2007

Network Security Devices and Protocols Using State Model Diagrams

C. Nuangjamnong
Edith Cowan University

D. Veal
Edith Cowan University

S. P. Maj
Edith Cowan University

DOI: 10.4225/75/57b53069b8756
Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007.

Network Security Devices and Protocols Using State Model Diagrams

C. Nuangjamnong, D. Veal, S. P. Maj
School of Computer and Information Science
Edith Cowan University
2 Bradford, Mount Lawley, 6050, Western Australia
cnuangja@student.ecu.edu.au

Abstract

Network security is concerned with protecting sensitive information, limiting unauthorised access, and reinforcing network performance. An important factor in network security is encryption. Internet Security Protocol (IPSec) is the de facto open standard for encryption and replaces the older Cisco Encryption Technology (CET). Both encryption protocols are typically implemented and managed using the text based Command Line Interface (CLI). A graphical user interface (GUI) is available; however, it is not routinely used. Regardless of whether the CLI or GUI is used, both encryption suites are complex to implement and manage. State Model Diagrams (SMDs) were developed and successfully used as the pedagogical foundation of internetworking technologies. SMDs integrate pertinent output from devices and protocol finite state information. SMDs are modular and hierarchical models thereby providing top down deconstruction as a cascaded structure. In terms of ease of use, hyperlinks may be used to navigate between different state tables and diagrams. Moreover, as hierarchical model characteristics allow technical detail to be presented and integrated to assist in managing devices. In this paper, SMDs were used to evaluate CET and IPSec via experiments in order to determine their potential value as network management tool.

Keywords State Model Diagrams, Network Security, Network Encryption, Diagram

INTRODUCTION

In computer networking security, controlling complexity is a problem for many devices such as routers, firewalls, and virtual private network gateways. These devices may or may not require different configurations, depending upon their purpose (Guttman et al., 2003). Deri (1996) stated that an increasing complication and disparateness of new-networked technologies has pushed the internetworking industry and research and development fields towards a coherent way of network security management. Moreover, awareness of network security issues is an important topic for organizational business and this includes other areas where internetworking technologies are an essential part of the organizations (Deri, 1996). Furthermore, the demand for trained network security professionals has increased exponentially due to the wide range of attacks upon computer networks (Ariyapperuma & Minhas, 2005). There are an increasing number of people, practicing professionals, network managers and advanced IT students who wish to understand and cope with the basis of security in internetworking technologies in order to protect computer networks.

There is a range of security protocols to protect networks. Network security is a primary concern for many enterprise organizations, companies, and academic institutions. These organizations need to implement security throughout their corporate network to prevent unauthorized access and to protect their information (Cisco Systems, 2007a). For instance, a protocol analyser tool can read packets and gain classified information (Cisco Systems, 2002a); consequently, the use of the encryption mechanism provides a means to safeguard network information that travels from one side of the network to another, across unsecured networks. The encryption mechanism is particularly important when classified, confidential, or critical information is sent (Cisco Systems, 2003). Hence, this paper aims to evaluate the modelling of security devices and protocols with State Model Diagrams (SMDs).

THE GENERAL PROBLEMS OF NETWORK SECURITY

With a lack of appropriate network management tools, a network is exposed to huge potential direct and indirect costs due to insecure networks. Andrew (2005) noted that security is a well-known problem for the business

community. These costs include the manual operation involved in fixing problems and system downtime while the network system is maintained (Andrew, 2005).

Considering staff issues, this issue mainly relates to inappropriate user action both accidental and fraudulent. Network security and network management tools are evolving at an ever-increasing rate and so is, unfortunately, complexity. Despite an abundance of technical controls, there are still a disproportionate number of information security breaches. Schultz (2005) pointed out that fundamentally, the primary problems in network security are mostly related with network administrators and network managers, and not technical problems. People need to interact positively with technology and overly complex technologies may lead to problems. Unfortunately, some security-related technologies do not have very good usability and it requires many user interaction steps or involves non-intuitive task sequences (Schultz, 2005). Moreover, Johnston et al. (2003) note that most computer users are exposed to technology through user interfaces based upon their experience, even though these interfaces were designed to help the user's understanding of and to increase productivity in using a particular technology. However, when they find it difficult to use a poorly designed interface they may not use it productively. A Graphical User Interface (GUI) ought to make a computer system as easy to use as possible; conversely, work by Johnston et al. (2003) suggests that security GUIs are merely more complex and may make a system more difficult to use.

According to Wool (2004), a system administrator must have sufficient experience to configure and manage the computer system in order to realize an appropriate security policy for the particular needs of the company manages its firewalls. A firewall configuration consists of a sequence of filtering rules and each filtering rule has a matching part, and an action part. The matching part of a rule consists of values for various fields in a packet header. When a packet enters the firewall, the firewall runs through a sequence of rules until it finds a rule that matches the header values in this packet, and takes action to apply in that rule. If no rule matches, a default action occurs.

Cisco internetworking devices and protocols are often configured and managed using by the hierarchical text based – Command Line Interface (CLI). The CLI is a tool used by practicing professionals but novices find it difficult to use and may be assisted to gain understanding via the use an appropriate model (Maj & Tran, 2006). According to Barnett et al. (2001), a model is a powerful learning tool for helping people understands complex systems. In particular, learning and managing the methods and processes of computer systems through models may result in a better understanding for the learners (Jackson et al., 1995). SMDs were designed in order to assist learning (Maj & Kohli, 2004). SMDs are a type of diagrammatic modelling method and are based upon abstraction. Abstraction has been used by many researchers to mean a process, or a model of identifying details which, in a given context, are essential. These details should be visible while non-essential details can be hidden (Frantz, 1995; Veal, 2003; Perrennet et al., 2006). In addition, levels of abstraction can assist to identify common components of objects, processes, and models in a way that makes those components re-usable in more than one context without needing to repeat all these details in every context (Maj et al., 2000). Both the encryption suites, IPSec and CET, are complex to implement and manage. SMDs were successfully used as the pedagogical foundation of internetworking technologies. SMDs integrate pertinent output from devices and protocol finite state information. SMDs are modular and hierarchical models thereby providing top down deconstruction as a cascaded structure. In terms of ease of use, hyperlinks can be used to navigate between different state tables and diagrams. Hierarchical model characteristics allow technical detail to be presented and integrated to assist in managing network security devices.

Furthermore, the data from the text-based CLI of internetworking devices can be extracted into the SMDs. An example of SMDs is two personal computers connected to a router as shown in figure 1. SMDs are diagrammatic, and easy to use and to understand. According to Maj, Kohli and Murphy (2004), the models are deconstructed as a hierarchical top-down structure, which covers the essential information concerning all networking devices. The models also provide a useful framework, via the OSI model, to categorise devices and protocols, while the details within SMDs are associated with networking device configuration (Maj & Tran, 2006). In addition, the diagram extracts the relevant data from the different CLI outputs and then transforms such data into a simple single diagram (figure 1):

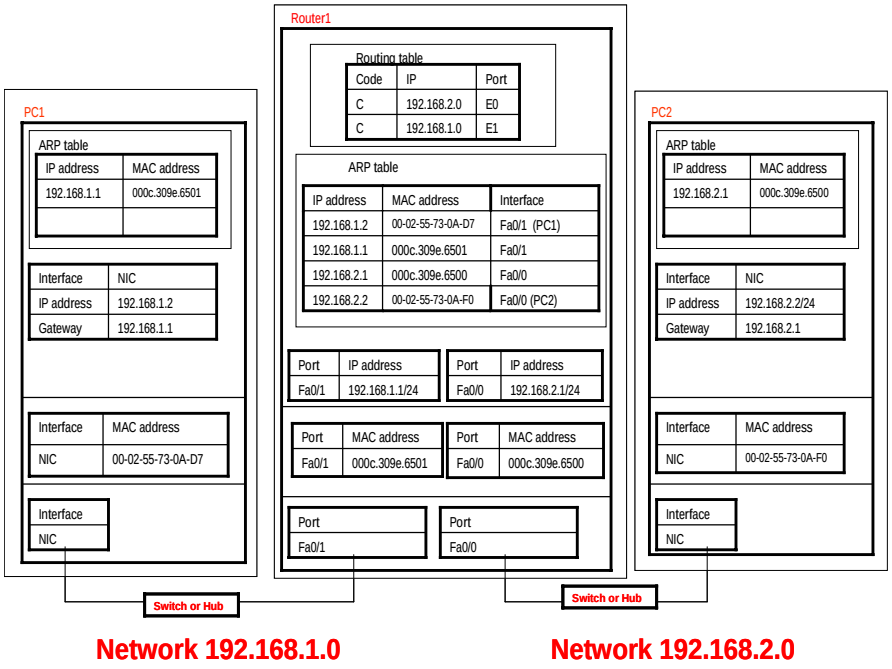

Figure 1: a SMD for the simplest network (Maj, 2007)

According to Maj et al. (2005), the advantages of using SMDs for controlling details in internetworking devices are:

- Only essential key information from CLI are conveyed
- The SMD contains sufficient information for managing internetworking devices
- As a diagrammatic and abstract model, the SMD is easy to use and improves the understanding of the network and users will have logical and physical views of the network
- SMDs allow hierarchical top-down structure to control details

In October 1997, Cisco Systems launched The Cisco Networking Academy Program (CNAP) at a cost of US $75 million. CNAP courses are available in approximately 10,000 local academies, in over 150 different countries and there are approximately 500,000 participating students (Cisco Systems, 2007b). Most CNAP contents are based on the CLI, which provides both advantages and disadvantages. In terms of advantages, CLI is a common interface tool, which provides greater control of the system. CLI consumes less computer resources as it operates on text-based commands. However, CLI does not offer the ability to view in multiple computer screens, and is difficult for novices to use effectively. More complex systems and large networks require memorization of certain factual situations, and use more complex CLI, in order to gain network familiarity to operate the security systems. Hence, the CNAP curriculum, as known, has no simple diagrammatic model; this circumstance makes CLI is difficult to get efficiently, information for managing and controlling network security. This problem is exacerbated for large networks.

Computer models are often based upon conceptual models (Maj et al., 2000; Menasce et al., 1999). Models should be easy to use and to understand. These models should not depend too much on the core technology, and they should provide the users with a more meaningful communication in term of the way of looking at the systems. In addition, they should offer the ability to hide none-essential information with top-down deconstruction, so that the models offer the user to construct meaningful information (Maj et al., 2004). Moreover, Menasce et al. (1999) noted that a model could be described as the body of information about a system for studying the system. Thus, SMDs are visual models, which take advantage of any of these limitations to display simply the operation of the network, by using simple diagrams. SMDs also represent the theoretical concepts of the internetworking technologies in use. By integrating the SMDs into network security devices and

network protocols, network administrators, network specialists and IT professionals can have a complete picture of the network and its security this yields a better understanding and a better view of the physical as well as logical network topologies.

In regarding computer security, the British Computer Society (BCS) (2004) states that computer systems are becoming more complex and in some situations, there is no exactly correct way to control how they work. This issue also relates with the commands that are used for controlling and managing the systems. The Command Line Interface is found on network devices such as routers, switches, and firewalls. The interface allows the management and controlling of those network devices. The major advantages and disadvantages between a CLI and a GUI are described as follows:

> ***Characteristics:*** CLI lacks in style it makes up for in speed and functionality, and the only tools necessary are a shell prompt, some service specific commands, and a simple text editor. For GUI, the interface is easier for the novice administrator, but the GUI tool often lacks completeness or efficiency for the administrator.
>
> ***Ease:*** because of the need for memorization and experience needed to operate a command line interface. New users find it difficult to navigate and operate a command line interface while new GUI users may have a difficult time for learning to use the mouse to monitor the systems, but using GUI interface should be much easier when compared to a command line interface.
>
> ***Control:*** a command line interface has much more control of a file system and operating system whilst a GUI provides plenty of control of a file system and operating system. However, advance users may require a superior command for that task.
>
> ***Speed:*** a command line interface often only needs to execute a few lines to perform a task. For an advanced command line interface users, CLI would be able to get something done faster then GUIs.
>
> ***Multitasking:*** many command line environments have competent of multitasking, but they do not provide the ability to view multiple things at once on one screen. For GUIs, GUI users have windows that allow a user to view, control, and manipulate multiple things at once, which are commonly much faster to do when compared to a command line.
>
> ***Low resources:*** a computer, which is only using the command line consumes much less of the computers resources while a GUI will require a lot more system resources because of each of the elements that need to be loaded such as icons, fonts and drivers.
>
> ***Scripting:*** A command line interface allows users to write a sequence of commands for performing a task or executing a program. For GUIs, users need to create shortcuts, tasks, or other similar actions to complete a task before running a program.
>
> ***Remote access:*** By accessing, another computer or networking device across a network, user will be able to manipulate the devices and files through using a command line, CLI, or other text manipulation. With GUIs, remote graphical access is becoming popular and is possible. Not all computers and particularly not all network equipment will have this ability.

(Sisler, 1999)

NETWORK SECURITY MANAGEMENT

Network security management is a complex process for managing and controlling which requires knowledge and experience. Ariyapperuma et al. (2005) state that the demand for trained network security professionals has increased regularly due to the wide range of attacks on computer network. Therefore, network security technology plays an important role for protecting all types of sensitive information and network resources. There are two types of data encryption, which currently use to protect the information between computer networks: Cisco Encryption Technology (CET) and Internet Protocol Security (IPSec).

CISCO ENCRYPTION TECHNOLOGY (CET): ROUTER TO ROUTER

Packet filtering devices such as routers, firewall systems and encryption are important components of network layer access control (Guttman et al., 2003). This also includes a network data encryption mechanism, which is provided at the network layer (layer 3), and it can be encrypted. An IP packet is encrypted and decrypted only if

the packet meets criteria that have been established, and the configuration of a router for encryption is set. The actual encryption and decryption of IP packets takes place only at routers that are used to configure CET (Cisco Systems, 2003). The routers themselves are considered to be peer-encrypting routers while intermediate hops do not participate in the encryption and decryption process as shown in figure 2.

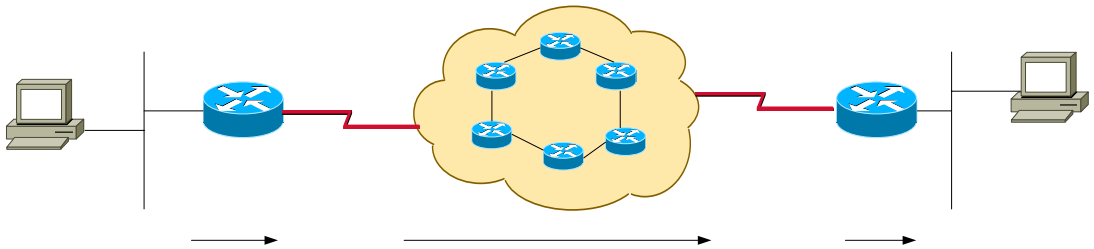

Figure 2: IP Packet Encryption (Cisco Systems, 2003)

Actual text or clear text, not encrypted, traffic that enters a peer router from the secure network side, is encrypted, and then forwarded across the unsecured network. When the encrypted traffic reaches the remote peer router, the router decrypts the traffic before forwarding it into the remote secure network. IP Packets are encrypted between the original router's outbound interfaces and decrypted at the terminal peer router's inbound interface (Cisco Systems, 2003). Encryption provides the use of a hidden transformation that requires a secret key to encrypt and to reverse the process (decrypt). However, some encryption methods can use the same key to both encrypt and decrypt the data. In encryption, there are two keys: one key to encrypt and another different one to decrypt which are referred to as asymmetric encryption. In an asymmetric encryption, one of the two keys is publicly known and the other is kept secret (Pike, 2002).

For the duration of the setup of every encrypted session, both participating routers try to validate each other. If both authentications fail then the encrypted session will not be established, and no encrypted traffic will pass. Both authentications guarantee that they know each other in terms of trusted routers exchanging encrypted traffic, and prevent routers from being tricked into sending sensitive encrypted traffic to illegitimate destination routers (Cisco Systems, 2003).

Actual Data
Clear-text

Encrypted Data

INTERNET PROTOCOL SECURITY (IPSEC): ROUTER TO ROUTER

In the context of the OSI reference model, there are several strategic methods whereby an encryption mechanism may be applied. An IPSec is a framework of protocols, and the Internet Engineering Task Force (IETF) developed it. The protocols provide security for IP packets and any upper-layer protocol that uses IP services (SANS Institute, 2001).

IPSec provides security for the transmission of sensitive information over unprotected networks which acts at the network layer (Layer 3) by protecting and authenticating IP packets between participating IPSec devices, for instance, Cisco routers (Cisco Systems, 2002a; Pike, 2002). Network security services with IPSec are provided as optional services. These services are:

Data Confidentiality: the IPSec sender will encrypt packets before transmitting them across a network

Data Integrity: the IPSec receiver will verify packets sent by the IPSec sender to ensure that the data has not been changed during communication

Data Origin Authentication: the IPSec receiver will authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service

Anti-Replay: The IPSec receiver can identify and reject replayed packets

(Cisco Systems, 2002a; Pike, 2002)

By using IPSec, data can be transmitted across the Internet or any public network without fear of observation and modification. This feature also enables applications, namely Virtual Private Networks (VPNs), intranets,

extranets, and remote user access. IPSec provides secure tunnels between two peer routers. If IP packets are considered sensitive, and they should be sent through these secure tunnels, where they will be defined by additional parameters. Then, when the IPSec inside the peer router sees a sensitive IP packet, it sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer. In the IPSec tunnels, there are sets of security associations that are established between two peer routers. The security associations identify which protocols and algorithms should be applied to sensitive packets, and indicate the security key to be used by the two peer routers. The IPSec mechanism will define what traffic should be protected between two peer routers by configuring access lists and applying these access lists to interfaces by way of crypto map sets. Therefore, traffic may be selected based upon source and destination address, and port number.

CET and IPSec are similar in that the access lists are used only to determine which traffic is protected by IPSec and CET, not which traffic should be blocked or permitted through the interface, should protect. Common uses of access lists on router configurations define blocking or permitting at the appropriate interfaces. A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched by the router which attempts to match the packet to the access list specified in that entry. After that, when a packet matches a "permit" entry in a particular access list and the corresponding crypto map entry is tagged, then IPSec is triggered, and connections are established if necessary. Additionally, IPSec uses the Internet Key Exchange (IKE) to negotiate with the remote peer router to establish the necessary IPSec security associations on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry (Cisco Systems, 2002a; Pike, 2002). Therefore, access lists associated with IPSec crypto map entries also represent which traffic the router requires to be protected by IPSec. Inbound traffic is also processed against the crypto map entries. If a packet matches a permit entry in a particular access list associated with an IPSec crypto map entry, that packet is dropped because it was not sent as an IPSec-protected packet.

STRENGTHS AND WEAKNESSES OF CET AND IPSEC

CET is a proprietary security solution introduced by Cisco Systems. Network data encryption is presented at the network level (layer 3) and standards are consistent: Digital Signature Standard (DSS), Diffie-Hellman (DH) public key algorithm, and Data Encryption Standard (DES). The Internet Engineering Task Force (IETF) developed IPSec, which is a framework for open standards to provide security for transmission of sensitive data over undefended networks. Similar to CET, IPSec is implemented at the network level (layer 3) and the implementation of standards is involved with IPSec, Internet Key Exchange (IKE), Data Encryption Standard (DES), MD5 (HMAC variant), SHA (HMAC variant), Authentication Header (AH), and Encapsulating Security Payload (ESP). Data authentication, data confidentiality services, and anti-replay services are provided in IPSec mechanisms, while CET provides only data confidentiality services (Cisco systems, 1998; Pike, 2002). More significantly, IPSec is a modular open standard.

DISCUSSION MODELLING SECURITY DEVICES AND PROTOCOL USING SMDS

Security devices and their associated protocols can therefore be quite complex with the corresponding network management problems. Even a simple configuration error on a firewall may lead to major security risk. Models are very useful diagrammatic forms for controlling detail and extracting complex information (Taylor, 2000). Significant model characteristics include diagrammatic, self-documentation, easy to use, and hierarchical top down deconstruction to manage every detail. By providing levelling a complex systems can be progressively analysed while still maintaining necessary links. Maj et al. (2004) suggest that internetworking devices such as switches and routers could be diagrammatically represented using a collection of tables called State Model Diagrams (SMDs). The research by the authors shows that SMDs were successfully used for teaching internetworking technology curricula.

According to Maj et al. (2004, p.10), "Using the models it is relatively easy to understand the purpose and structure of the devices. The models include implementation details, derived from CLI commands, hence it is possible to verify and validate device operation. The modular nature of these diagrammatic models allows the user to appreciate the interaction between the different protocols operating on a device. Furthermore, the modularity allows one to have a basic model (e.g. a router running the RIP routing protocol) whose functionality can be enhanced by the inclusion of additional state tables. Hence the router state model can be used for all the main Interior Gateway Protocols – distance vector (RIP, IGRP), link state (OSPF) and advanced hybrid (EIGRP)."

In CET and IPSec, an access-list is applied to encrypt all of data related in IP address; thus, by using ping command the results from each station that connects with the router can be operated. For CET, no encryption has been associated on web pages on each station including each web page is not encrypted and decrypted when

the data are sent and received (Figure 3). However, in IPSec, the encryption is associated with web pages on each station that connects with router; therefore, each web page is encrypted and decrypted when the data are transmission (Figure 4).

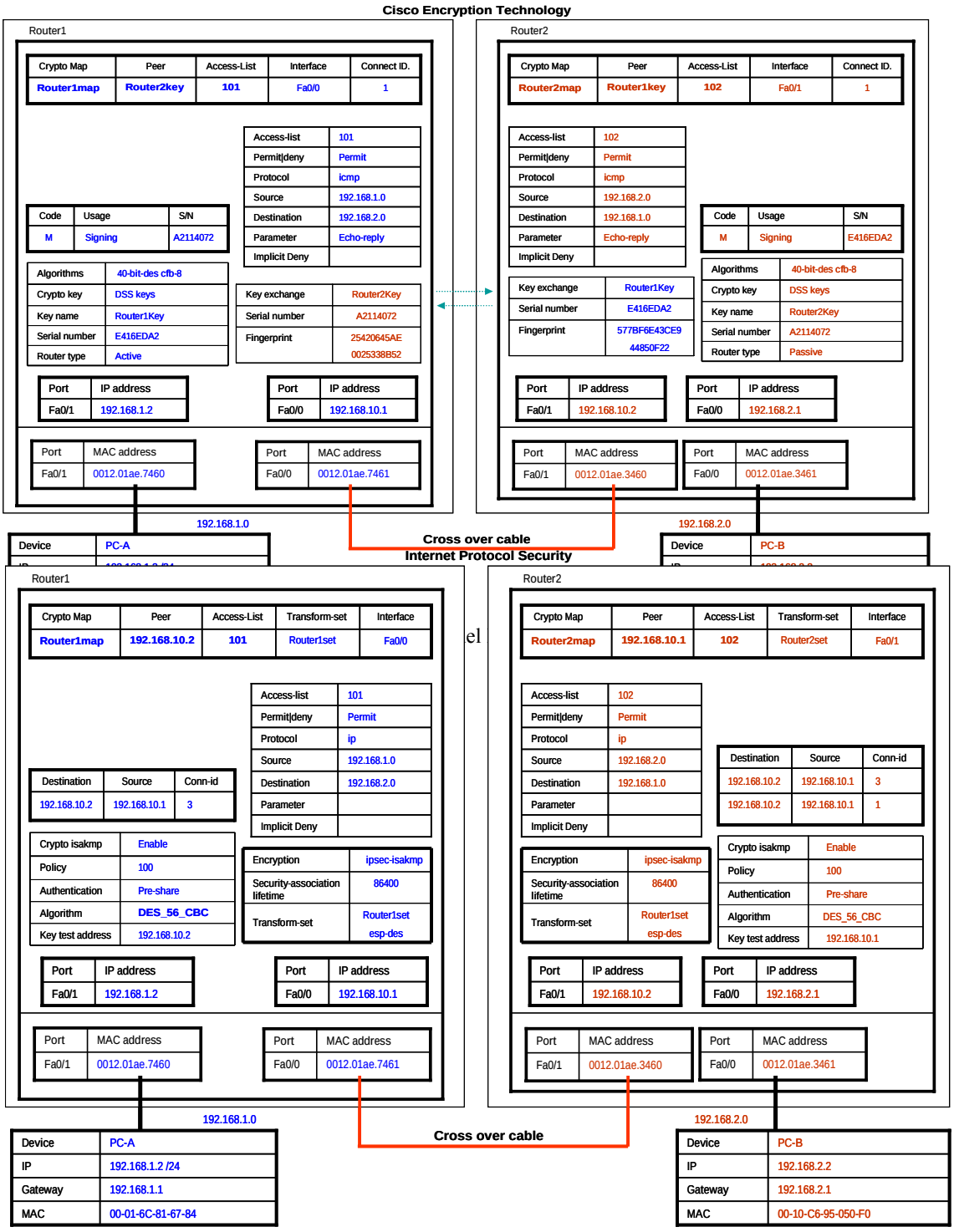

Figure 4: State Model Diagram for IPSec

As a pedagogical tool, the SMDs explicitly integrate the TCP/IP and OSI Reference Model. One of the most important features of SMDs is to be able to construct a variety of different levels according to the level of

abstraction required (Maj et al. 2005). By focusing on the definition of SMDs, at the initial stage of the diagrams, it can be applied into a high-level stack of protocols, which is used to connect between interconnection devices. Internetworking devices (switches and routers) are connected together to draw a map and then using CLI information map this data with the diagrams. After that, the details of a specific device are needed, and the greater technical complexity for that specific device can be acquired. Apparently, the different levels of diagram remain stable. The diagrams may be deconstructed to the sublevel that is meaningful for the specific purpose, and the diagrams are involved if necessary.

CONCLUSION

A number of studies have clearly demonstrated improved learning outcomes when the network curriculum were based on SMDs. Significantly SMDs are a universal template that can be used for all network devices and associated protocols based on finite state machines. Using SMDs it was possible to extract key data from the different CLI outputs in order to populate the SMDs of firewalls running two different security protocols, CET and IPSec. It can clearly be seen that the SMD of a firewall is diagrammatic and hence clearly shows the relevant detail. Furthermore, firewall SMDs may be used to document a device. Because the key information is consolidated into a single diagram, it is relatively easy to understand the purpose and structure of network security configurations. It is therefore relatively simple to verify and validate firewall and protocol operation – an essential aspect of network management and fault diagnosis. SMDs employ the principle of levelling and information hiding; hence, the details of quite a large secure network may be managed.

REFERENCES

Andrew, C. (2005) The five Ps of patch management: Is there a simple way for businesses to develop and deploy an advanced security patch management strategy? *Computer & Security*, 24(5), 362-363, URL http://www.elsevier.com/locate/cose/, Accessed 23 May 2007

Ariyapperuma, S., & Minhas, A. (2005) Internet security games as a pedagogic tool for teaching network

Security, *Frontiers in Education, 2005. FIE '05. Proceedings 35th Annual Conference*, URL http://www.ieee.org, Accessed 12 August 2007

Barnett, M., MaKinster, J. G., & Hansen, J. A. (2001) Exploring elementary students' learning of astronomy through model building, URL http://inkido.indiana.edu/mikeb/portfolio/papers/VSS_barnett_hansen_McKinster.pdf, Accessed 9 March 2007

BCS. (2007) Thought leadership. IT systems: scale, complexity and risk, URL http://www.bcs.org/, Accessed 2

August 2007

Cisco Systems. (1998) IP security and encryption overview, URL http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scencove.htm, Accessed 20 April 2007

Cisco Systems. (2002a) IPSec network security, URL http://cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_3/ipsec.htm, Accessed 3 April 2007

Cisco Systems. (2002b) Basic firewall configuration, URL http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/bafwcfg.htm, Accessed 3 April 2007

Cisco Systems. (2003) Cisco encryption technology (CET), URL

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scencryp.htm, Accessed 19 March 2007

Cisco Systems. (2007a) Cisco powered network: managed security services designation, URL

http://www.cisco.com/warp/public/cc/so/neso/sqso/mnsqss/prodlit/mss_ov.pdf, Accessed 15 March 2007

Cisco Systems. (2007b) Academy connection, URL http://www.cisco.com/web/learning/netacad/index.html,

Accessed 25 March 2007

Deri, L. (1996) Network management for the 90s, URL http://www.sce.carleton.ca/netmanage/NMfor90s/SimpleNM.html, Accessed 18 March 2007

Frantz, F. K. (1995) A taxonomy of model abstraction techniques. *Proceeding of the 1995 Winter Simulation Conference*, 1413 – 1420, URL http://www.acm.org/, 13 March 2007

Guttman, J. D., & Herzog, A. L. (2003) Rigorous automated network security management, URL http://www.ccs.neu.edu/home/guttman/ransm.pdf, Accessed 12 March 2007

Jackson, S., Stratford, S. J., Krajcik, J., & Soloway, E. (1995) Making system dynamics modelling accessible to pre-college science students, *Paper presented at annual meeting of the American Educational Research Association*, San Francisco, CA.

Johnston, J., Eloff, J. H. P., & Labuschagne, L. (2003) Security and human computer interfaces. *Computer & Security*, 22(8), 675 – 684, URL http://www.elsevier.com/locate/cose/, Accessed 23 May 2007

Maj, S. P. (2007). Diagram in fundamentals of computer and network technology: lecture note, [Handout], Available from Edith Cowan University, Perth, Western Australia.

Maj, S. P., & Tran, B. (2006) Network technology education: a novel pedagogical model for novices and practising professionals, *Teaching and Learning Forum 2007*, URL http://lsn.curtin.edu.au/tlf/tlf2007/refereed/maj.html, Accessed 16 March 2007

Maj, S. P., Kohli, G., & Fetherston, T. (2005) A pedagogical evaluation of new state model diagrams for teaching internetworking, *ACM International Conference Proceeding Series*, *102*; *Proceedings of the Twenty-eighth Australasian conference on Computer Science*, 38, 135 -141,URL http://www.acm.org/, Accessed 29 April 2007

Maj, S. P., & Kohli, G. (2004) A new state models for internetwork technology, *Journal of Issues in Informing Science and Information Technology*, 1, 385 – 392, URL http://proceedings.informingscience.org/InSITE2004/062maj.pdf, Accessed 5 April 2007

Maj, S. P., Kohli, G., & Murphy, G. (2004) State models for internetworking technologies, *Frontiers in Education, 2004, FIE 2004*, *34th Annual,* 20-23 (2), 10 – 15, URL http://ieeexplore.ieee.org/, Accessed 29 April 2007

Maj, S. P., Veal, D., & Duley, R. (2000) A proposed new high level abstraction for computer technology, *ACM*

SIGCSE 2001, Charlotte, NC, USA, February 2001, 199 – 203, URL http://www.acm.org/, Accessed 15 August 2006

Menasce, D. A., Almeida, V. A. F., Fonseca, R. C., & Mendes, M. A. (1999) A methodology of workload characterization for E-commerce server, *Paper presented at ACM Conference in Electronic Commerce*, Denver, CO., URL http://www.acm.org/, Accessed 15 August 2006

Pike, J. (2002) Cisco network security. New Jersey: Prentice-Hall, Inc.

Perrenet, J., & Kaasenbrood, E. (2006). Levels of abstraction in students' understanding of the concept of algorithm: the qualitative perspective, *Proceedings ITiCSE*, Bologna, Italy, 270 – 274, URL http://www.acm.org/, Accessed 10 August 2006

SANS Institute. (2001) Implementing site-to-site IPSec between a Cisco router and linux freeS/WAN, URL http://www.securitydocs.com/library/1341, Accessed 18 April 2007

Schultz, E. (2005) The human factor in security, *Computer & Security*, 24(6), 425 – 426, URL http://www.elsevier.com/locate/cose/, Accessed 22 May 2007

Sisler, E. (1999) System administration: CLI or GUI, URL http://wallace.westminster.lib.co.us/linux/cli-vs-gui.html, Accessed 26 May 2007

Taylor, K. (2000) Taylor diagram definition, URL http://www.ipsl.jussieu.fr/~jmesce/Taylor_diagram/,

Accessed 20 April 2007

Veal, D. (2003) An investigation into computer and network curricula, Ph.D. dissertation, Edith Cowan

University, Perth, Western Australia.

Wool, A. (2004) The use and usability of direction-based filtering in firewalls, *Computer & Security*, 23(6), 459-

468, URL http://www.elsevier.com/locate/cose/, Accessed 23 May 2007

COPYRIGHT