventeen organizations are seeking accreditation. They include KeyPost, KPMG Information Solutions Pty Ltd., Telstra, Centrelink, SecureGate Limited etc. The strategy also allows for cross recognition with other accredited digital certificate schemes. Development and use of Australian Business Number based Digital Signature Certificate (ABN-DSC) are being implemented to assist in the government's aim of having all appropriate services online by 2001.

Commonwealth Government has also established the National Electronic Authentication Council (NEAC) to enhance confidence in authentication technologies and promote their adoption (Commonwealth of Australia, 2000a). NEAC, national focal point for authentication matters, was established in 1999 to oversee the development of a national framework for the electronic authentication of online transactions with its mission to build industry and consumer confidence in the use of authentication technologies.
At the same time, the positive initiatives taking place in the B2B category is bound to have its spill over among the retailers. This would dramatically improve the security concerns and security provisions in retail web sites. However, it should be understood as to why the internet adoption rate among the brick and mortar retailers is low, and whether these categories are representatives of the retail sectors. Although CAs provide a high level of security, it is based on technological solutions to which consumers are not used to yet. For example, Josang (2001) argues that "other elements that we often rely on for authentication in the physical world such as company logo, face or voice are not presently part of certificates". Also could it be that the costs involved are beyond what retailers can cope with in a situation with little government incentive? Only a detailed follow up study of the web sites of Australian online retailers and surveys would give a better picture of the future of internet technology adoption including the role of certification authorities. The online retailers have to realize that security is not a product, but a process. As Schneier, (1999) argues, it is more than designing strong cryptography into a system; it is designing the entire system such that all security measures, including cryptography, work together.

REFERENCES


ABSTRACT

In this paper we explore how secure coprocessors can be used to secure client devices, especially mobile clients such as notebook computers. The goal is to protect data on the mobile client in case of theft, and to adapt the client's protection to the working environment --such as the Intranet or Internet-- without relying completely on the integrity of the client.

We show how physically secure coprocessors can introduce a security lifecycle into commercial off the shelf (COTS) clients by booting the client into a secure starting state, supervising the client's configuration and operation, and inspecting any network traffic that is sent or received by the client.

Keywords: Security, Secure Coprocessor, Applications.

INTRODUCTION

Physically secure coprocessors, such as IBM's 4758 (IBM 1997), nCipher's nShield (nCipher), and Baltimore's SureWare Keyper (Baltimore), have almost exclusively been used in server configurations, where the secure coprocessor primarily provides cryptographic acceleration and secure key storage. The use of secure coprocessors in client configurations has hardly been explored. This is surprising since physical protection offers many additional benefits for mobile clients. The need has been underscored by several recent high profile incidents in which notebooks containing highly sensitive information disappeared. A physically secure coprocessor would have offered much better protection in these cases.

Ideally we would like to secure mobile clients in the same way we do secure coprocessors, using a tamper responsive enclosure and a controlled execution environment, but the cost of such a system would be prohibitively high. In particular, we consider a new secure coprocessor implementation that we call Mycroft. It builds upon the features the IBM 4758 (IBM 1997), borrowing others from related projects (Neal et al. 2000), and adds a network Ethernet interface. This Mycroft device, in PCCARD/CARDBUS format, acts as an independent party within the mobile client.

In the following sections we discuss a number of applications of physically secure coprocessors and show how the security of the client is improved. In the 'Applications' section we describe those applications that, running on such a device, enhance the client's security. These include: secure bootstrap, host monitoring, intrusion detection systems (IDS), firewalls, and controlled VPN. Conclusions and future work are discussed in the last section.
APPLICATIONS

The order in which we present the applications is motivated as follows: First what security mechanisms must be implemented securely? Second, which security mechanisms, as parts of distributed applications, profit from secure environments? Third, which applications can utilize secure environments to run in potentially hostile environments?

Figure 1 depicts the inter-relationships of the applications that we present in this section.

![Application Inter-relationships](image)

The host secure boot application ensures that the host is booted into a secure state. The host monitoring system supervises the operation of the host and depends on the initial secure state of the host to determine the kernel data structures and configuration files that must be evaluated. The IDS and the firewall depend on the host information provided by the host monitoring system, e.g., to examine host configuration files for those services that are passed through the firewall. Finally, the VPN client depends upon all the other components to ensure that the security status of the host conforms to the security policy of the VPN server throughout the connection phase.

Host Secure Boot

Host secure boot (Arbaugh et al. 1997) is a collective term for a combination of mechanisms that provide integrity guarantees during system startup. These provide initial system guarantees such that, if an operating system kernel is started, the specific kernel and machine configuration are known. The latter includes hardware configuration (disks, Ethernet boards, amount of memory, etc.) and software configuration (firmware versions, bootstrap loaders, etc.). The initial system guarantees prevent an attacker from modifying the bootstrap loader or firmware, or adding additional equipment without approval.

The host secure boot scheme consists of two distinct stages. The first stage is the configuration stage and the second is the verification stage. During the configuration stage we checkpoint the state of the system, that is: enumerate all the devices within the system, compute secure hash values over all the host firmware and its controllers, and compute secure hash values over the bootstrap loaders, kernel image, and other crucial files necessary for bootstrapping the system. This configuration is then signed by a security officer and stored in the secure coprocessor. Only configurations with a valid signature are accepted.

Rather than assuming the host is secure, we have the secure coprocessor verify that the host is in a secure configuration. We accomplish this by giving the insecure host a large number of puzzles to solve that involve some computation. These puzzles are different on every reboot and every puzzle has a chance associated with it that the host can guess the right answer even though it did not perform the
associated computation. Since all puzzles are independent, these puzzles can be used to achieve a certain confidence level, say 99.99%, the host is executing with a valid configuration.

While the exact nature of the puzzle generation process is beyond the scope of this paper, the puzzles themselves need to be generated within a trusted environment that is different from the host. The puzzle answers should be verified within that same trusted environment. Obviously, the ideal place to generate the puzzles and verify them is within a secure coprocessor.

The secure boot process outlined above requires a safe place to store the secure state configuration for the host, and it requires the host to execute verification code. To trust the answers from the host we either ensure that a potential adversary cannot modify the verification code and its answers, or use the secure processor and software puzzles to achieve high confidence that the host is in the secure state configuration. We are currently exploring both approaches, but the former has preference because of its simplicity.

**Intrusion Detection Systems**

Computer systems commonly feature the ability to process programs of different users at the same time. The systems keep track of the users' identity and access rights to shield different users, their programs and data, from each other.

In practice, this does not work. Networked computer systems, offering services to remote users, are always as vulnerable as the authentication method that is used to determine the identity and access rights of remote and local users. Today, this is mainly user ID and password based authentication.

Additionally, computer systems have become more and more complex, and we do not know any general-purpose computer system that claims to run certified and formally verified (not to speak of verifiably correct) programs.

Exploiting weak authentication schemes or computer programs, users can gain administrator privileges on almost any commercial off the shelf computer system. Having such privileges, the system can be compromised. Information and programs of any other user can be modified and disclosed. Hence, tools have been developed to detect known attacks that might compromise the integrity of a computer system. Combining the IDS with notification services, alarms are sent to local or remote users indicating the type of potential ongoing attack and proposals for reaction, as illustrated in figure 2.
In this figure we illustrate (1) a host-based IDS with agents residing in the host, in the secure coprocessor, or both, (2) a simplified host monitoring system, and (3) a host-based network IDS, all with audit logs residing in the secure coprocessor (although these logs may be signed by the secure coprocessor and sent to the central control systems as well). The agents themselves could consist of pattern matching, anomaly detectors, and profile engines, or some of the analysis activity could be performed by the main IDS engine, which itself probably communicates with the central control systems.

There are different traditional approaches to implementing Intrusion Detection Systems. We will first discuss mechanisms that are based on host events and then mechanisms focusing on network events.

**Host Monitoring System**

Another application of a secure coprocessor is that of a host monitor, whereby an application on the secure coprocessor acts as an independent party that keeps a tap on programs executing on the host.

The monitoring application is closely associated with the host secure boot mechanism. Secure boot provides a strong integrity guarantee; it ensures that only an approved operating system is started on an approved hardware and firmware configuration. The ability to provide these strong guarantees vanishes as soon as the host processes external input, because the external input potentially allows code-injection attacks (for example) that inject foreign code into an initially secure configuration. While we are no longer able to provide strong integrity guarantees, we can take advantage of the secure coprocessor to ensure weaker integrity guarantees.

Weak integrity guarantees have the property that an adversary on the host may circumvent them. However, the level of sophistication required by the adversary depends on the level of difficulty of the monitoring program. Examples of monitoring programs include, a Tripwire (Kim & Spafford 1994) like process that, independent of the host, accesses the disk, computes checksums over the files stored on it, and then compares the result against a database of know values. Unlike the Tripwire product, where the checksum database and verification process reside on the host and are therefore vulnerable to attacks, our database and verification process reside within the secure coprocessor, which is inaccessible to attackers.

Another function of a monitoring device is data structure invariant checking. Here the secure processor is given invariants of the data structures in host memory (for example kernel data structures that describe user access permissions). At regular intervals the monitoring program checks whether the invariants still hold. If an invariant fails it can either log this event or disable the functions of the secure coprocessor.

The host monitoring capabilities still require further investigation. The advantage is that they can provide additional but weaker integrity guarantees when the strong guarantees no longer hold. A serious problem with host monitoring applications, however, is that they have the potential to invade the privacy of the user.

**Host-based Intrusion Detection Systems**

Host-based intrusion detection systems use information originating on the host to detect misuse. Different information sources can be used, such as system and application event logs, account usage statistics, critical data access and modification, etc.

Host-based IDS are usually agent-based, consisting of executables that run on the host and communicate with some central control system. Raw data is collected and sent to the central control system for analysis. If the analysis indicates known or potential attacks, the central control system is the originator of the prescribed response or remedy. Raw data can also be analyzed locally, whereby the agents send status and alerts to the central control system as appropriate, thus reducing the load on
the central control system and potentially affording nearer to real-time or in-time detection and response. Often, a combination of both approaches is taken.

The advantage of applying a secure coprocessor to host-based IDS is similar to that of service processors in many servers and mission critical systems today. That is, the ability to function independent of the host's system and application software and, to some extent, independent of various hardware components and subsystems of the host system. However, service processors are themselves not immune to physical or logical compromise. In most cases service processors are not designed with security in mind, and therefore cannot be trusted to the extent that secure coprocessors can (provided they have undergone various development process review and inspections, and more importantly, some sort of independent security evaluation). Most service processors also do not offer a general purpose computing environment, secure storage and management of data, or the ability to perform [hardware assisted] cryptographic operations in a timely fashion.

IDS agents, and the various policies they enforce, can be located and executed internal to the secure coprocessor where proper execution can be ensured. These agents would have access to data residing on the host --on storage devices (in file systems), or main memory-- for event log analysis, pattern/signature matching, and the like. In some instances, raw data such as the actual system and application event logs, behavior and usage statistics, etc., may reside in the secure coprocessor as well, ensuring the integrity and confidentiality of such data (integrity checksums/hashes maintained in the secure coprocessor for data that is resident on the host may be used for this purpose as well), and also controlling access to this data. Because of it's ability to ensure data integrity, housing raw data on the secure coprocessor with its trusted time stamping abilities, even temporarily, would also facilitate further [off-line] analysis, as well as data forensics and support for any potential litigation --e.g., prosecution support or liability defense.

The secure coprocessor can also be used for surveillance of targeted data, programs, system resources, or accounts when misuse is already suspected. Surveillance is similar to the general data gathering and analysis described previously. However, surveillance is more finely tuned for specific attack or misuse scenarios. With the use of secure coprocessors, the host is oblivious to the fact that surveillance is being conducted, or that any IDS functionality is taking place beyond the bounds of what is normally performed (e.g. a sudden or unexpected change in an IDS audit or detection policy), avoiding the possibility of alerting potential perpetrators.

The secure coprocessor may also be used in conjunction with the host's system software, via redirection or collaboration, to assert access rights and privileges, or to monitor specific system call and system resource usage. The secure coprocessor is also an ideal platform for certain automated responses, such as responding to an anticipated attack (where a set of activities matches the signature of known preliminary attack pattern), thus stopping the attack or misuse before it begins (Proctor 2001).

Scalability over time ('slow attacks') and space (large numbers of hosts), where the central control systems cannot adequately address the amount of data needing to be analyzed in a timely fashion, is a problem for many current IDS solutions (Ptacek & Newsham 1998). In an environment where secure coprocessors are employed almost ubiquitously for IDS [and perhaps other] purposes, the collective IDS, or at least the analysis functionality, can be implemented in a highly distributed fashion in order to take advantage of the processing resources of the collective system of secure coprocessors, each with the ability to communicate securely and independently with each other.

Reliability of information sources (e.g., sensors and agents), as well as reliability of the analysis engines and response mechanisms, is also problems for many of today's IDS solutions (Ptacek & Newsham 1998, Bace 2000). With their ability to securely execute specified programs and ensure the integrity of collected data, secure coprocessors offer unique advantages to address many of these reliability problems.
An IDS (its agents) must execute in a secure environment. Otherwise, if the host is successfully compromised before or without the IDS noticing, the IDS is itself subject to compromise, rendering it useless. Given the role of host-based IDS, it will likely be [one of] the first targets of an attack.

The patterns/signatures and rules/policies that define what the host-based IDS looks for, reports, and responds to, should be confidential. Otherwise, attackers will likely be able to avoid specific patterns, time their attacks in order to avoid event timing windows, or react by launching subsequent or related attacks before the IDS can counter the original attack. As IDS and pattern detection are likely to never be comprehensive, shielding information from attackers is important.

Having physical control and protection of the IDS is also necessary to protect the IDS from misconfiguration by the host's administrator / operator. This is a critical issue as IDS functionality becomes more ubiquitous and the number of devices benefiting from IDS increases dramatically.

Using physical security provided by the secure coprocessor and IPSec or SSL to establish secure connections from the corporate security center to the IDS (e.g., in a telecommuter's laptop), enables secure remote management, update, and monitoring. Using certified secure coprocessors enables users to establish trust in the state of the secure coprocessor.

Similar to many of the applications envisioned here, host-based IDS implemented with secure coprocessors need sufficient general purpose and cryptographic processing power to accomplish the necessary tasks in a timely fashion. Since IDS are data intensive, sufficient system and local bus bandwidth, as well as network bandwidth and the capacity of onboard secure storage, will also be important factors in seamlessly implementing IDS with secure coprocessors.

As the numbers of computing systems increase, the average costs decrease (especially for mobile and pervasive devices where disconnected IDS abilities will be necessary), secure coprocessor footprint and the need for cost-effect but secure platforms to aid in IDS functionality will also be necessary.

**Host-based Network Intrusion Detection System**

The more traditional network-based, or promiscuous-mode, IDS consist of several to many sensors deployed throughout the network monitoring all/most network traffic to and from many systems on a segment. Host-based network IDS, in contrast, are usually more widely distributed among systems on the network, but need only monitor and analyze network traffic to and from the target host. Host-based network IDS also tend to communicate and collaborate with each other more so than the traditional network-based IDS. Also, with the narrower scope of a host-based network IDS (not having to monitor all traffic on a given network segment), the number of packets that can be inspected, patterns checked, and the analysis performed, can be finer-grained.

The host-based network IDS periodically checks the "open" services of the host to keep its view consistent with the host. The IDS can even shut down services on the host if they contradict the security policy or it can be combined with a firewall that forwards traffic to a local dummy proxy (firewall/IDS integration). Therefore, many attacks based on confusing the network IDS or installing new services won't work on such guarded systems.

As the host's interface to the network or particular network segment, the secure coprocessor-based network IDS has access to all network traffic originating from or destined for the host, even before the host has a chance to see the packet in the latter case.

The secure coprocessor, with its hardware accelerated cryptographic abilities, can also address one of the biggest problems for a host-based network IDS: encryption. Encrypted networks and secure tunnels into and out of the host (VPNs) encrypt the payloads of packets, making it impossible for the IDS to analyze traffic data for known patterns, viruses, and the like.
Operating in promiscuous mode, the secure coprocessor-based IDS can even function as a traditional but secure network-based IDS sensor, with the necessary computing power to perform much of the necessary analysis— even more so should such devices be widely deployed across the network.

Having the IDS directly at the host affords a better means to counter insertion/deletion attacks (more effective, as host behavior can be predicted precisely). The secure coprocessor-based IDS could also handle packet de-fragmentation internally, countering overlap-attacks. And serving just one host, the IDS reacting to a detected attack can immediately isolate the host, shutting down questionable connections, and finally re-integrating the host into network.

Employing secure coprocessors for host-based network IDS offers many of the same advantages that using secure coprocessors in a purely host-based IDS solution does, including:

- Trusted and reliable execution of IDS agents, and secure storage of critical data—e.g., event log files, policy parameters, resource usage and pattern statistics, etc.
- The secure coprocessor can be independently updated and configured/managed from the host in a secure fashion.
- A highly distributed network IDS can take advantage of numbers and computing power of a system of secure coprocessor-based agents, communicating independently and securely with each other.

Secure run-time environments promote secure remote management and update of IDS software, patterns, etc. The secure coprocessor is a portable device that accompanies the user and can support multiple security policies, switching between a "telecommuter user" mode and an "company user" mode. Neither the organization nor the private user can install programs that are not certified by a common trusted party that—from a security perspective—owns the secure coprocessor.

Thus, we tackle a problem regarding privacy requirements for remote/mobile users: the potential supervision of remote users by organizational security officers. This problem is partly solved by enabling a user to determine the policy of the active IDS. By establishing a trusted third party, users can make sure that the corporate IDS software, being signed by the third party, only retrieves and stores the information agreed upon between the organization and its member, the user. Disabling the IDS, even temporarily, makes no sense from a security perspective, as successful attacks launched when the IDS is inactive remain undetected even when the IDS is later re-activated.

Host-based network IDS have challenges similar to host-based IDS implemented with secure coprocessors, perhaps with more emphasis on network bandwidth and sufficient onboard resource to perform packet inspection and re-assembly as necessary.

**Firewalls**

Firewalls protect sub-networks or host by countering attacks that originate from the network. They intercept any traffic from and to a protected host, here the client. This traffic is examined and restricted to specific ports and protocols as stated in the security policy; in doing so it restricts client applications that are remotely accessible (Cheswick & Bellovin 1994, Zwicky *et al.* 2001). Insecure services (such as NETBIOS on Windows systems or Sendmail on Unix systems) must be blocked when connecting directly to the Internet and enabled when connected to the Intranet where corporate firewalls offer protection against attacks from the Internet. As most applications listen on well-known ports using well-known protocols, a firewall can protect clients independent of the client's operating system and environment by filtering incoming packets based on port number and protocol.

To protect client machines inside and outside the Intranet, we need to enable firewalls at the client. Pushing firewalls from the sub-network boundary to the client machine has been discussed earlier by Steve Bellovin in his much-cited paper about distributed firewalls (Bellovin 1999). Recently, he also admits that there might not be correct client systems in the near future (Bellovin 2001). Thus, besides...
trying to identify attacks exploiting respective vulnerabilities as described in 2.2, remote access in unprotected environments (Internet) to vulnerable applications should be disabled or minimized by firewalls. For instance, there is no point in keeping Windows NETBIOS services open when the user is at home and connected to the Internet; although they might be needed open when the user is inside the corporate Intranet to access shared resources. The same holds for remote management services.

Users running vulnerable applications are prone to become the victim of remote attackers. Once attackers successfully exploit such vulnerabilities, they can easily manipulate the user's run-time environment and gain long-term control over the user's computer — without the user being aware of this.

In effect, the remote user's client becomes the weak point in the company security architecture and defeats the security policy that is established and enforced by corporate firewalls — a huge waste of money!

However, implementing firewalls on the client itself makes them as vulnerable to manipulation as any other host software. They are of no practical worth once an attacker gained access to the client (e.g. by executing a single --downloaded-- manipulated program on the client).

Thus, we propose to enhance mobile and home computers by a security device running a firewall that conforms to the corporate security policy. Incorporating firewalls into the secure coprocessor as illustrated above, these firewalls can be remotely managed and updated by the corporate security officer and are protected against user's misbehavior and against (potentially manipulated) applications running on the client. In order to optimize flexibility and security, we envision two generic operation modes for personal firewalls:

- **The company mode firewall** protects clients inside the company Intranet. It keeps more services open, as the client is protected against attackers by the corporate firewalls of the Intranet. Client services, such as NETBIOS on Windows OS and SNMP agents, remain accessible to share drives, access directory services, or remotely manage the client configuration.

- **The telecommuter mode firewall** protects clients that are connected through an ISP to the Internet. This mode is much more restrictive, as the clients are unprotected against attacks from the Internet. Any NETBIOS, mail, ftp, or telnet services of the client are most likely to be blocked.

To be effective, a company mode firewall must ensure that no other network interfaces are active through which attackers could bypass the firewall and build up a connection from the Internet into the corporate Intranet. Besides this, the environment must support remote configuration by the company security officer, remote management and regular inspection by a trusted party, protect company secrets such as management keys and passwords, filter rules, filter settings, security logging data, and should be certified to ensure the company that it works properly and the users that their privacy is not compromised by the device.

On our secure coprocessor we are going to extend the Linux filtering and firewall functions (Linux) to include checks of host integrity (interfacing the IDS) and checks of the configuration of the service being addressed by the inspected packet (interfacing the host monitoring system). The packet is then forwarded to proxies within the secure coprocessor, passed through to the client, or discarded depending on the policy settings.

As both user and corporation must trust the firewall, it must resist attacks in hostile environments (user, company, or environment, lost devices etc.). Secure coprocessors offer an ideal place to implement such personal firewalls independent of the client's operating system and management.
Although personal firewalls introduce a new granularity of protection, they are only part of the solution. They need to be combined both with IDS and with the host monitoring system to ensure effective and secure operation:

- The IDS ensures that those services that are open are not manipulated or used for break-ins via known vulnerabilities.
- The host monitoring system must ensure that those services that are open are configured appropriately (e.g., no read/write anonymous ftp directories, no overlapping ftp directories, ftpd run with chageroot and minimal privileges).

To conclude, personal firewalls protect mobile computers in a flexible way according to the situational need. Running these firewalls on multi-party trusted environments enables them to implement multi-lateral policies, namely the corporate security policy and the user's privacy policy. A general-purpose secure run-time environment also opens the possibility of running several proxy services on the secure coprocessor that implement finer-grained control of a single service (e.g., FTP, SMTP, HTTP application level command filters).

There remain some challenges. First, it is not easy to find the right policy, which is neither too restrictive nor opens vulnerabilities. Additionally, we need to discover and (to a certain degree) control any other potential network interfaces --e.g., internal modems, PCMCIA, parallel port, serial port-- that are controlled by the client and could be used to bypass the firewall.

**Virtual Private Networks**

As working from home becomes more and more convenient, such user-managed systems, directly exposed to the Internet, become part of the corporate Intranet by using VPN clients on the remote systems and connecting to VPN servers inside the VPN. The VPN connections are encrypted and are usually passed through the Intranet firewall to the VPN server without further inspection. The VPN server authenticates the user and implements the IPSec tunnel endpoint.

Thus, insecure and manipulated clients pose a substantial security risk to any organization that allows remote workers to access the company VPN or to process sensitive data. Figure 3 shows the basic scenario and the way attackers can circumvent the corporate firewall via a vulnerable client outside the Intranet.

![Figure 8: Circumventing the corporate firewall](image)

The figure shows that instead of defeating the well configured and professionally managed Intranet firewall of the corporation (1), attackers gain access to ill-managed remote clients attached directly to the Internet (2). Via this machine's VPN client, the attacker can go straight into the corporate VPN, whose traffic is usually allowed to pass the Intranet firewalls without further inspection. The attacker will always be able to pass into the corporate VPN server along with the regular user because the user opens the authentication door for any application on the client and for any Intranet service offered to remote VPN users.
Whether or not the attacker can walk in and out of the corporate VPN via manipulated clients depends mainly on the security of the authentication used:

- Systems using user password authentication are completely insecure once the client is hacked. An attacker controlling the client can easily eavesdrop the VPN userid and password. Having userid and user password, attackers gaining access to the VPN client code can effectively access the corporate VPN from wherever they like.

- One-time passwords --e.g., produced by SecuriID cards (RSA)-- disclosed to the client, e.g., entered into a pop-up window, offer more security, if the validity period is short enough and the timeout of VPN connections is reasonably short. The attacker must operate within the validity period of the one-time password after the user signs in and discloses a valid one-time password to the client machine; the security in this case is mainly defined by the expiration of a VPN connection, which determines the time window for attacks using a disclosed one-time password. The attacker cannot operate without the user logging into the VPN server.

- Disclosing one-time passwords or user passwords to the secure coprocessor only (via small keyboard or smart card), restricts attackers significantly. In this case, attackers cannot authenticate against the VPN server even if they possess the VPN client code (at least not by merely controlling the client). The attacker can operate only as long as the VPN client remains connected to the VPN server and the VPN client cannot be manipulated to keep open VPN connections hanging despite users closing them. Additionally, IDS, firewall and host monitoring system ensure that the client is very well supervised and protected against compromise right from the beginning.

The first two scenarios (user password and one-time password authentication) were less critical when clients were connected through the phone system to a single Internet Service Provider; in this case the client was either connected to the VPN or to the Internet. This posed security problems as manipulated clients could retrieve valuable information when connected to the VPN and later send the information to the attacker when connected to the Internet. However it was far more difficult to achieve:

- Clients had IP addresses assigned by the ISP and these addresses were dynamic. Thus attacking a dedicated client was difficult without real-time Internet Service Provider information -- although not impossible.

- Clients were not online all the time; thus networking attacks had to be synchronized with the client's connectivity.

- The gathered information had to be retrieved somehow by the attacker. As the IP address of the client changed, the client usually sent the information to a specific address, newsgroup or any other place; this addressing information is found on the client in case the manipulation is detected and raises the risk of disclosing the identity of an attacker.

Attacking clients that are connected to the Internet 24 hours and 7 days a week is far easier. First, IP addresses are static or do not change often, i.e., once a victim's machine has been successfully attacked, the attacker can address the machine remotely. Attacks can be scheduled any time the client is unobserved -- although, this could be countered by running IDS on the clients. Third, gathered information can be retrieved remotely without the need to disclose any remote address to the manipulated client (other than in forgotten log files). In a last step, attackers gain real-time connectivity to the company Intranet via the client and can hack other machines inside the Intranet to elevate their privileges.

Therefore, an effective security policy grants remote clients access to the corporate Intranet via VPN tunnels, if and only if the security status of the remote system is trustworthy to the company.
But how can we remotely determine the status and trustworthiness of a remote client?

At this point, we leverage our Mycroft device and its regularly updated evaluation of the client's security state. The remote access security policy could look as follows. A VPN client is connected to the corporate VPN server, if and only if the following conditions hold:

- The VPN client is running inside the secure coprocessor.
- The secure coprocessor is not tampered.
- The secure coprocessor is in telecommuter mode.
- The firewall and intrusion detection systems are activated (and then in telecommuter mode) and the logs suggest that the client is not compromised.
- The host monitoring system reports the client status as secure taking into account the history of the client since the last secure boot.
- The VPN tunnel setup is successful (IKE/IPSec in VPN client and server cooperate).
- The client authentication via the secure coprocessor is successful.

Applying our Mycroft device to protect a VPN client is shown in figure 4.

Implementing IKE and IPSec inside a secure device, any long-term secrets (such as keys for IKE authentication) are protected against the user and other potential attackers. Combining firewalls, intrusion detection systems, VPN client, and IKE/IPSec functionality inside the secure device enables secure remote management of the device.

This, in turn, gives organizations a valuable control over the remote end of their VPN tunnels. Decisions on whether or not to allow remote users access to the corporate VPN can be made based on the client's security status.

Additionally, the VPN client and VPN server can be enhanced to offer different security levels, in which different sets of Intranet services are available to remote users. The VPN client would tell the VPN server which security level it wants to connect and the VPN server would retrieve respective policy. Then, the VPN server would request the VPN client, who in turn requests the secure coprocessor, to establish this security level in the client (e.g. by rebooting it or changing configurations). In this way, the same client machine can participate in different security levels. To raise a security level, it will usually be necessary to reboot the client to re-establish an initial security level. Some security levels might not be achievable by clients managed by normal users.

We won't be able to completely prevent attackers using compromised clients to walk into the Intranet, but we can make it seriously hard for them and we can restrict access to services (e.g., differentiating access levels as WWW services, Mail, or Developer access).
CONCLUSION AND OUTLOOK

Secure, general-purpose, self-defending devices of various strengths provide the necessary platforms for ensuring trust and security. The examples elaborated above in the Applications section show how such a programmable device can be used in a variety of ways, controlled either by the user or remotely by an organization such as a service provider or an employer, for mutual benefit.

The embedded platform prototype of the Mycroft device is up and running. We chose to adapt Linux as the operating system on a PowerPC embedded platform, and to deploy FreeSWAN IPSec, IPTables, and open source IDS systems to implement the security services described above. We are going to integrate those applications, and develop useful configurations and remote policy management on the embedded system. At the same time, we will develop the host secure boot and the host monitoring application from scratch.

There are other applications which rely upon protecting sensitive data, or which are sensitive per se. Such applications may need to function in environments in which the host has weak security, or is controlled by parties with opposing interests. This area is eminently well suited to secure, general-purpose, coprocessors. Sensitive data (such as keys) used for authentication or signature services can be kept within the secure boundary. Sensitive programs can be stored and run within the secure coprocessor.
REFERENCES


*Baltimore SureWare Keyper* [On-line]
http://baltimore.com/products/sureware/keyper.html


*Linux IPChains and Firewall HOWTOs* [On-line]
http://linuxdoc.org

*nCipher nShield products* [On-line]
http://www.ncipher.com


http://secinf.net/info/ids/idspaper/idspaper.html

RSA SecurID [On-line]
http://rsasecurity.com/products/securid

Dataveillance and Compliance Verification: Knowledge Management of the True and False Positives

Peter Goldschmidt Ph.D.
Department of Information Management and Marketing,
The University of Western Australia
Email: pgold@ecel.uwa.edu.au

ABSTRACT

Surveillance systems are typically used by public and private organisations to monitor data and transactions for compliance. The information resulting from this monitoring and the decisions made and disseminated by these organizations, have the potential to impact their operations and the lives of individuals influenced by their decisions. Therefore assuring and verifying surveillance information quality and integrity is fundamental to the success of these modern information-dependant organization.

This paper discusses a method to support data-surveillance monitoring and a compliance verification knowledge management system, called CV-KMS.

Keywords: Dataveillance integrity assurance, Information verification, Knowledge management, Compliance verification infrastructure

INTRODUCTION

This paper discusses a method to support data-surveillance monitoring and a compliance verification knowledge management system, called CV-KMS.

Surveillance systems are typically used by public and private organisations to monitor data and transactions for compliance. The information resulting from this monitoring, the decisions made and disseminated by these organizations, have the potential to impact their operations and the lives of individuals influenced by their decisions. Therefore assuring and verifying surveillance information quality and integrity is fundamental to the success of these modern information-dependant organization.

Additionally, the emergence of electronic commerce activities using the Internet and the proliferation of national and organisational Intranet, Extranet and mobile commerce structures, has further raised awareness of security and compliance issues essential to ensuring and maintaining the security and integrity of transactions conducted via this new technology.

For the purposes of risk management, governments and commercial organisations typically use a filter to monitor transactions that may impact on their operations. These automated data analysis techniques identifying variances typically depend on data that identifies source agents and their relationships, and is used to draw a compliance agent's attention to a particular event or group of events that indicate possible anomalies and therefore potential non-compliance.
(Clarke 1988) describes the electronic monitoring of data related to individuals and groups of individuals as 'dataveillance'. He highlights the inherent dangers of drawing conclusions resulting from this data, and points out that a major problem in dataveillance is the high noise to signal ratio, which may result in misleading conclusions. Subsequent advances made in improving the quality of this data have, in general, reduced the problem of misleading results produced due to this 'noisy data'. These advances include improvements in data processing and the increased use of sophisticated computational techniques such as statistical, knowledge-based and artificial neural computational methods. These systems are centred on the events being monitored and the events' source agents. Their results however still require human judgment to determine their validity. A more detailed discussion of the sophisticated computational techniques available is presented in Goldschmidt (1996, 1999, 2001).

CV-KMS acts as a secondary monitoring facility. It is a novel and innovative approach to supporting, verifying and assuring data and information compliance by assisting in analysing and categorising exceptions, or results, generated by primary surveillance systems. These results are either true of false positive. CV-KMS assists in assuring the fulfillment of the necessary and sufficient evidence supporting (true positive / negative) or refuting (false positive) hypotheses of non-compliance. This is achieved by combining quantitative and qualitative evidence supporting or refuting the hypothesis, accumulating and recording this evidence, generating an audit trail of each step in the compliance decision process, and supporting the compliance review process through a compliance team or through an organisation's management hierarchy. Table 1 lists some of the advantages of CV-KMS.

The system is parameter driven, and for input requires the output resulting from the organisation's domain specific primary monitoring system plus related information.

- Adds functionality to primary monitoring infrastructure, without modifying primary system
- Proposes a framework for compliance verification knowledge management.
- Provides for the decomposition of surveillance tasks.
- Provides a consistent evidence evaluation and combination structure.
- Provides records of evidence from each stage.
- Adds value to surveillance operations by reducing the cost of surveillance monitoring, assisting in surveillance accountability and providing transparency, when required, thereby contributing to surveillance governance and due diligence.
- Employs a method that adds value to a generated exception by encapsulating and associating the event's attributes, its source agent's characteristics, the evaluating agent's analysis and the recommended remedial action plus the substantiating evidence.
- Exploits an infrastructure support construct and secondary filter, allowing for collaboration, truth maintenance, audit trails and decision support, thereby facilitating decision consistency and greater processing volume.
- Using the approach as a decision aid and secondary filter, analysis of results can then be used to review the analyst's decision-making processes and to refine the primary filter tolerance levels.
- Supports a structured, flexible and inclusive approach to surveillance analysis.
- By adding a cost function to the surveillance-monitoring infrastructure can capture cost-benefit trade-off.
- Insight is gained from the knowledge acquisition component when setting up parameters and heuristics.
- Assists in the development of an effective accountability structure.
- Reduces distrust of surveillance monitoring systems, by reinforcing accountability and transparency.

Table 1: Advantages of CV-KMS
DATAVEILLANCE AND COMPLIANCE VERIFICATION

To protect assets, and to enhance and encourage the security of electronic transactions, the US government (Ware, 1976, 1998, CIAO, 2001, Walker, 2001, O'Neill, 2001, for example) and the European Parliament (EC, 2001), have highlighted the need for increased surveillance of electronic transactions and communications conducted via the Internet. Other governments mirror these concerns. Interested readers are directed to (Clark, 1998).

Concurrent with the need for surveillance is a need to maintain personal privacy, due diligence, and accountability. (Cillufo, 2000).

In order to manage these seemingly conflicting objectives, governments and other organisations, public and private, employ regulatory authorities whose task is to maintain, support, and enhance corporate governance, security, compliance, accountability, due diligence, strategic advantage, and risk management. Examples range from standard data processing routines that ensure internal control, such as data input, processing and output compliance, (Weber 1999) provides a comprehensive discussion on these processes, to the monitoring of events transacted in more complex environments, such as fraud detection, intrusion detection systems and the like, via sophisticated statistical, artificial intelligence and neural computing techniques, or hybrid combinations. We describe these devices as primary monitoring systems.

These primary systems function as a process by which the integrity of transaction data as well as the entire transaction, or event, is examined to ensure that both comply with some predetermined conditions. If the event complies, it is accepted for future use; if it does not, it is rejected from further processing, pending some remedial action.

The monitoring techniques are used to assure the detective, protective, and corrective operation. Quantitative and qualitative information may be required to evaluate and assure the validity of the results of these systems.

The compliance monitoring process compares some predetermined conditions of acceptance with the actual data or event, which is a matching process. If any variance is detected between the conditions and the actuals, an exception report is produced, identifying the variance. This identification of the variance either fulfils the conditions of necessary and sufficient evidence, and thus determines an instance of non-compliance, or if not, may be only an indicator of possible non-compliance. In the latter case further evidence must then be sought to fully substantiate the hypothesis of non-compliance.

Surveillance mechanisms typically rely on deviation metrics, either using tolerance levels, pattern matching, checklists or past case comparisons. However with any set of metrics, deviant (even fraudulently motivated) behaviour may escape detection. Tightening tolerance levels limits increases the likelihood that these exception conditions will trigger an alert. However this increased detection capability does not come without cost. Tightening these limits also increases false positive alerts since the number of instances that fall outside the tolerance must necessarily increase, as the limits become more restricted. The cost for the analyst (the decision-maker) to review the additional non-exception condition alerts must be assessed in relation to the imputed value of identifying the additional true exceptions detected by more stringent limits. (Davis and Ord 1990, pp. 39 - 40).

This cost is due to the temporal and context sensitive nature of the information required evaluating each exception and to confirm or refute the evidence supporting the assertion of non-compliance in complex environments.
OBJECTIVES OF CV-KMS

CV-KMS was developed to provide compliance verification assurance via a method and a system of supporting surveillance analysts operating in a complex environment, enabling these agents to perform the task of decision making with greater accuracy, effectiveness and efficiency. The agent or agents may be human or machine based. Machine based or independent software agents function as repositories of human opinions related to the event under scrutiny. The system was originally prototyped for supporting capital market surveillance analysts at the Surveillance Division of the Australian Stock Exchange, and successfully tested.

The CV-KMS methods and system of supporting a compliance agent in surveillance assurance may find many other applications in fields as diverse as commerce, industry, medicine and defense.

Applications including electronic commerce compliance decision-making; log file analysis; data warehouse monitoring; enterprise resource planning (ERP) compliance monitoring (continuous auditing decision support). Intrusion detection analysis; fraud detection monitoring; medical and pharmaceutical safeguards; industrial safeguards; banking and finance, tax and insurance compliance; and privacy compliance monitoring.

Information filtering, retrieval, transfer and exchange; and, applications requiring the systematic reduction of noise associated with any surveillance, information acquisition or evaluation tasks; and, applications which assist in monitoring compliance of organisational strategic, managerial and operational imperatives.

See Table 2 for further examples of potential applications.

| Public organisations | agencies that routinely monitor activities to ensure compliance. Examples include, the securities and investment commissions; health insurance commissions; agencies that administer and oversee public rebate claims or payments, and privacy, such as departments of taxation, social security; medical insurance, customs and excise compliance monitoring; law enforcement; environmental protection agencies; and food, agricultural and drug authorities; national treasuries (US Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) detecting fraud and money laundering); GATT, NAFTA and EURO compliance (Echelon and the like); protecting critical national infrastructure (the proposed US government’s FIDNet system); |
| Private organisations | such as: corporate treasuries conducting continuous on-line auditing; credit rating agencies; capital market providers and intermediaries, such as stock exchanges and stock brokers monitoring member, client and employee activities, and monitoring portfolio performance and compliance; banks monitoring client and employee activities and portfolio performance and compliance; credit card and smart card providers; insurance companies monitoring client and employee transactions such as claims and claim disbursements; telecommunication and trading companies; and e-commerce participants such as banks, merchants, providers and customers; industrial safeguards. |
| Medical and Pharmaceutical Safeguards | Monitoring prescription compliance Hospital and medical centre patient treatment safeguards and monitoring medical insurance compliance. |
International Organisation | such as the IMF, the World Bank, UN
| The European Union Privacy Directorate.
Defense | various

| Table 2: Areas of Potential CV-KMS Application, for example |

The Compliance Verification - CV Process

The CV decision process helps to determine if there has been an instance of non-compliance, based on the evidence of an occurrence of a variance between the preset conditions and the actual data or event. The function of a CV is therefore twofold, namely identifying a variance, and producing and accumulating (if required) supporting evidence. When both conditions are met, the evidence points to the detective, corrective or preventative actions as required.

The observed variance takes the form of an exception report, produced by the primary monitoring system, indicating why the exception was triggered. The detective function is fulfilled by the recognition of the variance; the correction function identifies the changes to be made to the data or the event, which can then be re-processed; and the preventative function is fulfilled by recognising and reporting a variance that will result in the suspension or rejection of similar, future events.

Where the evidence or the accumulation of evidence does not directly indicate what action is required, or indicates only the possibility of non-compliance, it is then incumbent on human agents to interpret this evidence to determine what action is required, or to determine if the non-compliant indicator is a true or a false positive directive.

How is CV-KMS used?

The compliance analyst's (or evaluating agent's) primary goal is to evaluate all possible information that can support or repudiate the hypothesis of non-compliance. CV-KMS assists the agents by operationalising this goal. The results of the agent's analysis are summarised and posted to facilitate review by other team members or management. The results include an action list.

The CV Problem Solving and Decision Making Tasks

Secondary monitoring problem solving is the human evaluation of the exceptions produced by the primary monitoring system, a process of determining if a generated exception is valid. This is similar to the analytical review (AR) conducted by auditors and characterised by Libby (1985) as a diagnostic-inference process. Koonce (1993), reviewing past research of cognitive studies of AR, defines AR as the diagnostic process of identifying and determining the cause of unexpected fluctuations in account balances and other financial relationships. Similarly, the secondary monitoring problem solving is the CV diagnostic process of identifying and determining the cause of the unexpected variances resulting from the primary monitoring facility.

Blocher and Cooper (1988) found that auditors performing AR typically follow four distinct diagnostic inference components: mental representation - the accumulation and evaluation of the relevant problem information; initial recognition of unusual fluctuations in a company's financial statements; subsequent hypothesis generation - the generation of potential causes of the observed fluctuations; and finally, information search and hypothesis evaluation - the search for and evaluation of the information relevant to the causes.
With CV, the mental representation component is guided by the results of the primary monitoring facility that accumulates and evaluates the relevant compliance problem information leading to the initial recognition of a variance. This is followed by the subsequent hypothesis generation of the potential causes of the observed variance based on the search for and evaluation of the information relevant to its causes. The diagnostic approach to CV-KMS takes the form of defeasible logic, which means that any inference made may be only tentative, as the inference may require revision if new information is presented. This is due to the default assumption that there is a legitimate cause of the observed variance. It is the task of the decision-maker to evaluate all possible legitimate reasons for its occurrence. If none is found, the hypothesis of non-compliance is strengthened.

**A FRAMEWORK FOR CV USING MULTI-AGENT TECHNOLOGY**

The following presents a limited framework for CV using Multi-Agent Technology.


In a CV environment the problem solving process is collaborative, as the agents share the available data, processed or not, and they are organised sequentially, and hierarchically, with each successive agent having greater domain knowledge and experience. Heterogeneity between the human agents is relatively low, as we are dealing with the same domain. However autonomy is relatively high, as activities do not require either intervention by other agents or constant supervision. Each agent in the team completes their task, but their results may subsequently be modified or explained away by a more senior agent who may apply a different interpretation to the various aspects of evidence supporting or repudiating the hypothesis of non-compliance.

Functionally, the CV-KMS supports individual team members and provide coordination. This corresponds to Shaw and Fox’s (1993) model, which they define as a system whereby 'the overall problem to be solved is decomposed into sub-problems assigned to the agents, each agent, asynchronously, would plan its own action and turn in its solution to be synthesised with the solution of other agents. The agents use either task or data sharing to cooperate with other agents' (p. 352). Therefore each team member has his or her own CV-KMS node; database and graphic user interface [GUI], access to the team memory repository, the blackboard, access to other databases containing historical information and access to relevant external information sources such as real-time market information, news services, intelligence newsletters and the like.

This framework allows for the continuous support of the team members and assumption-based truth maintenance (ATM), (de Kleer 1986).

The team KMS contains the knowledge necessary for the support of each team member. The knowledge in the system supports the decision-making. This domain knowledge, at its lowest level, refers to the CV-KMS objects, events and actions. At a higher level there is knowledge about the domain knowledge: this is meta knowledge, which acts in determining the appropriate domain knowledge to be used in a given situation.
Coordination for ATM

The construct presented here is a variation on Chang et al.’s. (1993) research on distributed reasoning supporting multi-auditor cooperation. The Chang et al. presentation addresses the support for a team of cooperating auditors.

During the cooperation stage, the auditors must ensure that the empirical evidence of other team members does not contradict their default assumptions. The cooperation process requires a narrowing down of the areas of conflict, identifying the areas where further testing is required and the development of the explanation for the consensus opinion that emerges from the process Chang et al. (1993, p. 347).

As part of their analysis, auditors develop propositions or beliefs, based on their assumptions. These assumptions are by nature default assumptions, which hold that in the absence of evidence to the contrary, the item under review is sound.

These propositions may then be communicated to a more experienced auditor who may judge them as true, false or unknown. The judgments of the more experienced auditor are subsequently communicated back to the originating auditor who negotiates until a consensus is reached.

At the macro level, the CV-KMS default assumptions are similar to those of the auditor. That is, in situations where a suspected non-compliant event is presented, it is assumed that there is a legitimate reason for the observed variance, and that this condition can be fulfilled if the higher level Boolean response is positive and the lower level metrics are above a certain threshold level.

There are two fundamental differences between the CV-KMS construct and Chang et al.’s model: 1) the CV-KMS process is not based on a consensus between analysts for ATM but on an hierarchical review, and 2) even though at the macro level our construct uses the trivalent belief-disbelief-unknown, we refine this by applying a measure of the importance that individual pieces of empirical evidence and facts have on the propositions. CV-KMS uses fuzzy set theory to capture the quantitative and qualitative evidence (Zadeh 1983) and frames to represent this knowledge.

Dubois and Prade (1980, 1982), Labouschagne and Eloff (1998), Lee and Han (2000), and Lee and Kwok (2000) have shown that fuzzy set theory is a more appropriate technique in decision environments where there may be a high degree of uncertainty and ambiguity. More recently, Siegel et al. (1995) and Zebda (1989, 1991, 1995) argue the suitability of using fuzzy set theory in areas of auditing where there is uncertainty and ambiguous terms such as moderate risk or high risk are used.
CONCLUSION

The CV method and CV-KMS is presented as a construct for operating in highly complex environments where the threshold granularity is high and the decision making time factor is short, and the information is context sensitive. It is essential for accountability that organisations in these domains ensure transactions identified as suspected non-compliant events are scrutinised and substantiated. This will assist in minimising false positive conclusions that may result because of the speed, volume and increased complexity of the transactions, and the information used to analyse them. The construct also addresses some of the problems highlighted by Clarke (1988), that electronic monitoring of data, related to individuals and groups of individuals is subject to inherent dangers of drawing conclusions resulting from this data, may result in misleading conclusions.

A CV team infrastructure support KMS is discussed. It includes aspects of information systems, cognitive sciences, decision support and auditing judgment. Fuzzy set theory is used as a more appropriate technique in decision environments where there may be a high degree of uncertainty and ambiguity, and caters for qualitative and quantitative evidence validating and assuring the assertion of non-compliance.

Current research efforts in surveillance systems (UCD, 2001, SRI, 2001, Schneier B. 2001 for example), still concentrate on improving the accuracy, efficiency and responsiveness of the primary monitoring systems. Whilst this is necessary, further research opportunities exist in addressing and improving the utility and effectiveness of supporting the analysts responsible for evaluating the results of these primary systems and ensuring their accountability.

REFERENCES


http://www.counterpane.com/msm.html

http://www.sdl.sri.com/programs/intrusion/

http://www.csl.sri.com/research/


http://olympus.cs.ucdavis.edu/cmad/


Dr Peter Goldschmidt of the University of Western Australian has developed a Compliance Monitoring for Anomaly Detection - Decision Support System (CMAD-DS). His doctorate thesis on this subject won the 1997 International Outstanding Doctoral Dissertation Award. The software can be applied to analyse data and look for adverse trends and anomalies in a vast range of areas from military and nuclear monitoring to detecting credit card fraud and insider trading.

Since then it has been expanded as a knowledge management system for many types of data (Dataveillance Verification Knowledge Management System DV-KMS). The primary function of the knowledge management system is management of the true and false positives from the primary monitoring systems. It is an add-on to these primary systems.

One example is using DV-KMS to detect anomalies in the capital markets area. Here data is input from trading information on the stock exchange. A primary detection package would then generate a series of possible anomalies. This system would be tuned to provide few false negatives but potentially many false positives. DV-KMS would then act in a secondary role helping human agents to reduce the false positives. Typical anomalies include market manipulation and insider trading.

In June this year, Dr Goldschmidt applied for and was awarded a COMET Grant (Commercialising Emerging Technology), an initiative of the Commonwealth Government to assist the commercialisation of Australian technology. Further information on COMET is available on www.ausindustry.gov.au/comet.

Dataveillance Verification Technology (DVV) Pty, Ltd., holds all intellectual property rights to the CV-KMS business process methods and the DV-KMS system, the former entitled 'Compliance Monitoring for Anomaly Detection-CMAD'. An Australian provisional patent No. PP9615, and Patent Cooperative Treaty International Application No. PCT AU00/00295 10 + countries, covers this IP.

Compliance Monitoring for Anomaly Detection - CMAD - coined by P. Goldschmidt in 1995 has no relationship or affiliation with Computer Misuse and Anomaly Detection previously coined by UC Davis.
Stateful Intrusion Detection System (SIDS)

Arunabha Sen and Senthilkumar Krishnamurthy

Department of Computer Science and Engineering
Arizona State University

ABSTRACT

As more and more organizations rely on Internet for communication and e-commerce, the need to protect the integrity of the network and to ensure information security has become one of paramount importance. The Intrusion Detection Systems currently available use a stateless approach in which network traffic is analyzed on a packet-by-packet basis for detecting intrusion. This paper describes an architecture and framework for a Network-base intrusion detection system, which is both stateful and distributed. The proposed intrusion detection system can detect distributed attacks for which the attack pattern is spread across multiple packets, in addition to detecting all the attacks that a stateless intrusion detection system can. This system can also detect a collaborative intrusion where the attacker uses more than one network host for launching an attack. A working model of the proposed system has been developed and experimental validation of the system has been presented.

Keywords: Security, Intrusion Detection, Stateful IDS, Network attacks, DOS

INTRODUCTION

In the past decade, the Internet has grown from a fledgling network of computers to a multi million-dollar industry. With everyone interconnected, the problem of information security has assumed very high importance. The study of providing security in a network of computers has gained momentum in today’s computer dominated society (Mukherjee et al. 1994, Walter et al. 1989). The conventional approach to ensuring security is to build an Intrusion Detection System (IDS). IDS are based on the theory that an intruders behavior will be significantly different from the normal user’s behavior and that these unauthorized actions are detectable.

There are numerous approach to intrusion detection such as Neural networks, intrusion detection using system calls (Helmer et al. 1998), distributed host-based systems (Snapp et al. 1991), rule-based system (Nuansri et al. 1999), anomaly-based system (Helman et al. 1992), autonomous agents (Balasubramaniyan et al. 1998) and approaches based on genetic algorithms and artificial intelligence (Ilgun et al. 1993). A survey of intrusion detection system can be found in (Porras et al. 1992).

The prototype described and developed in this research is a Network based Stateful Intrusion Detection System (SIDS), which is deployed in a distributed environment. A network based IDS detects intrusion by monitoring network traffic on the wire to find specific signatures or patterns that would constitute an attack. A Stateful IDS can be defined as a packet filtering and analyzing mechanism which makes a decision on whether the security of a network is breached by analyzing information contained in the current packet and information from previous packets. In addition to detecting those attacks, which stateless IDS can detect, this system can also detect those attacks, which are launched from more than one host and those attacks that spans across multiple packets. A working system, which implements SIDS, is developed and tested.
This paper is organized as follows: Section 2 describes the key component of SIDS, viz., Statefulness and Distributedness. Section 3 describes the architecture of SIDS, the system design and its functionality. Section 4 presents the conclusion and future extensions possible for the system.

THE CONCEPT OF STATEFUL IDS

A stateful approach for building an IDS offers significant advantages over a stateless IDS. Stateless IDS enforce security by analyzing traffic on a packet-by-packet basis. A breach of security is detected by examining the information carried in a packet such as source address, destination address, source port, destination port and the protocol used. There are many scenarios where an attack is carried out as a sequence of steps that spans across multiple packets. Even though all individual packets look innocuous and may comply with access rules specified by the security policy, the contents of these packets when taken together may indicate a prelude to an oncoming attack. Such attacks cannot be detected by stateless IDS that operate on a packet-by-packet basis.

By contrast, a Stateful IDS can detect such attacks. They can maintain state information about the packets and use them in deducing attacks. Information about the current packet is stored in a session table for a specific time window. Using this table, the IDS can build a context based on contents of many packets and analyze this context against the access rules specific to the security policy.

Almost all the IDS available commercially follow a stateless approach. There are quite a few stateful firewalls available, but not stateful IDS. A possible reason for this could be performance. There is a processing overhead involved in the stateful IDS, as there is a need to maintain state information about every packet and a comparison needs to be made between the current packet and all previous packets. There is second round of parsing involved to build a context from related packets, which is essential for detecting intrusions. But this overhead is offset by the enhanced security offered by the IDS, which can detect distributed multi-stage attacks that cannot be detected using a stateless IDS.

Distributedness

The Stateful intrusion detection system employs a distributed architecture. In a network configuration that consists of many subnets, a sensor is plugged into each subnet to tap the network traffic in that subnet. A detection engine is deployed for each subnet to analyze the packets captured by the sensor in that subnet. Each detection engine operates independently from the other in detecting intrusions and concentrates on detecting intrusions onto a target machine in that subnet only. Each engine maintains a database that gives information about offending hosts that have already launched an attack. New filter rules are dynamically generated to detect packets from any of these offending hosts. Any packet matching these filters is immediately reported to the security personnel.

The detection engines share information about the attacks they detect with each other to increase the overall security of the network. When a detection engine finds an intrusion it sends a formatted message to all the other engines giving information about the attack detected, the pattern used to detect the attack and information about the offending host or hosts. The detection engines then update their database to include the attack detected.

SIDS ARCHITECTURE AND SYSTEM DESIGN

This paper concentrates on security related issues in a single broadcast domain, such as Ethernet. The packet sniffing software used in the research operates efficiently at 10 MB networks. The software can be used for sniffing packets from a 100 MB LAN too. However, the performance of the software would degrade if the load on the network increases and it would start dropping packets.
Network based IDS are server platform independent (Heberlein et al. 1990, Vigna et al. 1998). The system’s operating environment and the setting in which SIDS is deployed, is outlined in Figure 1. The target network, which needs to be protected from attack, consists of a number of host computers (including devices such as file servers, printers, name servers, etc.) and a LAN through which the hosts are inter-connected. The LAN is assumed to employ a broadcast medium, such as Ethernet, and all packets transmitted over the LAN are potentially available to any device connected to the network. The LAN is also assumed to be physically secure, in the sense that an attacker will not be able to directly access the network hardware such as the connecting medium and the network interface at each host. The LAN is connected to the outside world through one or more gateways. The system security personnel when configuring the SIDS would have to define the list of hosts in the LAN that needs to be protected. The list is stored as a configuration file network.conf and is used by the rules generator to build filters. Only those machines listed in network.conf would be protected from intrusion. The security personnel would also need to define the locations of SIDSs running in other subnets. The SIDS, in order to communicate with other SIDSs, to make them more distributed, uses this information.

System Design

The SIDS architecture follows the traditional sensor based architecture where one of the target machines is dedicated to run the sensor and the detection engine. The SIDS is developed on a SUN SPARC Workstation running Solaris 2.7. It consists of six components — sensor, parser, analyzer, archive daemon, logger daemon and the web interface daemon. All the components are modular and can be modified independently without affecting the system, as long as the interfaces between the modules are maintained.

Sensor

One of the target machines in the network is dedicated to run the sensor. The network interface of this machine is configured in promiscuous mode and the packets are captured using lipcap-0.4 module. It provides a system-independent API for user-level packet capture and low level framework for network monitoring. The SIDS is kick started by running the sensor daemon. The sensor daemon requires root privilege to sniff packets. It uses tcpdump to capture packets from the network. Tcpdump uses the file network.conf to filter only those packets that are either originating from or destined to hosts that need to be protected.
The SIDS defines a time-window for which the state information should be maintained. The time-window has been fixed at 120 seconds after experimenting with prototypes. This value is configurable by the security personnel and depends on the number of hosts in the protected domain, the traffic load on the network and service access pattern. The sensor process forks to create a child process. The child process executes tcpdump, using network.conf to filter packets and writes all packets to a log file. The parent process 'sleeps' for the time-window of 120 seconds and then kills the child process which has 'exec'ed a tcpdump process. Thus in effect, the child process collects log files for duration of 120 seconds.

Detection Engine

The detection engine consists of two components – the parser and the analyzer. The packet log created by the sensor is passed as input to the detection engine. The detection engine parses the information and analyzes it to find intrusions. The engine has to finish the analysis before the time-window expires, as another packet log would arrive at the end of the current time window.

The parser component parses the packet log created by sensor and extracts all relevant information from the packet and stores them in a file. The parser is run in two phases. The first phase extracts information from the packet log and the second phase organizes the information into groups of related connection sessions. The following information is extracted from the packet header by the first phase of the parser.

- Source address
- Destination address
- Source port
- Destination port
- Sequence number of the packet
- Acknowledgement number of the packet
- Time to Live (TTL) value of the packet
- TCP Flags (SYN, FIN, ACK, PSH, URG)

The information extracted is stored onto a flat file and passed as input to the component which implements the second phase of the parser. This component organizes the information into groups of packets belonging to the same session. Sorting the input file based on the source address, source port, and destination address and destination port fields does this. After the sorting, duplicate packets, i.e., packets with the same four connection identifiers, are eliminated. Count of the number of packets with same connection identifiers is calculated and stored in another file. This file forms the basis for the analyzer component that detects the intrusion.

There are two phases to the analyzer component. The first phase of the analyzer involves detecting all the stateless attacks by looking at the protocol headers. In the second phase, all stateful attacks, which are spread across multiple packets, are detected by analyzing the state information collected by the parser.

Defining a filter rule for each well-known attack identifies the stateless attacks. The tcpdump program defines the syntax of the filters. The signatures for all these attacks are given out by the Center for Emergency Response Team (CERT) as security advisories. All the stateless attacks can be detected by analyzing the protocol headers. Applying the filter rules sequentially on the binary packet log created using tcpdump by the sensor component can detect the attack. Tcpdump is again used to run the filters on the packet log:

```
tcpdump -r <log-file> -F <filter-file> -w <filter-output>
```
This is done for each filter file. If any of the output file of tcpdump, <filter-output>, is non-empty, then one or more packets in the log file has passed the filter rule, indicating an attempt at intrusion. This incidence of attack is recorded and the incident handling subsystem is invoked to handle this attack. The incident is also mailed to the security personnel and posted onto the web page.

The second phase of the analyzer tries to detect stateful attacks that are spread across multiple packets. As of the current implementation, 9 attacks have been identified and could be detected by maintaining state information. A separate module has been coded for each attack. Each module takes as input, the packet log generated by the sensor. They all operate by extracting information from the packet log and maintaining the state. This information is then analyzed to detect attacks. Following is an example of an attacks that can be detected using SIDS.

**Loki Information Tunneling attack**

Loki is an information tunneling attack in which arbitrary information files and commands can be transferred through a firewall to a target host using the payload of ICMP echo traffic. The exploit requires that a loki server be running in the target host, with root permissions, inside the protected network.

Once the server has been installed, the loki daemon listens for ICMP echo requests. If the target host receives an ICMP echo request, the daemon grabs the packet and processes the contents of the data payload. If the echo request was sent from a loki client, then the loki server executes the commands sent in the payload. Any data resulting from the execution of the commands is sent back to the client in the guise of echo replies.

**Detecting Loki attack using SIDS**

The main principle behind loki attack detection using SIDS is that, when ICMP echo packets are used to carry the covert channel, there will be one echo request coming in into the target host, followed by more than one echo reply to the attacker. By maintaining the state information about the packets for the current time window, the SIDS can detect loki attack by looking out for ICMP echo requests for which there is more than one ICMP echo reply.

The loki attack detection module extracts all ICMP traffic from the packet log generated by sensor, using tcpdump icmp filter. This data is sorted to group all packets from the same source address and port together. Then the module finds out the number of echo requests and echo replies sent by each source address, port pair to a destination address, port pair. If the replies are greater than the number of requests, the SIDS concludes that these packets are part of a loki information tunneling session and reports the incident to the security personnel.

Loki attack cannot be detected by intrusion detection systems that analyze traffic on a packet-by-packet basis. All they see is that a particular packet is an ICMP echo request or echo reply. They have no way of knowing if there are more than one reply for a request without maintaining state information.

**Archive and Web Interface Daemons**

Archive daemon runs in the background and is invoked every one hour as a ‘cronjob’. It ‘tars’ all log file collected in the previous one hour, compresses them and stores them in an archived directory. All log files other than the compressed file are erased from the disk to save space. The SIDS is bundled along with an Apache Web Server that sets up a home page for the system. The web page acts as a point of notifying alerts and also for analyzing the packet log manually. The web page primarily displays alerts detected on the current day, alerts detected previously for one month, the complete packet log file derived in ASCII format using tcpdump, a summary of network traffic for each time window and statistics about number of host scans and number of port scans.
Incident Handling

An incident can be defined as an instance of a successful attack that is detected by the intrusion detection system. Reacting to the incident is as equally important as detecting an attack. After a successful detection of an attack, the reaction to the attack is two phased. The system first has to bring the incident to the notice of the security personnel and then respond to the incident according to pre-configured semantics. The primary means by which SIDS notifies the security personnel of an attack are Email and Web alarms. The SIDS includes an Incidence Response Subsystem, which is tasked with the damage-control exercise in a post-attack scenario. Typical responses include, tearing down an offending connection by resetting it, logging off the offending user or in a very severe attack, shutting down the gateway to disconnect the protected network from the outside world. The response subsystem is effective only if the source address of the offending host is not spoofed, except in few cases such as TCP SYN flooding, where even spoofed IP addresses can be handled.

CONCLUSION

In this research work, an architecture and a toolkit for an intrusion detection system that follows a stateful approach has been presented and tested. The proposed intrusion detection system (SIDS) is a network-based IDS which can operate both independently and in collaboration with other SIDSs protecting different networks. The proposed intrusion detection system detects intrusion by analyzing information from the current packets and from information from the previous packets. Thus it can search for patterns based on context spread across multiple packets and is more efficient and responsive. The proposed system maintains a time-window for which the state information is collected. This time-window is fixed at 120 seconds. The value can be configured according to the traffic load and the number of machines in the network.

In addition to those attacks that the conventional stateless intrusion detection systems can detect, the proposed system can detect a set of additional attacks, which are characterized by the fact that the attack pattern for these attacks is spread across multiple packets. These attacks include, Trinoo Distributed Denial of Service attack, SYN attack, Teardrop attack, Loki information tunneling attack, FTP bounce attack, Network mapping attack, TCP/IP Stack Fingerprinting attack, TCP Stealth host scanning using SYN packets and Port scanning using Nmap. The existing defense for these attacks is weak and inefficient. They operate under the premise that security assumes higher priority over availability of certain services, the vulnerabilities of which are exploited by these attacks. So, these services are shutdown and made unavailable to everyone, including legitimate users.

Current limitations of the proposed system include all the limitations common to network-based intrusion detection systems. These limitations include encryption, high-speed networks and switched networks. As technology grows, these limitations are expected to be solved. However, a combination of network-based intrusion detection and host-based intrusion detection would work better in such environments.
REFERENCES


Denial of Service and Protection of Critical Infrastructure

Helen L. Armstrong

School of Information Systems
Curtin University
GPO Box U1987,
Perth, Western Australia 6845
Email: H.Armstrong@curtin.edu.au

ABSTRACT

Denial of service attacks generate massive volumes of illegitimate traffic and utilize system resources in a way that renders the system inoperable, thus denying access to authorised personnel. Denial of service attacks can be projected against systems controlling critical information infrastructure and have the potential to be an effective weapon in cyberwarfare. This paper explains the concept of a denial of service attack, discusses the different methods of achieving denial of service and looks at the impact this type of attack may have on critical infrastructure. Although there are no fail-safe ways to protect against denial of service attacks, several means of minimising damage to information systems are discussed.

Keywords: Denial of service, distributed denial of service, critical infrastructure, cyberwarfare, security

INTRODUCTION

In many countries across the globe the systems used to manage and operate service industries are controlled by computer networks. Electricity, gas, water, sewerage treatment and other services are highly automated and computerised. These systems, in addition to banking, defense, government, telecommunications and transportation systems form part of a society’s critical information infrastructure.

Denial of service (DoS) attacks on information systems controlling such critical infrastructure can be devastating for a nation. Computer networks offer a cheap and fast means of projecting warfare – information warfare. It has been forecast that electronic and computer weapons will increasingly be used to destroy an adversary’s information infrastructure, and thus their economic power, in the 21st century (Boni & Kovacich, 2000, p 209). Why send an army to physically fight when a distributed denial of service (DDoS) attack on numerous key information systems could cripple an entire nation.

CSI (2000b) reports in December 1998 the Chinese military at the Communication Command Academy in Wuhan staged its first infowar simulation exercise. Thirty-one courses in information warfare were also run for Chinese military personnel. The international JWID (joint warrior interoperability demonstration) exercises involving the USA, Canada, UK, Australia, New Zealand and NATO annually engage in cyberwarfare exercises (see http://www.defence.gov.au/jwid/1999/menu.html). DoS tools are part of the information warrior’s arsenal, and can be used for both offensive and defensive action.

This paper aims to present an overview of DoS attack methods. Various types of denial of service attacks on computer systems are explained and the impact of denial of service attacks on critical infrastructure is discussed. Methods of limiting vulnerability to this type of attack are discussed in the final section.
RECENT DENIAL OF SERVICE ATTACKS

DoS attacks are an effective means of attacking information systems of a competitor or opponent in both military and business environments. With organizations becoming increasingly reliant upon information systems for day-to-day operations on core systems, denying access to such systems can result in a range of outcomes, from frustrating to devastating, for the victim organization. The CSI/FBI Computer Crime and Security Study (CSI/FBI, 2001) reports denial of service attacks rose from 60% in 2000 to 78% in 2001 for those participating organizations acknowledging Internet abuse.

In February 2000 a distributed denial of service attack was launched upon the web sites of Yahoo!, eBay, Amazon.com, Buy.com, CNN.com, E*Trade, Excite and ZDNet.com. Web sites ground to a halt as they attempted to handle all the requests that were bombarded from unknowing hosts. It is estimated that these web sites suffered losses of US $1.2 billion (Denning, 2000b). In a list of recent cybercrime events in the same article Denning also reports that the number of cyberattacks and unauthorized intrusions into US Department of Defense systems rose from 5,844 in 1998 to 22,144 in 1999. In a keynote address at the InfoWar Con 2001 in Washington in September, Major General David Bryant stated attacks on US Department of Defence computer sites doubled over the 2000-2001 period (Bryant, 2001). In early May 2001 the White House web site was hit by a DoS. The CERT/CC (Computer Emergency Response Team/ Coordination Center) was hit by a DDoS attack for three days later in May. Due to the distributed nature of these attacks and the spoofing of IP addresses the legitimate source of the attacks is not known.

The threats of disruption and destruction of information and communications related to critical infrastructure are areas of concern highlighted in the report on cyber threats and information security undertaken by the Center for Strategic and International Studies in the USA. This report states that the probability of the threat of disruption materializing is considerable, as the tools needed to create disruptive viruses and DoS attacks are rudimentary and pervasive (de Borchgrave, Cilluffo, Cardash & Ledgerwood, 2001; page XVII). These tools are also readily available on the Internet.

WHAT IS DENIAL OF SERVICE?

In the context of this discussion, denial of service is denying authorized access to a service provided via a computer network. Denial of service can result from errors and unintentional actions such as bugs in software and poor coding, as well as intentional acts of abuse. A denial of service attack is an intentional act designed to degrade the computing or communications service or bring it to a halt, thus denying access by authorised users (Garfinkel & Spafford, 1997; Ghosh, 1998; Stallings, 2000; Wadlow, 2000).

Denial of service attacks are particularly difficult to defend against because they exploit weaknesses or flaws in operating systems, network interface software and Internet protocols. Each attack may have a specific target: for example, a perpetrator may suppress or re-route all messages directed to a particular destination, or the aim may be the disruption of an entire network, either by disabling the network via a known weakness or by overloading it with messages to degrade performance.

DoS can also occur from inadvertently activated bugs in Internet browsers by allocating gigabytes of memory and causing the browser to crash the system. For example, there is a bug in the Netscape Navigator HTML layout engine that can be used to allocate gigabytes of memory in Navigator versions 1, 2 and 3 (Garfinkel & Spafford, 1997). Although there is a patch available, this vulnerability joins a long list of potential tools for attack. Known vulnerabilities in operating systems and network software can be harnessed to perform denial of service attacks. For example, Costello (2001) discusses the potential for increased DoS attacks from Unix Sockets in Windows XP, Microsoft’s new operating system.
A distributed denial of service attack occurs when DoS software is installed on a number of servers, and these servers unwittingly attack a target server. Tools such as TFN – Tribe Flood Network, trinoo and Stacheldraht, allow remote projection of denial of service attacks from hundreds of servers. Infected systems execute the denial of service attack when triggered by the infected host. Figure 1 illustrates how a distributed denial of service attack works.

Using well-known vulnerabilities in operating systems, the perpetrator hacks into the network of an organization or university and installs a ‘daemon’ on unsuspecting hosts or ‘masters’. The servers attached to each host then act as ‘agents’ or ‘zombies’, carrying out the attack when the daemon is activated by the attacker. The zombies generate traffic on their own network targeted at the victim’s server. The victim’s server becomes so inundated with requests that the system slows down or grinds to a halt, thus denying access to authorized users.

Information system environments that allow global resources to be allocated and do not limit the allocation of such resources will be prone to DoS attacks. Code for DoS attacks can be embedded in Java and Javascript programs, web pages or sent via email. Java and JavaScript seem to be especially sensitive to DoS attacks as they command large amounts of system resources and it is difficult for a user facing such an attack to regain control of the system (Garfinkel & Spafford, 1997).
TYPES OF DENIAL OF SERVICE ATTACKS

Internet Security Solutions (ISS) list approximately forty different types of DoS and DDoS tools or 'signatures' their software uses for identifying DoS attacks. The most common means of projecting a denial of service attack is via flooding. Flooding is the generation of spurious messages to increase traffic on the network and degrading the service to other users (Pfleeger, 1997). Examples of flooding are SYN flooding and the Ping of Death and these are discussed below. Other types of denial of service attacks briefly described include CPU and memory attacks, window multiplication, email flooding and communications re-routing.

SYN Flooding

A SYN flooding attack is the sending of a series of TCP/IP packets, each attempting to establish a TCP/IP connection from a remote source system. Activating a TCP/IP connection is a three-phased process (see Figure 2); the remote user requests a TCP/IP connection on the target machine, the target machine establishes the necessary TCP/IP buffers and sends a message back to the remote user, and the remote user sends the final handshake to complete the opening of the TCP/IP communications channel.

SYN flooding attacks will often consist of numerous requests to a target system to establish TCP/IP connections (see Figure 3). The target system allocates buffers for the requested TCP/IP connections, and these are held open awaiting the final handshake to arrive, however, the final handshake is not returned by the users requesting the connection. Thus the target system allocates all of the buffers for incoming TCP/IP requests and can accept no more, resulting in the system hanging or operating at a deathly slow pace.
The source code for launching a SYN flooding attack has been released within the underground community (daemon9 et al, 1996) in Phrack Online. Windows NT and Unix systems are prone to this type of attack.

**Ping of Death**

The 'ping' function in the TCP/IP ICMP protocol is a network testing tool that allows a machine to determine if another machine is contactable via the network. The requesting machine pings the target machine and if the request is received the target machine will acknowledge the ping request. Figure 4 illustrates the sequence of ICMP ping requests and responses.

![Figure 4: CMP Ping request and response](image)

The ping of death attack utilizes this 'ping' function by sending a huge number of ping requests to the target machine (see Figure 5). The target machine is overwhelmed by requests and as this function operates at a low level (either in the operating system kernel or the network interface) the system is unable to execute other functions whilst it is replying to the ping requests.

Microsoft Windows NT and Windows 95 are particularly susceptible to the ping of death and if not patched will also hang when sent an ICMP ping packet where the size of the packet sent does not match the size specified in the packet header.

![Figure 5: The ICMP 'ping of death' used for denial of service](image)
CPU and Memory Attacks

Javascript programs can demand too much memory or CPU resources resulting in DoS. Memory hungry code or intentional coding of infinite loops will cause the system to hang or crash. Internet browsers executing JavaScript code use the same thread that is used to handle events from the user, hence the system is unable to execute other user requests. In addition, Netscape Navigator and Internet Explorer do not allow a user to stop the execution of a running Java or JavaScript program, and the user must either exit the browser, turn off the browser or turn off the machine. This type of denial of service may not be catastrophic on a one-off occurrence, however multiple attacks on core systems could cause an organization’s system to crash.

Window Multiplication

Java and JavaScript downloaded from web browsers can create windows on the user’s system. These are used extensively for advertising banners and product sales windows. The window multiplication is activated by the user clicking on the close box icon of the first window displayed, resulting in the first window disappearing, however this window is immediately replaced by two other windows. As each window is closed two more windows are opened. The only way to stop the process is to exit the browser. This technique is used to present images of goods for sale or sexually explicit pictures. An example of this type of code can be found at http://www.digicrime.com (Garfinkel & Spafford, 1997, page 61).

Email Flooding

Email flooding of a competitor’s system is easy to arrange. By placing the competitor’s email on a large number of email distribution lists and subscribing the victim person or organization to large listservs will result in the competitor’s email system being flooded with email messages. This can be difficult to trace as the perpetrator can use an anonymizer remailer or spoof the source address.

Re-routing and Blocking Communications

Connectivity denial of service is the failure of a critical path or node in the network, resulting in blocked communications. Modification of routing tables can establish one host as the closest host on the network and either disable all communications, disable communications to a given host or route communications to an unauthorized user (Pfleeger, 1997). Altering routing tables can cause bottlenecks in given parts of the network or bring the network down entirely. Attackers can hack switches, eavesdrop and hijack sessions and change router addresses using tools such as Ethereal, Dsniff, Linsniff and Fragrouter.

Misuse of Network Management Software

A program called a ‘ping sweep’ can be used to scan a network to gather information about other machines on the network (Wadlow, 2000; Zwicky, Cooper & Chapman, 2000). Other network mapping software tools are available on the Internet, allowing unauthorized parties to determine other machines available on the network for further investigation and attack (for example, Nmap, WhatsUp Gold, NetRecon, Web Trends). Network scanning tools (such as SATAN, SAINT, Internet Scanner) can then determine vulnerabilities in the network. A dissident with a mission can download DDoS software from a number of hacker web sites and install the software on unsuspecting machines within the network, activating a denial of service attack remotely at the desired time.
DENIAL OF SERVICE ON CRITICAL INFRASTRUCTURE

In 1997 the US Department of Defense and NSA conducted an unannounced exercise called Eligible Receiver. The NSA hired 35 hackers to hack computerized critical infrastructure systems in the USA to determine the level of vulnerabilities. The exercise found that the power grid, emergency 911 systems and Defense networks had weaknesses that could be exploited by an adversary using only publicly available tools from the Internet (CNN, 1999; Denning, 2000b). CNN also report in the same article that in 1999 hackers took control of a British military communication satellite and demanded money in return for control of the satellite. It also reports a co-ordinated attack was projected at US Air Intelligence Agency computers with part of the attack being sourced to Russia. The recent attacks by Chinese hackers on US computer systems were designed to plant viruses, thus destroying data and denying services to authorized users.

The vulnerability of critical infrastructure is constantly reinforced by regular media reports. Intruders hijacked a US electric company's servers and used the systems to host and play games (CSI, 2001). In May, 2000 a hacker altered parameters on sewage pump stations causing raw sewage to overflow on the Australian Sunshine Coast in Queensland (CSI, 2000a). Denial of service can result from errors and unintentional acts, and the loss of power or errors in control systems pose the greatest concerns for systems managing critical infrastructure. The severing of power and communications cables by farmers, rodents and oblivious workmen frequently result in extended power and phone blackouts and failure of air traffic control systems. In October 2000 air traffic control radar systems failed for four hours, resulting in airports throughout the USA being gridlocked with grounded aircraft (CSI, 2000c).

Warnings of denial of service attacks on critical infrastructure have arisen from numerous sources (Denning, 2000a; Ghosh, 1998; Weil, 1998). Approximately 120 countries or groups have developed, or are in the process of developing information warfare systems according to a report by the US Government Accounting Office (CNN, 1999). Many governments and nations have established departments or services for the protection of critical infrastructure (for example see Becker, 1999). The non-availability of critical services such as power, emergency services, communications, water, etc. through a DDoS could cause damage to services, damage to infrastructure, severe economic damage or even loss of life. Attacks on critical infrastructure resulting in non-availability of crucial services can be used as isolated means of protest or acts of political or military warfare.

Governments need to establish mechanisms for determining when such attacks against military as well as non-military targets represent an act of war and be able to respond accordingly. The Pentagon has established a warning system for cyberwarfare attack, known as Info-Con or Information Conditions warnings based upon US military Defense Conditions, or Def-Cons. (ABC, 2001). This system is designed to alert authorities to subversive cyber activity and promote military readiness to react to threats of information warfare attack. This type of warning system appears more appropriate to military environments where preparedness for attack is highly desirable and defensive mechanisms can be quickly implemented. However, if protective mechanisms are not already in place in a civilian computing environment, then reactive measures against DoS attacks can do little to protect the system.

Many believe that hackers are the main offenders in the cyberwarfare arena. For example, hackers gained access to California's primary electric power grid operating computer and remained undetected for seventeen days (Verton, 2001). Although the potential vulnerabilities associated with these grids are well documented and have been known for years it is not believed that hackers have sufficient knowledge of the systems to pose a real threat. Many sources claim that the threat of massive cyberwarfare by hackers is low for a number of reasons. First, hackers do not have the expertise to penetrate systems that control critical infrastructure to the level of denying services. Secondly, hackers individually have insufficient incentive to wage war and the majority do not wish to cause harm to society and finally, hackers generally do not have the mindset of organized criminals and terrorists.
It is the author’s view the main threat of cyberwarfare will emanate from organized crime and
dissident groups rather than hackers. It will result from political groups or nations using cybertools
like DDoS assaults to attack their opponent’s systems as an alternate or additional means of waging
war.

PROTECTING AGAINST DENIAL OF SERVICE

There is no known way at present to fully protect information systems from denial of service attacks. As previously mentioned, this type of attack utilizes shortcomings and opportunities in operating
system and network software. Blocking packets from the attacking hosts is not effective as the
perpetrators spoof their IP addresses and attacks can be launched from connected systems owned by
legitimate business partners. It is difficult to trace the original source of DoS and DDoS attacks as the
counterfeit IP addresses ensure anonymity. Organizations must protect their systems as best they can
until a more effective means of protection is devised.

Forums of experts have met in an effort to formulate a solution to the denial of service attack problem, but no fail-safe solutions have been forthcoming. However, there are a number of measures that
organizations can implement to reduce the risk and damage of DDoS attacks including removing
critical information systems from public networks, limiting system resources, installing patches and
configuring firewalls and intrusion detection systems to more comprehensively identify known
vulnerabilities, and establishing effective security incident response programs and contingency
planning.

Removing Critical Systems from Public Networks

The need for information systems controlling critical infrastructure to be connected to the Internet
should be reviewed and the connection requirements substantiated. The CSIS report on cyber threats
states “the Internet, by its very nature, is and likely will remain an unstable, immature, and insecure
technology, open to abuse and exploitation” (de Borchgrave et al., 2001; p XVII). Critical systems
must be isolated to ensure their safety. Where such systems must upload and download data via hosts
on public networks then connection times must be limited, true proxy servers and demilitarized zones
implemented with all transactions and packet contents scrutinized and closely monitored.

Limiting System Resources

The amount of system resources allocated to functions can be limited via operating system and web
browser features. Software manufacturers generally set the limits for resources at a high level to allow
maximum connectivity and usage. To protect from denial of service attacks it is recommended that
organizations identify critical or limited resources and monitor their usage. For example, Stein (1998)
recommends settings should be altered to lower the maximum number of connections allowed (the
default is usually around 100,000 connections), set a limited time to hold connections open (the default
connection timeout is 15 minutes), set a lower limit for memory usage, lower the number of files the
system can open simultaneously, set a lower limit for the number of child processes it can spawn and
limit the amount of CPU time used.

Patches, Firewalls and Intrusion Detection Systems

The majority of attacks occur on systems where known vulnerabilities have not been patched. It is
important therefore to apply the patches provided for SYN flooding and ICMP ping attacks, and other
operating system vulnerabilities.

Installing a firewall will not remove the risk of DoS attacks, however firewalls can be configured to
filter forged or malformed requests before they reach the server (Zwicky et al, 2000). Firewalls can
also be configured to limit services available to avoid monopolization of a resource.
Implement intrusion detection systems to identify the signatures of attacks in real time and send out an alarm or activate protection mechanisms. Unfortunately, there are tools available that bypass firewalls and intrusion detection systems (for example Fragrouter and Firewalk) by breaking down TCP or UDP packets allowing these packets to get through firewall filters as well as gather information about the network behind.

As previously mentioned, denial of service attacks use spoofed IP addresses. Agents and Masters in a distributed denial of service attack commonly spoof their legitimate IP address so they cannot be easily traced. This means that internal firewalls can be configured to identify and block outgoing DoS attack packets that have IP addresses outside the organisation's or ISP's network domain. This will stop attacks at their source.

Security Incident Handling and Contingency Planning

It is imperative that organizations establish good security incident handling procedures. Guidelines for identifying security incidents, reporting of incidents and procedures for minimizing damage and reacting to intrusions are essential components. Procedures for bringing systems down in the wake of an attack must be detailed, including guidelines covering who has the right to sever connections, under what circumstances, and for how long.

In the event of an attack, good contingency planning is necessary for an organization to be able to recover quickly and effectively. Reliable backups and tested procedures are crucial for fast recovery. Educating personnel in the identification and handling of crises will assist.

Change Culture surrounding Security in System Design

Unfortunately, systems are not designed with security as a prime feature and protective mechanisms are still add-ons. Factors that drive the design of new computers are speed, reliability, ease of accessibility and breadth of features in an effort to increase market share and profit margins. Security is not high on the manufacturer's list of desirable features as security restricts accessibility and speed and limits available features. Dittrich (1999) claims that network builders must choose only two of the following three desirable factors – fast, reliable, secure. The CERT/CC workshop at Carnegie Mellon University on distributed systems intruder tools reports that 'the tools and attacks demonstrate that a network that optimizes its technology for speed and reliability at the expense of security may experience neither speed nor reliability, as intruders abuse the network or deny its services' (CERT/CC, 1999; p 20). While security remains low on the list of desirable features, opportunities for abuse will continue to abound. A change of culture is needed to raise the profile of security in system hardware and software design.

CONCLUSION

DoS attacks are designed to halt systems and deny access to authorised users. DoS attacks can be achieved in a number of ways including flooding, reconfiguring systems and excessive resource utilisation. Incidents of DoS attacks on systems connected to public networks continue to be reported. The insecurity of operating systems, software development tools, network and communications tools and protocols and availability of DoS software on the Internet will ensure attacks of this nature will continue to rise.

When projected against critical information infrastructure, DoS attacks can be used as offensive weapons of information warfare. Private citizens stand to lose the most from both military and non-military acts of traditional warfare and information warfare targets. Not only can DoS attacks produce substantial economic losses and physical hardship, but they also threaten the underlying fabric of public confidence. Random and continuous DoS attacks may result in increased military alertness, but may also cause financial losses to organizations and individuals thus eroding economic stability. They
may also cause disruption to communications, emergency and public services, thus jeopardizing individual well-being. Furthermore, sustained asynchronous DoS and DDoS attacks that debilitate a nation may result in erosion of confidence in public and private-sector institutions established to ensure public well-being and safety.

There are no fail-safe means of stopping DoS attacks, however, there are some measures organizations can put in place to minimize the damage. The aim of DoS attacks is to deny access to services. In the absence of effective protective mechanisms, the only solution may be to pull the plug and bring down those computer systems under attack. Either way, access to services are denied thus achieving the attacker’s aim.

At this point in time our stance is still reactive. While the design of computer and communications systems concentrates upon speed, reliability and accessibility at the cost of security, networks will not be able to protect against abusive actions such as denial of service. A proactive, holistic approach is necessary to build comprehensive protection mechanisms to ensure robustness and continuity of access to vital information and systems. We still have a long way to go.

REFERENCES


Culture And Sensemaking In Information Warfare

Jill Slay

Advanced Computing Research Centre
School of Computer and Information Science
University of South Australia
Email: Jill.Slay@unisa.edu.au

ABSTRACT

This paper examines military Command and Control (C2) systems as complex distributed information systems, using Kline's multidisciplinary perspectives and soft system methodologies. It contends that culture, which is viewed from both an organisational and an anthropological perspective, is an important system variable and argues that the application of models and theories from anthropology can be helpful in the understanding of the development of shared meaning and sense making within such a system. This analysis provides a means by which collaboration in C2 can be developed in the cross-cultural information warfare that is a by-product of the Revolution of Military Affairs.

Keywords: Information warfare, Information operations, culture.

INTRODUCTION

This paper examines Information Warfare as one aspect of the military Information Operations that are now a part of War, Anti-War and Operations Other Than War and Anti-War (OOTWAW). It takes the US Department of Defence definition of Information Operations as a working definition of Information Warfare in a military context:

'Information Operations (IO) involve actions taken to affect adversary information and information systems while defending one's own information and information systems.' (DOD, 1998)

However, since all parts of society has become increasingly dependent on the development of large and complex systems, and with moves towards global competition in many spheres, information warfare takes place in many contexts including business-business and government and-government ones. Therefore, hypotheses raised here can be equally applied, to e-commerce, e-government and e-education scenarios.
COMMAND AND CONTROL RESEARCH

Command and Control research is focused on the use of communications and computer systems in a military context with the aim being develop appropriate technology and methodologies to allow all kinds of warfare to be won.

Researchers see their practice as an art, which depends on many factors including operational culture and individual leadership styles, as well as information theory and systems engineering, and so draw on various paradigms for the understanding of their own discipline and advancing their body of knowledge.

Part of the issue they face is the need to understand how a historically hierarchical form of leadership and management, which now depends heavily on network-based information systems, can operate in an environment where technical skills and expertise now reside much lower down the chain-of-command. This situation is also made more complicated by the move towards joint and coalition operations that raise the need to deal with complex organizational and national cultural barriers.

RESEARCH IN CULTURE AND INFORMATION SYSTEMS

The research questions being asked here are ‘what is the role of culture in effective C2 systems? How can the systems be modelled to show the effect of culture? How can these models be used to shape organisational and operational decision-making’.

The research objective here is to first develop an informal model of the role of culture in such complex distributed systems and, from thence, to develop a formal understanding. Once the role and effects of culture are clarified, it becomes easier to ask questions about effective collaboration (‘how shall we make sense of each other as we work together?) and system security (how can we work out how our competitor/opponent may react in these circumstances?).

Soft Systems Methodologies

The use of soft systems methodologies allow us to identify internet-mediated distributed systems as complex socio-technical systems since they can be idealised as open systems which depend on the technology, the sentiments of the members, and the organisational environment (Checkland, 1981). Although the system is organised to focus on a primary task (military communications) this cannot be separated from the environment and the social factors, including cultural ones.

Checkland also notes that a reasonable method for gaining an understanding of such a system is to produce an overview of the system from several perspectives. It allows us to incorporate subjective and objective impressions of the system into a bricolage, a rich picture, which allows us to include the human agents, the problems, conflicts and other seemingly ‘soft’ aspects of the system so as to determine the areas, which need improvement. Formalisation of these conceptual models allows for solution of the problems within the system.

Issues of complexity force us to turn to Kline (1995) who also gives us an understanding of how to derive credible perspectives on the complex system under examination. He maintains that three foundational perspectives of a multifaceted and hierarchical system are a synoptic, a piecewise and a structural perspective.

A structural view is one that provides details of how a particular system fits together within its hierarchy and provides information on the relationship between local and global effects within the system.

A piecewise view is one that looks at the smallest portions of a system that might be relevant in providing information to aid in the solution of any particular problem.
A synoptic view is an overview, which extracts, synthesises and thus maps a desired property of the system.

**DEFINITIONS OF CULTURE**

Culture is a concept that is often discussed in academic literature. Before attempting an analysis of the role of culture in complex systems is important to gain a working definition from appropriate literature.

**Anthropology**

A classic definition of culture found in early anthropological literature is that it is the ‘knowledge, belief, law, morals, customs’ (Tylor, 1871), which are passed on from one generation to another within a particular society or group of people. Anthropologists of Tylor’s generation were expected to examine a ‘civilisation’ and produce a taxonomy with categories such as weapons, myths, rites, and ceremonies.

Malinowski (1948 [1922]), another early anthropologist, is famous for his ethnographic fieldwork particularly among Trobriand islanders. It had already become traditional, in his time, to rely on the written opinions of experts on specific aspects of culture such as religion or magic. However in his work, Malinowski demonstrated the study of culture as an art rather than a science, and failed in his attempts to produce anthropological and positivist scientific laws regarding culture from his collected work. He stated that he wanted to keep interpretation separate from ‘pure fact’. Malinowski’s perspective on the study of culture was that it consisted largely of identifying particular human behaviour, and interpreting the underlying beliefs causing the specific behaviour.

‘Civilisations’ and enterprises have become much more complex during the twentieth century, and anthropological concepts of culture have been applied in many fields of study, including nursing, studies of policing and factory work (Van Maanen, 1995). The definition of ‘culture’ has thus been extended, and described in many complex and diverse ways. Van Maanen comments (1995) that there is still considerable debate concerning ‘the sacred heart of ethnography, the culture concept’. Postmodernists and deconstructivists also have problems with the concept of discrete and finite cultures and an ‘incredulity towards metanarratives’ (Lyotard, 1984). Others regard the concept of culture as something left over from a colonising era (Fabian, 1983).

The definition of culture that is most commonly found in the literature of science and engineering (Cobern, 1991; Waldrip & Taylor, 1995) is that of Clifford Geertz who indicates that ‘The concept of culture I espouse ... is essentially a semiotic one. Believing .. that man is an animal suspended in webs of significance he has spun, I take culture to be those webs, and the analysis of it to be therefore not an experimental science in search of law but an interpretive one in search of meaning. (Geertz, 1973, p.3)
WORLD VIEW

The terms ‘worldview’ and culture are often used interchangeably. It is important to realise that, once ‘culture’ has been defined, then members of a particular cultural group will share a common worldview.

The term ‘world view’ (Cobern, 1991) has two different connotations in English. The first has a philosophical meaning and involves a person’s concepts of human existence and reality; the second is an individual’s picture of the world that he or she lives in. The term ‘world view’ as used in anthropology refers to the ‘culturally-dependent, implicit, fundamental organisations of the mind (Cobern, 1991, p.19). It therefore carries the concept of ‘sensemaking’ – if we understand a worldview then we can also understand how the people within that particular group make sense of the world around them.

Kearney’s (1984) model of worldview presumes a logical and structural integration of presuppositions within any individual and therefore the model is known as a logico-structural one. He then identifies seven logico-structural categories contained within a given individual’s worldview: The Other, Classification, Causality, Relationship, Self, Time & Space.

These categories serve as a framework for analysis of a worldview. Kearney (1984, p.65) draws the parallel between these factors of an individual worldview and the categories a doctor uses for the diagnosis of a patient’s disease. In order to determine the worldview of an individual, his or her understanding of the seven categories of Other, Self, Time & Space, etc., need to be identified and integrated to produce a picture of the complete worldview.

KLINE’S ANALYSIS OF COMPLEX SYSTEMS

Kline’s hypothesis, (Kline 1995) is that at least three views are needed for a reasonably good understanding of hierarchically structured systems with interfaces of mutual constraint: synoptic, piecewise and structural.

Structural View

Arguably, the most common type of architecture view is the structural view in which a system is depicted as a set of inter-related elements. Examples include:

- the taxonomies used by biologists to categorise forms of life;
- the high-level designs of software systems;
- the blueprints used by the architects of buildings and engineers in general;
- the master-plans used by military and business strategists to depict the inter-relationships of other subsidiary plans;
- the organisation charts used to depict the authority/responsibility structures in institutions.
Piecewise View

Another common view is the piecewise view that depicts the smallest relevant parts of a system for a particular problem. Examples include:

I. The detailed wiring diagrams produced by electronic and electrical engineers that show the smallest components of the devices with which they are concerned and the way that they are inter-connected;
II. The detailed design drawings produced by mechanical engineers that show the smallest components of the devices with which they are concerned and the way that they are inter-connected;
III. The musical scores used by composers to depict the notes to be played by the instruments in orchestras;
IV. The inventories of repositories.

Synoptic View

A less common type of architecture view is the synoptic view. Synoptic views treat systems as an atomic entities or wholes. They selectively emphasise characteristics of the system that are deemed to be salient in a given context and suppress (or omit) information that is not pertinent in these respects. Examples include:

- The synoptic weather charts used in television and newspaper weather reports.
- ‘Black-box’ system diagrams that emphasise the inputs and outputs to a system (the black-box) and the relationships between the inputs and outputs resulting from the action of that system.
- Topographical, political, climatic, demographic etc. maps.

When considering the possibilities of multicultural military operations or institutional cultures or international expansion (and thus forming a system of systems), it is important to recognise therefore that an understanding of the dominant culture of each sub-system is necessary before the beginning a military operation.

Anthropological techniques whether viewed as scientific ones, as Tyler did, or the more artistic and interpretive ones, allow for the creation of ethnography which can provide the synoptic view of a military enterprise. An understanding of the local political situation and local worldviews, from modern and historical sources, provide different perspectives on the effect of culture on the human activity system

DISCUSSION - AN APPLICATION FROM C2 SYSTEMS

In considering a situation where two countries forces are working collaboratively against a common enemy, a superficial examination will establish that cultural differences are evident. These might include differences in:

- native language
- religious beliefs
- political beliefs or systems
- philosophy (eg. Confucian or non-Confucian)
- attitudes towards gender equity
In a complex situation where personnel from two collaborative forces are using complex information systems to communicate information on battle situations to senior officers (and simultaneously protect their own information systems from external enemy intrusion), cultural complexity is a hindrance to sensemaking. It is possible therefore to use Kline’s analysis to determine the role of culture within the complex systems made up of each of the forces involved in the conflict.

**Structural View**

In considering a C2 system it is apparent that a structural view of a particular military force’s command and control would include a top level view of the elements within that force and the particular hierarchical way in which the elements relate to each other. It is possible to imagine a situation where the troops of two countries, establish a military operation in a third country. An organisation chart of each country’s force would provide the structural view of the forces.

**Piecewise View**

A piecewise view of the C2 system would give the details of the smallest relevant pieces involved in the system, including the hardware, software and human activity which comprised the system. This would give a comprehensive layout and specification of all hardware, software and staff needed to allow effective internal and external communication by the collaborative parties.

**Synoptic View**

A synoptic view, and one which emphasized the role of culture within the system, would focus on the role of culture within the system, the inputs and outputs that were affected by cultural issues. As has been stated, culture is a semiotic concept which implies that the system is dependent on the meaning which each human agent within the system gives to important features of the system. Worldview theory gives an opportunity to examine the system from the individual human operator upwards and to determine his or her particular response to:

- The Other
- Classification
- Causality
- Relationship
- Self
- Time & Space

With this understanding it is therefore possible to predict the response of an individual to a particular stimulus or change and to begin to have an understanding of the effect of this change on the system dynamics. A synoptic view that allowed only for the effect of culture might examine the differences of an individual, and thus the group within one country’s troops, in their interactions with their collaborating partner on an individual and group level and the issues that they might face in a joint operation in a third country.

If one of the forces were, for example, the Royal Australian Air force (RAAF), then the cultural aspects would involve issues derived from Australian culture (anthropologically) and RAAF culture (organisationally). So for each individual, we could derive a matrix based on worldview theory generally classified by the universals of World View theory.

World View theory uses universal ‘cognitive categories’ to describe people. These have been described above but, taking the first, Relationship, as an example, it is possible thus to use an analysis which ‘classifies’ individuals from the three countries involved and develop a series of attributes to represent the cultural factors under consideration.
In examining the concept of Relationship, one is examining the general issue of ‘how do people within this culture relate to others?’ Therefore issues to be considered include such as cultural and organisational attitudes to:

- Authority
- Leadership
- Wisdom and Age
- Male and Female communication
- Formality and Informality in communication

Examples of Relationship, with some typical indicators, that have impact on military communications and information systems include:

- Command approach
- Control free
- Selective control
- Problem bounding
- Problem solving

It is also possible to consider cultural attitudes towards Causality and examine:

- Belief systems
- Religious
- Political systems

Gathering Data to Support World View Analysis

Qualitative research, anthropological fieldwork and ethnography provide basic data that can indicate, to a researcher, basic information about the meaning that a particular cultural group assigns to a particular piece of data. An example of this is found in a particular cultural understanding of ‘time’. For Western thinkers, time is a linear variable, never repeated, while, for some from a different culture, time is non-linear and seen to be a permanently repeating loop. This means that there might be a weak emphasis placed on speed of response to a stimulus, or in decision making, inherent to members of that cultural group – coupled with a particular belief system there may in fact be more than one opportunity to complete a particular task.

The author (Slay, 2001) made the following assertions after comprehensive ethnographic fieldwork carried out among college students in Australia and China (PRC). These provide a comparison of Chinese and Australian attitudes to science, as demonstrated in their understanding of the natural world.

**Chinese study**

I. Chinese college students tend to discuss the natural world using a homogeneous set of perspectives set of perspectives. The students do not display a diverse range of attitudes.

II. The level of science integration with everyday thinking is high. Discussion of nature by Chinese college students involves the use of school science knowledge.

**Australian Study**

I. College students from semi-rural Northern Queensland tend to discuss the natural world predominantly using a wide range of aesthetic and religious perspectives. These views do not appear to be linked or to or held in tension with scientific ones.
2. The level of science integration with everyday thinking is low. Discussion of nature by semi-rural Northern Queensland College students involves little use of school science knowledge.

This kind of qualitative data is useful in providing a general indication of patterns of belief and behaviour. The above data indicates that a Chinese group might be more 'scientific' in its belief system than an Australian group from the population sampled. Qualitative data can provide results that can be expressed as traditional statistics, which give an indication of features of a culture. These can then provide a simple graphic description of a culture. Qualitative data such as that produced from fieldwork sometimes provides incomplete and contradictory information, and in this case, fuzzy logic and rough sets can be used to generate an algorithm on which a dynamic simulation of interacting thought systems could be based.

So Force A might be pictured as:

\[ P(\text{Control free}) = 85\% \]
\[ P(\text{Belief system}) = \text{religious} = 35\% \]
\[ = \text{political} = 42\% \]
\[ P(\text{View on natural world}) = \text{western scientific} = 23\% \]

If a similar analysis of Force B and Force C were carried out and a diagnosis were to be made using similar cognitive characteristics, it might be found that Force B was made up of people whose belief system was much more homogeneously religious and political and with animistic views of the natural world, for example, and with a command approach which was largely problem bound. If it were known that Force C displayed another quite different profile then command and control issues could be anticipated well in advance. With this kind of qualitative information, useful decisions as to the nature of battle command arrangements could be made well before the commencement of a mission.
FURTHER WORK AND FORMALISATION OF THE MODEL

While a relatively clear informal model of the role of culture can be obtained from observation, influenced by anthropological frameworks founded on world view theory, in the development of a synoptic view, further work is needed to collect rich data from specific military and anthropological cultures and then it is necessary to develop formal models to describe and simulate the intercultural interactions.

REFERENCES


A Duality Security Risk Analysis Method for e-Commerce

M Warren 1 and W Hutchinson2

1School of Management Information Systems
Edith Cowan University,
Western Australia, 6018,
Email: mwarren@deakin.edu.au

2School of Computing and Mathematics,
Deakin University,
Geelong, Victoria, Australia, 3217.

ABSTRACT

E-Commerce security is a complex issue, it is concerned with a number of risks that appear at a technical level and organisational level. This paper uses a systemic framework, the Viable System Model (VSM) to determine the high level risks and then uses baseline security methods to determine the lower level security risks. The paper examines the way in which the method works using examples.

Keywords: e-Commerce, Security, Viable System Model, Baseline Security.

INTRODUCTION

Information systems are now heavily utilized by all organizations and relied upon to the extent that it would be impossible to manage without them. This has been encapsulated by the recent development of e-Commerce in a consumer and business sense. The situation has arisen that information that operate on-line on a global basis are being and transparency in operation is considered normal place. The situation now arises that these global information systems are at threat from a number of risks and what is needed is a security method to allows for those risks to be evaluated and acted upon.

MODELING METHODS

The aim of the research was too combine a information systems modeling method with a baseline security method to form a hybrid security method. This method could be used to evaluate high and low level security risks associated with e-Commerce. The methods used in this model are the Viable System Model (VSM) and Baseline Security standards (minimal levels of security). The VSM is used to model an organisation's basic functions and associated data flows, whilst Baseline Security standards are used to apply sounds security procedures. Both of these are explained in detail in the next two sections.
THE VIABLE SYSTEM MODEL (VSM)

The Viable System Model (VSM) developed by Stafford Beer (1985), using the principles of cybernetics has been successfully used to diagnose existing organisational structures and design new ones. It is the generic nature of the VSM that allows it to be used in different situations (see Hutchinson and Warren, 2000). In terms of this paper the model will be used as framework to analyze potential vulnerabilities to an organisation’s information systems at a high level.

Before using the VSM, it is essential to understand the dynamics of its applicability and a diagrammatic representation is shown at Figure 1. The VSM consists of five subsystems, or functions, which Beer contends are necessary for a system to have long term viability. They are:

- **Implementation (S1):** this function consists of semi-autonomous units, which carry out the operational tasks in the system. These are the functions that are basic to the existence/purpose(s) of the system. They interact with their local environment, and each other. Each unit has its own local management, which is connected to wider management by vertical information flows. This function is the ‘doing’ part of an organization. The VSM has a recursive element, and each S1 has another VSM embedded in it.

- **Co-ordination (S2):** this function co-ordinates the S1 units to ensure that each S1 unit acts in the best interest of the whole system, rather than its own. This could be represented by something as simple as a timetable, or as subtle as morale among the workforce.

- **Internal Control (S3):** this function interprets policy information from ‘higher’ functions (S4), and ‘lower’ functions. It is the function, which controls the operational levels. Its function is not to create policy, but to implement it. Information arriving from the S1 function must periodically be audited for its quality and correctness. This is the S3* audit function.

- **Intelligence and Development (S4):** this function acts as a filter of information from the S3 function and the overall outside environment. Its purpose is to ensure that the policy making function (S5) is adequately briefed, and decisions are transmitted to S3.

- **Strategy and Policy (S5):** this function is responsible for the direction of the whole system. It must balance internal and external factors.

The data flows between S1 and S5 and the environment are shown in Figure 1. These flows show the potential points of vulnerability to an 'information attack'. With this conceptual model of a viable system (organisation), strategies and tactics can be developed to make the system 'non-viable' or dysfunctional. The logic being that investigating functional shortcomings can be used to improve an organisation and show its weaknesses, but also, to show possibilities for attack.
Figure 1: The Viable System Model

(Note: Env = Environment, mgnt = management)
BASELINE SECURITY APPROACH

The aim of risk analysis is to eliminate or reduce risks and vulnerabilities that affect the overall operation of organisational computer systems. Risk analysis not only looks at hardware and software, but also covers other areas such as physical security, human security, and business and disaster protection. In practice, there are major problems with the use of risk analysis; the time taken to carry out a review, the cost of hiring consultants and/or training staff. To overcome these negative aspects, baseline security standards were developed. Baseline security standards offer an alternative to conventional risk methods as they represent the minimally acceptable security countermeasures that an organisation should have implemented. These countermeasures are applied in a generic manner, for example, every organisation should have the same baseline security countermeasures.

The advantages of using baseline methods include (Warren and Hutchinson, 2000):

- cheap to use;
- simple to use;
- no training is required to use the method;
- it is quicker then undertaking a full security review.

Commonly used baseline methods include: the Australian and New Zealand AS/NZS 4444 standard (Australian and New Zealand Standard Committee, 1998), the British BS7799 standards (British Standards Institute, 1995 & 1998) and German BSI standard (BSI, 1994).

There has been research undertaken in regards to the problem of baseline security and e-Commerce (Gaskell, 2000). This research was focused upon AS/NZS 4444 and the fact that its security countermeasures are insufficient for e-Commerce deployment in several areas. This research also determined that anything other than a full risk assessment for e-Commerce projects could result in systems with unacceptable security weaknesses (Gaskell, 2000).

The problem with that conclusion is that:

- it does not take into account the advantages of baseline approaches;
- it does not take into account the limitations and problems associated with risk analysis;
- it does not take into the account that risk analysis is only effective on single systems and not multiple systems which represents majority of e-Commerce systems.

The authors decided to develop a security assessment method by which baseline security weaknesses can be overcome and help form part of a stronger framework that allow for organizational security reviews to be undertaken.

DUALITY RISK ANALYSIS MODEL

The aim of the duality risk analysis security model is to develop a security analysis model that combines the strength of VMS and baseline approaches. Another aim is to overcome the weaknesses associated with baseline security models and allows for the VMS approach to be used in a security environment.
The stages of the duality risk analysis model are:

Stage 1 - VMS Stage

This stage of the model is concerned with using the VMS model to determine the impacts and risks that a particular security threat would have upon an organisation. The impact can be assessed upon the whole organisations as shown by figure 1. Vulnerabilities of the various functions (S1 to S5) are used to examine various options for attack.

Stage 2 - Baseline Stage

The appropriate baseline countermeasure are selected that would be applicable to the security threat as defined in stage 1. The idea is to apply baseline security that is a minimal level of security into organizations.

The authors have created special software that allows for appropriate countermeasures to be selected easily e.g. what are the BS7799 guidelines that relate to computer viruses. This software also supports query searches and reporting functions.

Stage 3 - Evaluation of Impact

The stage 1 process is repeated but this time the impact of the security countermeasure is evaluated. This will allow for the evaluation of the security countermeasure and show its effectiveness across the whole organization. The information provided by this will allow management to determine their security countermeasures.

This approach can by used to evaluate any security risk associated with e-Commerce. This type of approach will allow an organisation to model what it perceives are the important security risks and how they relate to their organization.

VALIDATION OF MODEL

To validate the model the authors having been looking at a number of security risks that could impact upon e-Commerce. In this paper will look at the impact of viruses. The type of virus attack that is being modeled would be a Word macro virus infection similar to the 'Lovebug' virus.

Stage 1 - VMS Stage

Figure 1 illustrates the different levels of a sample organisation. The impact of the virus attack upon that sample organization would be:

S1 Implementation

During the attack the S1 operating units will be affected. Within an organization each S1 might well have their own IT infrastructure as part of the overall organization's system. A virus outbreak would focus upon the communication infrastructure of the S1 unit. The impact will be that e-mail servers will crash under the extensive volume of data and possibly cause a cascade affect through the S1 unit by the increase of email traffic caused by the viruses. For example, if the mail server crashes what else will crash? Therefore a macro virus attack might affect S1 units' ability to interact from their operating (local) environment as well as disconnecting from other S1 units and separating them from management functions. The attacks on the S1 unit will decrease the efficiency of the whole organization because of the disruption it will have upon the operational aspects.
**S2 Co-ordination**

There would be a dramatic impact upon the coordinating function of the S1 units. Because of the impact of the macro viruses S2 would not be able to work due to the isolation of the S1 units. There is also a chance that the S2 function would be affected by viruses spreading from the S1 units and therefore become isolated causing the coordination function to collapse.

**S3 Internal Control**

The internal control of the information system will be disrupted because of the chaos at the lower levels. It is therefore difficult to implement policy when structure of the information system infrastructure to be neutralised

**S4 Intelligence and Development/S5 Strategy and Policy**

The virus will nor directly impact the S4 and S5 functions, unless the cascade effects of failures were dramatic to affect these higher level systems or unless the S4 and S5 functions were identified for attack and they would then become isolated from the rest of the organization. Normally the Planning and Policy functions are long to medium term focused, so short term failures do not seriously affect strategy, although in this fast paced world that is not always the case.

**Stage 2 - Baseline Security Stage**

The decision support security software would be used to pick an appropriate baseline countermeasure. Figure 2 shows a screenshot from the baseline security tool.

![Security Baseline Tool](image)

**Figure 2: Security Baseline Tool**

This will work by the user selecting an appropriate baseline security countermeasure that could be implemented. The user would use the Security Baseline Tool (as shown by figure 2) and find an appropriate security countermeasure that would relate to computer viruses. The software would then show the appropriate baseline security countermeasure such as:

"Implement appropriate virus protection strategy"

The user can select this as being the security countermeasure they want to assess.
Stage 3 Re-evaluation of Impact

The user reviews the situation with the existing new countermeasure in place.

**S1 Implementation**

The virus protection strategy localises the damage to a few S1 units, assuming that some S1 units did not effectively implement a proper virus protection system for example, virus checkers out of date.

**S2 Co-ordination**

There would be localised disruption of a few S1 units. Co-ordinations functions can be adapted to overcome these localised difficulties until the problem is quickly resolved.

**S3 Internal Control**

No direct impact.

**S4 Intelligence and Development/S5 Strategy and Policy**

No direct impact.

Stage 2 and Stage 3 can be repeated if a security countermeasure does not have the required effect.

**CONCLUSION**

The paper has shown that hybrid security models can be used to model complex security solutions in relation to e-Commerce. The aim of the research is not to fully replace detailed security risks analysis methods but to offer an easier alternative that can be used to model different e-Commerce security risks and determine the impact of appropriate security countermeasures.
REFERENCES


ABSTRACT

The aim of this paper is to investigate how the software development industry is influenced by Open Source Software (OSS) projects by analysing the role of Hackers as the drivers of the Open-Source movement. It will be necessary to first briefly outline the common misconception of Hackers in the general public and understand the ideas behind Open Source. According to hackers' ideals, the concept of open source code for everyone and anyone to modify is commendable, however, in our profit-oriented societies, the economic cycle is based on value systems associated with commerce for profit outcomes.

Keywords: Hackers, Open Source, Business Models, Information Warfare

INTRODUCTION

In the past 30 years, society has become highly dependent on technology. Our vulnerability increases in proportion to our dependence on computers and technology; virtually all critical infrastructure, governmental organizations, as well as companies are reliant on computer networks. Each computer user could make cyberspace more secure if the general public were better educated about computer security (Lupo 2000). Furthermore, most software is released before it is secure, due to commercial pressures and profit maximisation of software-producing firms (Denning 1999). Finally, system administrators also often act in a negligent way (Taylor 1999).

Media regularly reports about Hackers taking advantage of this vulnerability spreading malicious viruses, penetrating government computers, and with credit-card fraud. Hackers are perceived by society to be those people who destroy and steal via Internet. However, they are quite the opposite. It is other individuals, who are misleadingly called Hackers that do so.

Hackers have no malicious intent and continuously shape technology, as we know it. They are the watchdogs of the Internet and technology companies. They put pressure on companies by publicly exposing security flaws i.e. of software (Denning 1999). Furthermore, they are the drivers of the Open-Source movement. Linux is the most commonly cited example for a successful Open-Source project created by Hackers. This Operating System has become increasingly popular in the last years since it is a freely available as well as highly secure and stable, as opposed to licensed products like Microsoft’s operating systems.
Today Linux is the fastest growing OS competing in one of Microsoft’s most profitable markets. The commercial software-developing industry condemns the Hacker’s ethic as it sees its profits endangered by the movement around Linux. Microsoft’s executives claim that Open-Source software like Linux endangers the IT industry arguing that ‘there is not much value in free’ (Mundie 2001). But, in spite of Linux’ technological success SUSE’s officials, a leading Linux vendor, recently declared that Linux as a business wasn’t working out. SUSE has already had to lay off two-thirds of its staff, explaining that the company was a victim of irrational expectations (O’Gara 2001).

**HACKERS – A COMMON MISCONCEPTION**

Hacking has its origin in the early 1960s, at a time there were only military institutions, universities and big corporations were privileged to have access to computers. There is general consensus that the first Hackers where computer science students at the MIT. These first generation Hackers formulated the original Hacker Ethic in the 1960s. It was an informal code that was accepted by most Hackers with the following tenets (Levy 2001): (i) Access to computers should be unlimited and total. (ii) All information should be free. (iii) Mistrust authority and promote decentralisation. (iv) Hackers should be judged by their hacking not bogus criteria such as degrees, age, race, or position. (v) Create art and beauty on a computer. (vi) Computers can change life for the better.

However, with the changes in cyberspace over time, the Hacker ethic was extended. Many old-school Hackers do not accept the new tenets of the modern Hacker ethic. Nevertheless, it is widely accepted by the younger generation of Hackers (Himanen et al. 2001): (i) Do not damage computers or data. (ii) Share information. (iii) Help system administrators. (iv) Protect Privacy.

Media started the daemonisation of Hackers by calling computer criminals Hackers in the mid 1980s. It is not likely that there was any intention to daemonise Hackers then, but journalists were rather ignorant about what and who Hackers are. Today the term Hacker is associated to a computer criminal by the general public and has become a colloquial general expression for Crackers, Hactivists, Cyber-vandals, Script-Kiddies, Cyber-terrorists, and many more who act with malicious intent (Denning 1999). As opposed to real Hackers these groups can be considered as those who practice illegal online activities with malicious intent, which can be compared to criminal acts in the physical world.

**THE OPEN SOURCE MOVEMENT**

In the early days of computing, programs came bundled with the hardware and complete with the source. It was only in the 1970s, as computing spread, that firms started to withhold the source code, thereby making software proprietary and turning it into a big business. Many early Hackers were horrified by the decision to withhold the source code, because it discouraged cooperation. Today, classical technology standards bodies have turned out to be rather slow and inefficient in many cases. Monopolies are faster and do a better job, but they tend to put the brake on innovation in order to keep their dominant position. The Open Source idea allows everyone capable of writing code to make modifications to a given source code without complex bureaucracy, which leads to more robust and secure software and more diverse business models (OSI 2001).

Characteristics of open source software are: (i) price of software is zero; (ii) software is distributable, (iii) unlimited users and usage, (iv) available source-code, (v) modifiable source-code. Users of open source software are traditionally expert users and early adopters, usually incorporating user and developer in one person. As more OSS projects focus on usability this profile will change (Feller and Fitzgerald 2000).
The advantage of OSS is that the software comes free and customisation only costs the man-hours involved, whether it be in-house or outsourced. When software is debugged or modified, everyone profits, and thus costs and risks are shared between consumers in the long term. You get what you pay for, and you know what you get.

BUSINESS MODELS FOR OSS

From the Free Software Foundation's perspective, the term free software refers to freedom, not price. 'It is not contradictory to say that software can be both for sale and free simultaneously' (Ming-Wei and Ying-Dar 2001). Software is free if it implies the freedom to run the program, modify it, redistribute copies for a fee or for free, and redistribute modified copies, so that the community can benefit. Open Source software is a superset of free software, with different occurrences.

As opposed to OSS, proprietary software is based on the idea that software is a commodity. Selling as many licensed copies as possible, thus obtaining highest possible economies of scale, maximizes profits. For further maximising profits, new versions are released on a regular basis, even if systems have security flaws or other bugs. In a quasi-monopolistic market, as is the case for desktop operating systems and office software tools, the consumer has no choice but consume and pay. Things are very similar for business software like SAP. Once a critical mass of companies deploy a certain software, the need for training staff on popular software system will be lower than on less popular ones, and making business with business partners that already have SAP is easier than with any other tool.

Even if the OSS comes at no costs, or low costs, there are still possibilities to make business with OSS. The software comes free with the code, but third party vendor or service companies like Red Hat Linux sell their value added services; in particular by modifying the source code to the needs of customers, as well as providing training and consulting services.

It is a philosophical question whether this is a stable business model. In the end there will probably always be a vendor that tries to maximize profits without following hackers ethic. Software that requires high standardisation, like office software, is a challenge for vendors to generate economies of scale. On the other hand the OSS concept is likely to provide interesting business models for software that requires much customisation.

OUTLOOK AND FURTHER RESEARCH

This paper discussed that Hackers should not be demonised but appreciated for their achievements, since they are not the destructors of the Internet but its architects who believe the Internet to be a medium of free information and open communication. Furthermore Hackers role in the Open-Source movement was discussed and as well as whether and how the Open-Source movement will replace the common practices in the software development industry. Further research will go from here and analyse business models for OSS development in detail. In particular the correlation of software costs with the type of licensing scheme and the type of software will be analysed, in particular considering aspects of license costs, costs of security flaws, costs for system administration, and trainings costs.
REFERENCES


Desktop Warfare in the Data Gridlocked Information Age

D. W. Maguire

School of Management Information Systems
Edith Cowan University, Australia
E-mail: allmaguires@bigpond.com.au

ABSTRACT

This paper looks at information overload which it discusses as a more common form of information warfare affecting business environments as the increased availability and supply of data causes gridlock in decision-making processes. It examines literature dealing with the creation of data and its impact on management and puts into context the effects on the financial and security industries.

Keywords: information warfare, overload, knowledge, data, delivery, ammunition

INTRODUCTION

The magnitude of information flow resulting from the development of IT continues to increase and there are new methods of delivery regularly being added. The Information Age has led to the democratisation of data and consequently there is a build-up of information supply that not only exceeds demand but also human capacity to cope. As the post-modern concept of Information Warfare migrates from its IT-era origins in the battlefields of the Persian Gulf to the cusp of a network society, it can be argued that the armoury is on all desktops and the ammunition an abundant supply of data in digital bits and bytes. This concept is not at the level of targeted logic bombs, viruses and back door or denial of service attacks. The problem of information overload has a universal impact: when it manifests negatively in user groups critical to business performance it creates a strategic advantage for competitors and thus becomes a potential weapon of Information Warfare. This article proposes through a review of relevant literature that there is too much information becoming available and there is evidence it can have enough of a debilitating effect on business and managers to make them susceptible to predators.

TOO MUCH INFORMATION

Timing, speed of movement and numbers are integral to the formation of strategy in traditional warfare. The same elements are as important in waging information warfare but are enhanced by the power of the technology age. The Pony Express traveled at 10mph, the mail train at 60mph, the airplane at 160mph, the jet at 580mph and an e-mail sent from San Francisco to New York can travel at about 30,000 miles per second (anonymous, 2001). A century ago, the average person could only create and access a small amount of information. Now, ordinary people not only have access to huge amounts of data, but are also able to create gigabytes of data themselves and, potentially, publish it to the world via the Internet (Lyman and Varian, 2000). A weekday edition of The New York Times contains more information than the average person was likely to come across in a lifetime in 17th century England (Wurman, 2000).
The Internet is dramatically changing the way people live and work and has the capacity to bind professionals, interest groups and communities like never before with its interactive attributes, ease of use and speed of response. It is making wide ranges of information available, more than is needed by the average individual who can log-off when they've had enough. The workplace, however, is coming under different pressures with a new paradigm of information availability changing the way people work and the way decisions are made. More information should lead to better-informed decisions however the masses of data and information being collected are adding to the time taken to get to a knowledge-enhanced decision. The subsequent pressure growing from this situation is building a different form of Information Warfare to what would normally be categorised under this subject heading. A study mentioned later in this paper outlines the injuries suffered by the wounded in this combat. Unlike what would be expected to be covered in this category, the information warfare being experienced by the victims of information overload is that they are being overwhelmed to such an extent that decision gridlock creeps into their businesses. Information becomes the enemy.

How much is too much information and how much is hollow information? DiNardo and Hughes (1995) posed the question in their post-Gulf War critique of Information Warfare as they identified the looming spectre of data overload. They recognised the danger that commanders (read managers and workers) would be so bombarded by a blizzard of largely extraneous or even unessential data that it would obscure the real issues that had to be dealt with. The reverse of data overload was also a problem. What should a commander do in the absence of all the data or information he wants or thinks he needs or has learned to depend on? If information is the most important thing in modern warfare or business, does its absence give an irresolute leader the excuse to do nothing? History shows that the great captains have always sought information concerning their opponents. Ultimately, however, they had to make decisions in the "fog of uncertainty" to use the key phrase from 19th century military strategist Carl von Clausewitz (1988).

WELL INFORMED, WELL CONNECTED

Our understanding of the mass of information available and being created daily is enhanced by the findings of a team from University of California at Berkeley, led by Lyman and Varian. They assessed that the world produces between 1 and 2 exabytes of unique information per year, roughly 250 megabytes for every man, woman, and child (an exabyte is a billion gigabytes, or 1018 bytes) and that it would soon be technologically possible for an average person to access virtually all recorded information.

The study underlines that data and delivery systems are available for every IT connected person to engage in a form of information warfare. The researchers were surprised by the "democratisation of data" (Table 1). A vast amount of unique information is created and stored by individuals; original documents created by office workers are more than 80% of all original paper documents, while photographs and X-rays together are 99% of all original film documents. Camcorder tapes are also a significant fraction of total magnetic tape storage of unique content, with digital tapes being used primarily for backup copies of material on magnetic drives.

Also notable was the "dominance of digital" content. Not only is digital information production the largest in total, it is also the most rapidly growing. While unique content on print and film are hardly growing at all, optical and digital magnetic storage shipments are doubling each year. Even today, most textual information is "born digital," and within a few years this will be true for images as well. Digital information is inexpensive to copy and distribute, is searchable, and is malleable. Thus the trend towards democratization of data, especially in digital form, is likely to continue.
In 2000, the World Wide Web consisted of about 21 terabytes of static HTML pages, and the study reveals that is growing at a rate of 100% per year. Many Web pages are generated on-the-fly from data in databases, so the total size of the "deep Web" is considerably larger. Although the social impact of the Web has been phenomenal, about 500 times as much e-mail is being produced per year as the stock of Web pages. It appears that about 610 billion e-mails are sent per year, compared to 2.1 billion static Web pages. As Odlyzko (2000) puts it, "communication, not content, is the killer app."

Though the main focus of the report is on the supply of information, it is worth looking at data measuring the consumption of information as well. Table 2 depicts hours per year of time spent on various media in US households comparing the years 1992 and 2000.

<table>
<thead>
<tr>
<th>Storage Medium</th>
<th>Type of Content</th>
<th>Terabytes/Year, Upper Estimate</th>
<th>Terabytes/Year, Lower Estimate</th>
<th>Growth Rate, %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper</td>
<td>Books</td>
<td>8</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Newspapers</td>
<td>25</td>
<td>2</td>
<td>-2</td>
</tr>
<tr>
<td></td>
<td>Periodicals</td>
<td>12</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Office documents</td>
<td>195</td>
<td>19</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Subtotal:</td>
<td>240</td>
<td>23</td>
<td>2</td>
</tr>
<tr>
<td>Film</td>
<td>Photographs</td>
<td>410,000</td>
<td>41,000</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Cinema</td>
<td>16</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>X-Rays</td>
<td>17,200</td>
<td>17,200</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Subtotal:</td>
<td>427,216</td>
<td>58,216</td>
<td>4</td>
</tr>
<tr>
<td>Optical</td>
<td>Music CDs</td>
<td>58</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Data CDs</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>DVDs</td>
<td>22</td>
<td>22</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Subtotal:</td>
<td>83</td>
<td>31</td>
<td>70</td>
</tr>
<tr>
<td>Magnetic</td>
<td>Camcorder Tape</td>
<td>300,000</td>
<td>300,000</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>PC Disk Drives</td>
<td>766,000</td>
<td>7,660</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Departmental Servers</td>
<td>460,000</td>
<td>161,000</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Enterprise Servers</td>
<td>167,000</td>
<td>108,550</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>Subtotal:</td>
<td>1,693,000</td>
<td>577,210</td>
<td>55</td>
</tr>
<tr>
<td>TOTAL:</td>
<td></td>
<td>2,120,539</td>
<td>635,480</td>
<td>50</td>
</tr>
</tbody>
</table>

Lyman and Varian (1999)
Table 2: Summary of yearly media use by US Households in hours per year, with estimated megabyte equivalent. (Hours from Statistical Abstract of the United States, 1999, Table 920 (projected).

<table>
<thead>
<tr>
<th>Item</th>
<th>1992 Hours</th>
<th>2000 Hours</th>
<th>2000 Mbytes</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>TV</td>
<td>1,510</td>
<td>1,571</td>
<td>3,142,000</td>
<td>4</td>
</tr>
<tr>
<td>Radio</td>
<td>1,150</td>
<td>1,056</td>
<td>57,800</td>
<td>-8</td>
</tr>
<tr>
<td>Recorded Music</td>
<td>233</td>
<td>269</td>
<td>13,450</td>
<td>15</td>
</tr>
<tr>
<td>Newspaper</td>
<td>172</td>
<td>154</td>
<td>11</td>
<td>-10</td>
</tr>
<tr>
<td>Books</td>
<td>100</td>
<td>96</td>
<td>7</td>
<td>-4</td>
</tr>
<tr>
<td>Magazines</td>
<td>85</td>
<td>80</td>
<td>6</td>
<td>-6</td>
</tr>
<tr>
<td>Home video</td>
<td>42</td>
<td>55</td>
<td>110,000</td>
<td>30</td>
</tr>
<tr>
<td>Video games</td>
<td>19</td>
<td>43</td>
<td>21,500</td>
<td>126</td>
</tr>
<tr>
<td>Internet</td>
<td>2</td>
<td>43</td>
<td>9</td>
<td>2,050</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>3,324</strong></td>
<td><strong>3,380</strong></td>
<td><strong>3,344,783</strong></td>
<td><strong>1.7</strong></td>
</tr>
</tbody>
</table>

Lyman and Varian (1999)

The notable features of this table are the hours spent on TV and radio consumption and their consistency over time, the reduction in time spent on printed information, and the dramatic increase in home video, video games, and Internet usage. It is noteworthy that total time spent in media access has hardly changed in eight years. Even while information supply is growing dramatically (especially in electronic media) the actual consumption of information is barely changing: a smaller and smaller fraction of what is produced is actually consumed, a point which supports the notion that no matter how much is produced, only so much can be consumed.

Table 3 summarizes the yearly production of information by and about individuals. The amount of "individual" information is over 600 times larger than the amount of published information. Although the Web, Usenet, and e-mail include a great deal of individual information, they have been omitted from both of these tables, since the report’s authors found it difficult to know whether to classify this material as "individual" or "public."

Table 3: Yearly production of published information

<table>
<thead>
<tr>
<th>Item</th>
<th>TITLES</th>
<th>Terabytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Books</td>
<td>968,735</td>
<td>8</td>
</tr>
<tr>
<td>Newspapers</td>
<td>22,643</td>
<td>25</td>
</tr>
<tr>
<td>Journals</td>
<td>40,000</td>
<td>2</td>
</tr>
<tr>
<td>Magazines</td>
<td>80,000</td>
<td>10</td>
</tr>
<tr>
<td>Newsletters</td>
<td>40,000</td>
<td>.2</td>
</tr>
<tr>
<td>Office Documents</td>
<td>7,500,000,000</td>
<td>195</td>
</tr>
<tr>
<td>Cinema</td>
<td>4,000</td>
<td>16</td>
</tr>
<tr>
<td>Music CDs</td>
<td>90,000</td>
<td>6</td>
</tr>
<tr>
<td>Data CDs</td>
<td>1,000</td>
<td>3</td>
</tr>
<tr>
<td>DVD-video</td>
<td>5,000</td>
<td>22</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>285</strong></td>
<td></td>
</tr>
</tbody>
</table>

Lyman and Varian (1999)

The authors concluded that it was clear we are all drowning in a sea of information and the challenge was to learn to swim in that sea, rather than drown in it.
REDUCED TIME TO DECISION

Availability, speed and access are significant determinants in the amount of information individuals seek to engage with (Alberts et al, 1999). Across a broad range of activities and operations, the time required to access or collect the information relevant to a decision or action has been reduced while the volume that can be accessed has increased exponentially. In some competitive domains, such as on-line share trading, the timeliness for creating value has been reduced from hours to seconds. The Information Age is making distance less relevant. Information, and the decisions that result, can travel almost instantaneously to where they are needed, making the location of those who gather, analyse, make decisions, and possibly those who act on them, largely irrelevant. The Information Age is also compressing the time dimension. First, by making location less important it reduces the need for travel. Second, to the extent that information gathering, analysis, and decision-making are activities on the critical path, advances in Information Age concepts and technologies are compressing process cycle time. These changes in the dimensions of time and space are increasing the pace of events, or operating tempo, in many different environments. This phenomenon is seen in the shortening half-life of a breaking news story, in the shrinking time it takes for a product to reach the market and in the waning attention span of the public.

The human impact of this tempo and pressure adjustment wrought by the new operating dimensions of Information Age business has been assessed in a study commissioned by Dow Jones through Reuters (1998). It found that an excess of information was strangling business and causing personnel to suffer mental anguish and physical illness. One in four of over 1300 managers surveyed admitted suffering ill health as a result of information they now handled and nearly half predicted the Internet would further aggravate the problem in coming years. Some of the consequences of the information glut were delaying of important business decisions, tension, stress, illness, procrastination and time-wasting, ailments that lead to the core ability of the corporation to succeed or not.

A third of managers received “enormous amounts” of unsolicited information and 49% felt frequently unable to handle the volume of information they received. Almost half of them believed that information collection was needed to “keep up with” colleagues when making decisions and two-thirds believed the information was under-utilised.

Singaporean managers cited the need for information management policies to be implemented to deal with the problem as 37% of those surveyed said information overload left them unclear about their job responsibilities. Of all the nationalities surveyed, the Hong Kong respondents felt they had suffered the most from information overload and they were the most likely nationality to cite the problem as a barrier to effective information retrieval.

KNOWLEDGE-ENHANCED ENVIRONMENTS

Too much information is causing different challenges to the international security sector and the financial sector, both of which rely on as much data as possible to make strategic decisions that have potential bearing on people’s lives and livelihood. It could be argued that the more information collected, the better they will be able to achieve their objectives, in these cases to make the world safer and more comfortable. This is not necessarily the case.

The largest US spy agency – the National Security Agency (NSA) – has been beset by too much information, as well as too many targets and the challenges created by increasingly sophisticated technologies (Ensor, 1999). In this sector, data and information is life-and-death critical ammunition, potentially jeopardising the lives of millions of people. The agency is more than twice the size of the CIA, is at least twice as secretive, produces probably 80 per cent of intelligence the United States uses and its mission is to listen for threats to US national security. It is, though, in information overload. After a period of having to listen to only the Soviets, it now has dozens of targets including international drug cartels, nuclear weapons dealers and terrorist-minded citizens that want to bomb
buildings. The agency has sophisticated eavesdropping equipment strategically placed around the world and a staff of crack code-breakers with the world’s latest array of supercomputers but it is not enough to handled the current load of information.

Difficulties posed by new technologies threaten to make the NSA’s “big ears” increasingly deaf, including:

- The worldwide move to digital, rather than analog, phones makes eavesdropping harder
- Fax machines and fibre-optic cables are much harder to tap
- Good encryption software lets even drug lords and terrorists scramble their signals
- The Internet creates mountains of public—not secret—data that needs to be analysed, a job for which expensive eavesdropping equipment is of no use.

Information transparency is an integrity platform of the financial sector in which millions of dollars worth of shares are traded every day and where investors rely on the validity of data and information to form a knowledge-enhanced decision as to where to put their money. Information is the raw material, the predominant fuel and the product that can be used to create wealth and the emergence of real-time awareness and real-time transaction capabilities is changing the dynamics. The Chairman of the Federal Reserve, Alan Greenspan, (2000) said that, at a fundamental level, the essential contribution of information technology is the expansion of knowledge and its obverse, the reduction in uncertainty. Before this quantum jump in information availability, most business decisions were hampered by a ‘fog of uncertainty’, he said, borrowing from von Clausewitz (1988).

Wall Street indulges in a unique game: a blend of fundamental theory, intuition and often blind luck. It has been jokingly repeated that most stock traders, given notice, would want to have more luck in the stock market than they would want to have greater insight into it. Many investors operate on hunches and feelings and not on commercial calculations which could easily be automated. (Gilbert, 1995)

The speed of information has gained importance over the centuries ever since the southern tip of Manhattan became a fledgling financial centre in the 1790s. The business world of the 21st century moves with a lightning quickness: online investing, global trading, an increasingly volatile stock market and an extreme abundance of information. Too much information here is not enough; there is no suggestion of information overload and there is no stress about having to process all and more that the new technology can deliver. The money and media cultures have reached a grand convergence with information technology in which corporate executives boost their companies by trying to steer the non-stop coverage, while news outlets move stocks with an endless cascade of predictions, analysis and data-enhanced recommendations.

What happens on Wall Street is a quintessential example of how a style of information warfare is waged in the true context of the new parameters of the information society. In this arena, financial journalists are players, in fact they’re the soldiers. They make things happen instantaneously; and their impact is gauged by the stock prices. A single negative story, true or not, can send a company’s share price tumbling in a matter of minutes. A report about a possible takeover attempt can immediately pump up a stock, adding billions of dollars to a company’s net worth. The clout of financial journalists affects not just the corporate bottom line but the hard-earned cash of millions of average investors.

As Kurtz (2000) observes, in business, unlike politics, the reporting of rumors is deemed fair game, since rumors, even bogus ones, move markets. In an age of lightening-quick Internet reports, saturation cable coverage and jittery day traders, moving the market is a remarkably easy thing to do. The journalists, of course, don’t operate in a vacuum; they are used everyday by CEOs, by Wall Street analysts, by brokerage firms, by fund managers who own the stocks they are touting or are betting against the stocks they are denouncing. These money men are practiced in the art of spin, measuring their success in minute-by-minute prices. In an information overloaded, confused world where
everyone is jockeying for advance intelligence on what to buy or sell, information is power and it is the ammunition.

CONCLUSION

Systematic Information Warfare is being facilitated by the overflow of information that is being created to vast levels as the “democratisation of data” is enabled by new technology. Managers are being diverted from their core responsibility by the weight of information and data being generated by the new Information Age. Knowledge-enhanced decisions are taking longer because of the imperative to look at more data and the subsequent job pressure created is impacting on non-work hours. The quality of the new data is being questioned and the capacity of business to handle it is in doubt. This is an atypical interpretation of information warfare according to the general thrust of the literature but there are symptoms reported here which show a looming technology-facilitated threat to business which is potentially greater in impact than occasional endemic subterfuge.
REFERENCES


Ensor, D (1999). CNN, Fort Meade, Maryland, November 25


Lyman, P, Varian, H. R (2000). *How Much Information*? School of Information Management and Systems at the University of California at Berkeley, USA


Security Culture as a Defence against Information Warfare.

Colin Armstrong

Centre for Information Warfare
Edith Cowan University

ABSTRACT

Management of Information Warfare in a business environment is more than just intrusion detections systems, encryption and electronic security measures. Management in the Information Warfare sense includes the less prominent activities such as, policies and procedures, documentation, command and control and responsibility distribution, contingency planning, security incident handling, and intelligence gathering about opponents. These activities may be considered as the foundations that under pin and give substance to a corporate security culture. This paper discusses some of the managerial aspects that are overlooked in the effort to protect information systems in an electronic environment. The importance of a proactive and holistic approach is also discussed in preference to the more common reactive approach.

Keywords: Corporate Culture, holistic perspective, security awareness and education, policies and procedures, risk analysis, responsibility distribution, incident handling, contingency planning, intelligence gathering.

INTRODUCTION

The reactive approach to information security and information warfare is not a preferred solution. A preferred solution would incorporate some preventative measures and therefore be considered a proactive approach. Management needs to grasp the issues firmly, and then take an holistic approach requiring forethought and the implementation of measures that combine to form the foundations of a corporate security culture. This would build a basis upon which an organization may defend the integrity of its most valued asset - information.

This paper presents the need for a proactive approach to the management of security. Development of a security culture is discussed as a means of protection against cyberattacks. The components of such a stance incorporate building sound security management structures and processes, including security policies and procedures, risk analysis, security education and training, security responsibility, security incident reporting and handling procedures, contingency planning and intelligence gathering.
THE NEED FOR A PROACTIVE HOLISTIC APPROACH

Reports on computer crime and security continue to indicate cybercrime is constantly on the rise. While it is difficult to garner accurate and comparable figures accounting for all computer crime from one year to the next, the perception is that security never seems to catch up, leaving the victim reacting in defence. Figures extracted from the “Computer Crime and Security Survey” conducted by Computer Security Institute, (CSI) in participation with the San Francisco Federal Bureau of Investigation, (FBI) support this hypothesis. The 2001 survey shows that for 2001, 186 respondents reported US$ 377,828,700 in financial losses. This compares with 249 respondents in 2000 reporting US$ 265,589,940 in financial losses. The average in financial losses for the three years prior to 2000 was US$ 120,240,180. (Rapalus, 2001)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>400 Million</td>
<td></td>
<td></td>
<td></td>
<td>$377,828,700.00</td>
<td></td>
</tr>
<tr>
<td>350 Million</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>300 Million</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>250 Million</td>
<td></td>
<td></td>
<td></td>
<td>$265,589,940.00</td>
<td></td>
</tr>
<tr>
<td>200 Million</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>150 Million</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100 Million</td>
<td>$120,240,180.00</td>
<td>$120,240,180.00</td>
<td>$120,240,180.00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50 Million</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 Million</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Increasing Financial Losses caused by Computer Crime

Cybercriminals are proactive and have the upper hand. “Despite efforts to improve security and the investigative capabilities of law enforcement, the threat as a whole appears to be getting worse. .. it is worth considering whether our current practice of allowing – even encouraging – unfettered development and distribution of cyberweapons is serving us well.” (Denning, 2000, p.44.) Allowing this trend to continue will constantly place the organization in a reactive mode. Denning goes on to say in the future, cyberweapons may have the potential to be even more destructive and lethal than they are today. She warns that ubiquitous computing is coming, and with it Internet appliances, Web portals for people and objects, body LANs, and implants. This extends the range of opportunity for cybercriminals who may be able to turn on and off appliances, interfere with micro robots used in telesurgery, or send harmful signals to implants connected to a person’s brain. Rather than using force in a reactive stance to cripple or destroy the opponent’s or the organization’s own assets, or both, a proactive approach will assist in protecting valuable systems and information and possibly minimise human suffering and the loss of life.

Information is identified and accepted as a corporate asset yet all too often the need for protecting this asset is either not recognised or is placed so low on the corporate priority agenda to render the asset under protected. It is not a difficult matter to identify:

- The information that needs protection
- Threats to the information from, competitors, activists, and saboteurs.
- How access to the information may be gained
- Weaknesses to current protection methods

Management is then able to:

- Assess risk according to value and vulnerability
- Determine methods of protection and the associated costs.
Management should aim to ensure prediction, avoidance, deterrence, detection, interception, containment, recovery, and correction in physical and technical security together with personnel and procedural safeguards. (Pattakos 1997).

Louwrens and von Solms (1997) suggest security vulnerabilities can only be addressed by taking an holistic view of the total enterprise security environment. The use of reactive measures to security violations and prominent threats only places stop-gaps measures over small parts of an insecure environment. An holistic approach considers security in its entirety from an organizational perspective. Viewing something holistically means concentrating upon its wholeness, ie the totality of elements comprising the whole (Kiountouzis and Kokolakis, 1996, p.25). The goal of a proactive and holistic approach is to increase the perception of value of what you do within your entire organization, as well as to provide people with tools for thinking about the security issues faced every day so that they can act as an early warning system (Wadlow, 2000, p.46).

COMPONENTS OF A SECURITY CULTURE

The components of a security culture include, but are not limited to, the following actions –

- Security Policies and Procedures
- Security Responsibility Distribution
- Security Awareness and Education
- Security Incident Handling
- Contingency Planning
- Intelligence Gathering

Viewed from the holistic perspective, the Corporate Security Culture may be graphically depicted as in Figure 1. This of itself certainly should not be taken as the panacea to all security culture woes. It is not uncommon to see business situations where these ingredients were espoused but not enacted. The important word here is culture, and the culture ought to be a lived intention not just the stated objective. Each of the items within this nest is appraised separately below.

Figure 1: The Corporate Security Culture
AWARENESS AND EDUCATION

Before awareness and education programmes may be introduced, their necessity and value must be recognised and acknowledged. The "ever repeated problem within IT security is awareness and understanding" (Yngstrom 1996, p.351). Management cannot expect their employees to secure information if they do not understand its value or possible means of protection to be applied. The proactive approach would inculcate security education within life long learning and continuous company security awareness campaigns. According to Alan Stanley, Managing Director of the European Security Forum, management commitment to security and increased security awareness and education are current global security concerns (Stanley, 1997).

Denning (1999) suggests security education and awareness programs can serve to inform employees about their organization's information security policy, in addition to making them aware of risks and potential losses, and to also train them in the use of security practices and technologies. Without security awareness, employees will not be able to identify risks and threats to sensitive information.

SECURITY POLICIES AND PROCEDURES

All too often only lip service is given to the area of Policies and Procedures. The costs associated with the formation, implementation and then practicing of them may initially seem to be unwarranted. The "It will never happen to us" attitude is a poor risk management methodology. Policies and procedures of themselves may be of little value unless they are prepared and presented in a logical, interconnected and structured manner.

Leiwo and Zheng (1997) suggested that in order to support a harmonized framework for the development of information security within corporations, security policies and strategies be applied at three different levels:

- the strategic decision level, incorporating international and national objectives, standards and guidelines
- the organizational administrative level, incorporating a systemic approach addressing storage, processing and transmission of information, and
- the implementation level, incorporating mechanisms for guaranteeing an adequate level of systems protection.

RISK ANALYSIS

Maybe management understanding the concepts of risk is assumed or maybe they are just too busy to conduct the analysis. While the chances of an occurrence happening maybe remote, the fact that the result of that occurrence happening is fatal or of a critical nature demands that that risk be considered a high risk.

When it comes to information security few corporations go beyond securing the outer perimeter, the firewalls and such like. It is not just a matter of keeping the bad guys out. We must at the same time let the good guys in. Organisations have many relationships outside the immediate operational environments of their company. IT support maybe outsourced. Strategic partnerships are accommodated by permitting and indeed encouraging easy access to information assets, and the risk from within is often discounted. Wise organisations are investigating the options and methods that provide for the safe and reliable transmission of information between trusted and authorised persons. Encryption of all company information may be an option and partial solution.
Corporations that have divested control of other than their "core business" may have little influence over the protection of valuable information assets. The solutions must be incorporated into a risk management, minimisation strategy. Define the needs. There will be several sets of needs so each situation within the whole should be considered by its own merits and those needs addressed individually before being combined into the overall plan. The associated costs may then be determined and compared with the value of the information asset.

RESPONSIBILITY DISTRIBUTION

One of the management techniques, or maybe it is only a short term business fashion, adopted during the past decade has seen the responsibility of management decision making devolve from the most senior manager to a whole team of managers in the senior level of management. As a result of this shift in management style, no one individual is directly responsible, nor accountable. Obtaining fast responses to occurrences impacting on critical factors is more than a desirable situation. Slow decision making processes amount to an abrogation of responsibilities.

SECURITY INCIDENT HANDLING

While the handling of a security incident may be considered as reactive, and it is certainly only after an incident that this may be affected, it is the establishing of effective procedures that will enable the organisation to examine and then improve its proactive capabilities.

Denning (1999) suggests the following response to information warfare attacks:

- Investigation and assessment
  - Investigate to identify the perpetrator, plus the origin and extent of the attack, including vulnerabilities exploited, methods used, damages and options for responding

- Containment and recovery
  - Actions include breaking network connections, disabling accounts and shutting down systems, restore contaminated or deleted files from backups, backup site activation where necessary, employee termination or removal of access rights where appropriate, and handling of media

- Improving Security
  - Eliminate vulnerabilities, reconfigure systems, and fix security holes.

- Notify perpetrator and request them to stop their actions

- In-Kind Responses
  - Launch an offensive operation against the perpetrator using a similar method ie flooding websites can be responded to with software to open window after window on the perpetrator's system.

These suggestions by Denning are based upon reaction to an information warfare attack, rather than proactive. A proactive approach would incorporate establishing security measures to minimise the risk and impact of information warfare attacks through the adoption of improved planning as a result of careful analysis of the incident.
The Reaction section of the emergency response plan determines how to respond when there is a security incident. It must define the process of responding to probable scenarios. The response must be identified, documented and tested before there is an incident so that everyone knows what to do during the crises. The incident response plan is a critical part of the business continuity plan. Preparation is key to a successful response.” (Pipkin, 2000, p.17)

CONTINGENCY PLANNING

While it may never happen, a Contingency Plan may be the one thing that prevents the termination of an organisation. Many organisations take these risks without any risk analysis or understanding the dangers of being unprepared. This is paper is not going to tackle Contingency Planning in depth but points out that countless publications support this as a sound business practice.

There are two aspects of Contingency Planning that require a little thought and may be left unconsidered in the Planning Process.

One is Practice. We know that practice makes perfect and when included as a part of an Organisations corporate culture may be very effective. The military practice procedures, and business can emulate these, where computer systems are “hit” and then recovered to back on line status in very short periods of time. Times as short as 2 minutes have been mentioned and while it is not yet possible to provide references from published documents one can assume that the use of exchangeable hard disks combined with lots of practice could facilitate these sorts of times.

The other aspect is questions. Asking the right questions. Questions such as:

- How important to the corporate survival is the computer systems?
- How long can the organisation survive without any of its computer systems?
- Which parts of the computer system are of critical importance?
- Which parts of the computer system can be withdrawn without crippling the organisation?
- How long can the organisation survive without electrical power?
- How quickly can the organisation be back on line?
- How much of the total computer systems can be back on line within set time periods?
- Does the organisation have Contingency Plans?
- Can the organisation have a series of smaller Contingency Plans to accommodate specific incidents?
- Is the organisation encumbered with an inflexible Plan that only addresses a situation of complete and absolute failure of the computer systems and not the shades of grey between the black and white? and
- Does the organisation conduct Practice Exercises?

INTELLIGENCE GATHERING

Gathering information about business competitors has always been a legitimate business activity. Spying however is not socially acceptable. What is the difference?

Intelligence gathering may be considered under two aspects, internal and external. Internal intelligence gathering is probably more important and is certainly easier if handled correctly in the first place and incorporated into the culture of the corporation or organisation.

External intelligence is the area that we think of most often when considering intelligence gathering. Spies prey on naivété and are often passive information collectors operating legally. (Davis, 1998)

Table 2 summarises examples of Corporate Intelligence threats from within and external to the organisation and provides and indication of the likely reason for the vulnerability. Accidents are just that, accidents, and unpredictable, but also included under the heading of accidents are those
incidences where under trained staff may through error cause a loss. The loss, while not intentional, may be disastrous and is seldom the fault of the perpetrator. Invariably it is a management issue that when properly addressed removes the likelihood of reoccurrence.

Dissatisfied staff is directly within the scope of the corporate culture sculptures to manipulate, senior management. And naïve staff happen. A world of sceptics is not an attractive alternative.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Source</th>
<th>Vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidental Losses</td>
<td>Internal</td>
<td>Under trained staff</td>
</tr>
<tr>
<td>Vandalism</td>
<td>Internal</td>
<td>Dissatisfied staff</td>
</tr>
<tr>
<td>Bribery of staff</td>
<td>Internal</td>
<td>Dissatisfied staff</td>
</tr>
<tr>
<td>Staff Deceived</td>
<td>Internal</td>
<td>Naïve staff</td>
</tr>
<tr>
<td>Covert acts</td>
<td>Internal</td>
<td>Disgruntled staff</td>
</tr>
<tr>
<td>Covert acts</td>
<td>External</td>
<td>Criminal activities</td>
</tr>
<tr>
<td>Overt attacks</td>
<td>External</td>
<td>Criminal activities</td>
</tr>
</tbody>
</table>

Table 2: Corporate Intelligence Threats

Externally, threats may be overt or covert and both are undoubtedly going to incorporate criminal activities. The decision to notify the appropriate authorities or not is another matter. It was far better to never have to be in this situation in the first place.

**DRAWING TOGETHER – A CORPORATE CULTURE**

Few companies would deny the competitive necessity and value of Information Technology (IT) to their business systems, but many of these same companies fail to appreciate the new vulnerabilities associated with IT, especially when that IT is conducted by a third or outsourced party. For every new electronic security device that detects, scans or records there are counter devices designed to circumvent protects. (Wiltshire 2001)

Need for holistic approach. Need for the big picture of information at the planning stages of this process so that managers can make informed decisions in establishing the above. This limits the need for reactive management.

These items and areas discussed above may be referred to as holons. The term ‘holon’ refers to complex entities, particularly organisms and people, that are both simultaneously, whole individuals, and participating parts of more encompassing wholes (Koestler, 1967) Each is a complex entity that is simultaneously both a whole individual aspect and a participating part of a more encompassing whole, Information Warfare.

The use of visualisation tools is preferable as it enables all parties to see this big picture. Allows what if situations to be presented and the impact of actions taken to be seen prior to implementation. It is essential that the visualisation process is a combination of technical and managerial visions/views. Technical security measures provide an essential part of the defensive process, however the managers make the decisions to make it happen.

In summary a corporate security culture emerges from taking a view based upon the big picture. Security education and training raises awareness of security risks and the importance of protection. Security policies and procedures present guidelines for the handling of sensitive and valuable information. The allocation of security responsibility to all employees makes each individual accountable for information under their care. Risk analysis identifies the risks inherent in the organizational environment and encourages implementation of appropriate and cost-effective protective measures. The security incident response plan details how actual and potential security violations can be identified and actions to minimise the damage. Contingency planning presents
recovery strategies. Intelligence gathering provides information about the extended environment and offensive and defensive trends within the industry. Each measure on its own contributes only an isolated benefit. When all these measures are combined, a security system is formed. The value added is a corporate security culture.

CONCLUSION

Don’t underestimate the importance of the above mentioned management measures. While the technical security measures are necessary, the technicians do not make the decisions at the management level, they are made by the executives. The strength of the Corporate Culture could ultimately be the difference between the survival and the demise of an Organisation.

Dan Eigeles (2001) refers to cyberattacks as the “war of brains”. “The aggressors have the initiative while the security people and those subjected to aggression are in a permanent state of defense.” (Eigeles, 2000, p.13)

Regardless of the size of the organisation or the amount of time and money made available, the aggressors do hold the advantage and are able to attack as and when soft targets are identified or vulnerabilities are exposed. To maintain a proactive approach requires careful and considered analysis. There are however situations that are impossible to defend against and in those situations recovery procedures may be to only answer or option.

The policies we write and adopt today will define the condition of our organisations tomorrow. Prudence suggests that we protect our assets today and enjoy the fruits tomorrow.

How decision makers respond to an attack situation could be critical to the ultimate survival of the organisation. If or when we do detect the presence of an invasion of the corporate information, how and when should we respond to the perpetrators is important. Being reactive versus being proactive could pass the element of control over to the perpetrators. Being too heavy handed or opting for the soft touch will undoubtedly influence the behaviour of the perpetrator. What are the Duty of Care Issues and how do they impact on the corporate decision, then on the publics response to the corporate decision? Likewise with the matters relating to due diligence issues. What information should be passed on to Shareholders and or the Owners. Who has the authority to withhold this information and under what circumstances. How does the organisation manage the media and media relationships during a crisis situation?
REFERENCES


