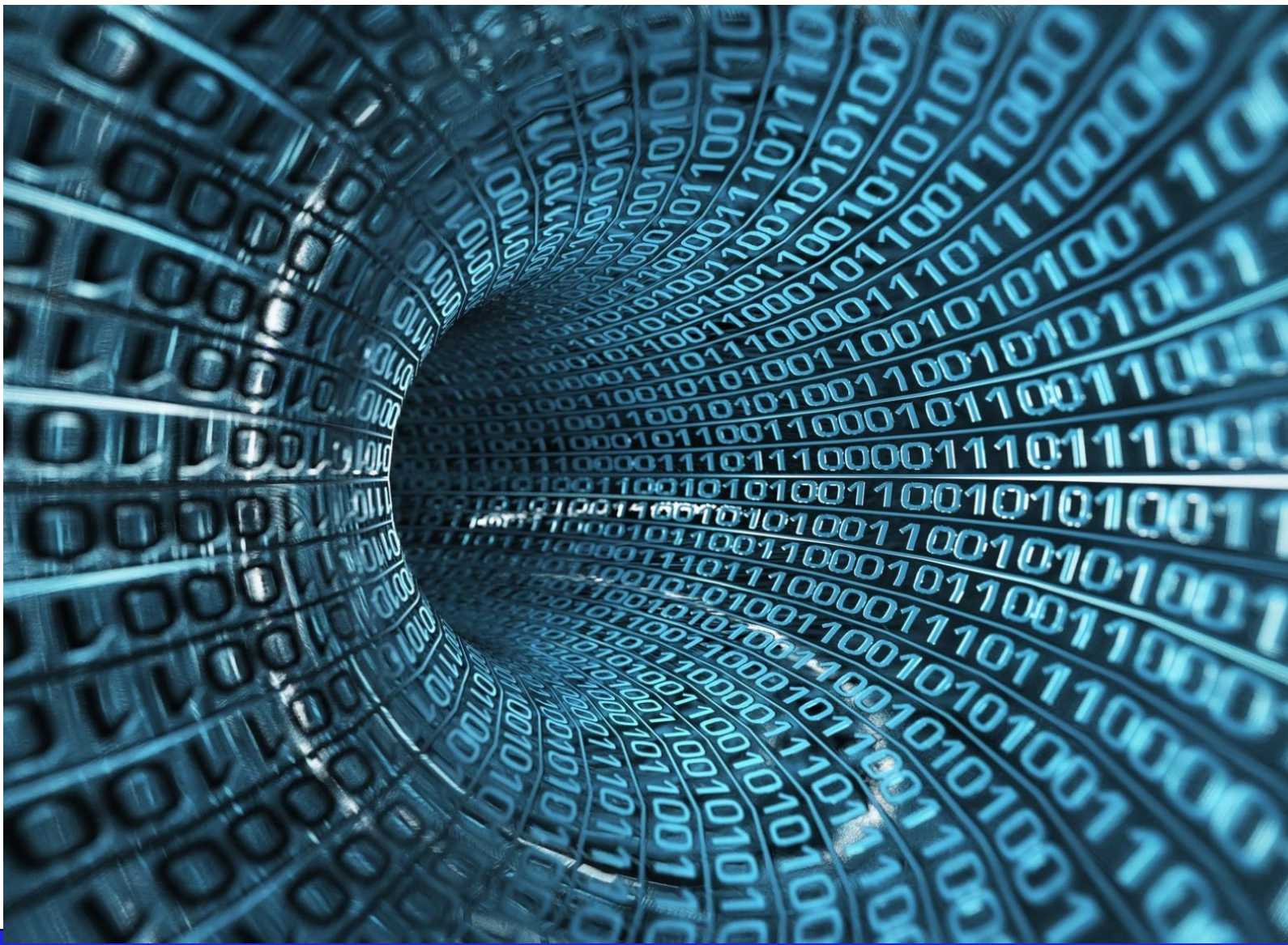
1-1-2010

The ADSL Router Forensics Process

Patryk Szewczyk
Edith Cowan University

JOURNAL OF NETWORK FORENSICS



Volume 2 Issue 1
Autumn, 2010

Journal of Network Forensics

Volume 2 Issue 1

ISBN 1834-5336 (Print)
ISSN 1834-5344 (Online)

secau - Security Research Centre
Edith Cowan University
270 Joondalup Drive
Joondalup Western Australia

Journal of Network Forensics

FOCUS AND SCOPE

The journal is a platform for contemporary research into network forensics. Network forensics is the study of forensics as it relates to network data and network devices.

PEER REVIEW PROCESS

All articles submitted for review are double blind peer reviewed. Articles submitted for review will be judged on the following criteria:

- Originality
- Contribution to discipline
- Readability
- Suitability for the Journal

CHIEF EDITOR

EDITORIAL PANEL

EDITING AND LAYOUT

Table of Contents

Editorial

Welcome to the second issue of the Journal of Network Forensics. The journal aims to provide a platform for the scholarly discussion of advances and techniques related to the forensic acquisition of data from networks, network centric information systems and associated client devices. The journal is the second security related journal published by secau - Security Research Centre at Edith Cowan University with now long-running Journal of Information Warfare being the first.

The first article in this issue is about the forensic acquisition of evidence from ADSL routers using a variety of techniques to access information stored in memory of these devices. The second and third articles were selected from the fifth annual conference of the ADFSL Conference on Digital Forensics, Security and Law was held in St. Paul, Minnesota, USA on May 19-21, 2010. These articles focus on the forensics relating to the use of social networking forums and services.

The second call for papers is currently out and can be accessed from the secau - Security Research Centre homepage at http://www.secau.org where you will also find details of subscription as well as submission requirements for authors.

Craig Valli
Editor
Journal of Network Forensics
secau - Security Research Centre
http://www.secau.org
Edith Cowan University
Perth, Western Australia

About the Authors

Richard Mislan
Richard Mislan is an assistant professor specialising in the area of Cyber Forensics at Purdue University. Richard's areas of research include Small-Scale Digital Device Forensics, Unusual Sources of Digital evidence, Mobile Malware and Spyware, and the Application of Artificial Intelligence Techniques for Improving Efficiency in Cyber Forensics. He is also a faculty member with the Center for Education and Research in Information Assurance and Security (CERIAS).

Tejashree Datar
Tejashree Datar is a PhD Student in the Purdue University Cyber Forensics department. He received an undergraduate degree in Electronics and Telecommunication from the University of Pune in India. He received a Masters degree from Oklahoma State University in Telecommunications Management. During his Masters studies, Tejashree took a course in Digital Forensics and from there became interested in the field of Cyber Forensics.

Bill Harshbarger
Bill Harshbarger is the IT Security Engineer at Purdue University. He has a Bachelor of Science in Telecommunications and Networking Technology, and a Masters of Digital Forensics at Purdue University. He is a member of the Association of Information Technology Professionals (AITP) and he is involved in performing security assessments, penetration testing, web application scanning, and vulnerability scanning at the university.

Patryk Szewczyk
Patryk Szewczyk is currently a lecturer within the School of Computer and Security Science at Edith Cowan University. He completed a first class honours degree in the field of users' perceptions of wireless security. This has then continued into undertaking PhD research in Computer Security in the field of ADSL Router Forensics. His research interests include ADSL router forensics, embedded system forensics, penetration and vulnerability testing of SoHo security applications, and the analysis of end-user behaviour in computer and network security.

The ADSL Router Forensics Process

Patryk Szewczyk
secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
p.szewczyk@ecu.edu.au

Abstract
In 2010 the number of threats targeting ADSL routers is continually increasing. New and emergent threats have been developed to bypass authentication processes and obtain admin privileges directly to the device. As a result many malicious attempts are being made to alter the configuration data and make the device subsequently vulnerable. This paper discusses the non-invasive digital forensics approach into extracting evidence from ADSL routers. Specifically it validates an identified digital forensic process of acquisition. The paper then discusses how the approach may be utilised to extract configuration data ever after a device has been compromised to the point where a lock-out state has been initiated.

Keywords
ADSL routers, digital forensics, router forensics, psyb0t, SoHo

INTRODUCTION

According to the latest Australian Bureau of Statistics report, there are currently over nine million active Internet connections in Australia alone. Of these approximately ninety percent comprise of non-dialup connections (ABS, 2009). With the continuing fall of broadband pricing, individuals have further incentive to adopt a broadband Internet connection. The main incentive behind adopting a broadband Internet connection is due to dialup connections becoming obsolete. This outdated technology is no longer suitable from a performance perspective for Small office Home office (SoHo) environments.

To obtain a broadband Internet connection, individuals are required to utilise an Asymmetric Digital Subscriber Line (ADSL) router. SoHo users benefit from vendors shipping ADSL routers preconfigured with common networking requirements. This allows consumers to bypass the tedious configuration process and connect to the Internet in a streamlined manner. Within Australia, Internet Service Providers (ISPs) are further supporting end-users in providing ADSL routers pre-configured with the client's username and password. In-turn this permits the end-user with little knowledge of Information Technology, to simply connect the physical cables and be on the Internet within seconds.

All these preconfigured networking devices come at a significant cost. Conversely, pre-configured ADSL routers usually incorporate little or no security. This may reduce the amount of skill required to initially utilise the device. However, this also results in the security aspects employed not protecting the device itself, or the internal hosts. As a result

many SoHo ADSL routers are vulnerable to a range of emerging threats. The number one method by which to secure an ADSL router is to change the default password to something less evident. Unfortunately, the majority of vendors do not encourage end-users to undertake this process (Szewczyk & Valli, 2009). As a result changing of the password may be omitted by SoHo users leaving the device vulnerable.

Since 2008, the number and sophistication of manufactured threats and identified vulnerabilities targeting ADSL routers has increased significantly. To date there are limited scholarly publications detailing the motives to compromise and control a router. As a general rule, ADSL routers are the first electronic device in a SoHo network. As a result, it is appealing for attackers to compromise and control a vulnerable router, compared to attempting to dominate internal hosts. Internal hosts may encompass the latest operating system updates, personal firewalls and anti-virus software. In contrast, SoHo or enterprise grade routers do not have methods by which to detect and/or remove malware or prevent security breaches from occurring.

Typically an ADSL router is manufactured by vendors to be accessed through internal IP addresses only. However, emergent threats are compromising the device from external IP addresses. The default firmware on many first generation Netcomm routers, encompassed a web server flaw which permitted the device to be accessed, compromised and controlled via a host external to the network (Sajdak, 2009). In contrast, SourceSec (2010) has also developed and published a proof-of-concept tool designed to compromise D-Link ADSL routers from external IP addresses. The tool named “HNAP0wn” (Kirk, 2010) allows an un-authenticated or un-privileged user to manipulate configuration settings on a range of D-Link networking devices. In both of these cases, the intention behind the attack is to alter the configuration of the router to allow the controller to redirect traffic, and manipulate the devices behaviour – creating a zombie in a botnet farm. The botnet consisting of compromised hosts may be used to initiate subsequent Denial of Service attacks towards vulnerable hosts.

Whilst ADSL routers are susceptible to manual attacks, automated worms are beginning to compromise SoHo based devices which encompass MIPS processor architectures. Forms of malware including “Psyb0t” (Baume, 2009; Hunt, 2009) and the “Chuck Norris” worm (McMillan, 2010) have been specifically designed to alter configuration settings through autonomous methods. The beneficial aspect of these two worms (for the attacker) is that an unsuspecting victim may download the malware onto their computer whilst on the Internet. To date anti-virus vendors are not openly admitting that they can actively detect and remove the worm from a workstation, resulting in a continuous re-infection to the router.

Malware on ADSL routers tends to reside in Random Access Memory (RAM). The simplest known method by which to remove malware is through a power-cycle process. This instruction is in most instances provided to end-users whom contact their ISP, in the event of the ADSL router malfunctioning. Unfortunately even if the malware is removed through a power cycle, the modified configuration settings will remain intact, and a re-infection, from the internal workstation is highly likely. This is due to the malware specimen residing

on the victim's workstation, often undetected by anti-virus scanners. Psyb0t and the Chuck Norris worm both attempt to modify and fabricate configuration settings specific to the attacker's requirements for control.

THE NECESSITY FOR ADSL ROUTER FORENSICS

Computer forensics is a discipline generally pertaining to the extraction of legal evidence from computers and digital storage mediums. Modern digital devices including computers, PDA, mobile phones and GPS devices have a reasonable amount of storage space and processing power. As a result, these mentioned devices may store a vast amount of media, files, and personally identifiable information. Unfortunately many ADSL routers are limited in storage and processing power. The D-Link DSL-G624T and Netgear DG834Gv4 (OpenWRT, 2010) which are popular, high-end routers have at most four megabytes of flash coupled with sixteen megabytes of RAM. As a result the device in itself has few avenues to store potential evidence for law enforcement agencies to analyse and investigate. However, ADSL routers do encompass the entry and exit points to and from a network. By examining the configuration data, a forensic examiner may utilise the evidence to identify; where traffic is being transmitted, ports and services utilised to undertake further attacks, and other factors which may result in the device being abused by third parties.

To date there are no commercially available products or methods by which to obtain and analyse evidence from ADSL routers. The field of ADSL router forensics is relatively new, although there is significant interest from law enforcement agencies. In 2009 a paper entitled "*ADSL Router Forensics: Methods of Acquisition*" (Szewczyk, 2009b) detailed a series of acquisition methods and explained the benefits of utilising Telnet, SSH, JTAG, and a serial approach to acquire data of interest. In 2010, the United States National Institute of Justice, specially funded a project to develop an automated process of acquiring evidence from ADSL routers (Router Marshal, 2010). Whilst the developers of Router Marshal do not justify the specific necessity for such software, it is claimed that there is a significant quantity of evidence to be obtained from an ADSL router utilised within a criminal case.

ADSL router forensics may fall within the category of network forensics. However, ADSL routers encompass very limited storage. Hence, these devices generally lack the capability to monitor and store network activity – in the form of logs. The majority of ADSL routers do have a simplistic form of network logging capability. Unfortunately, none of the data is stored within the device itself. As a result the device must be configured to transmit the collected data to a specific host.

As discussed previously, vendors are already manufacturing and shipping ADSL routers in a manner to ensure a trouble free experience for the end-user. As a result, the logging feature is disabled by default on all SoHo grade networking devices. An end-user would require a significant amount of expertise to create and maintain a workstation to collect and analyse the collected logs. An examination of the network activity logs that routers can generate in the event of an incident, are in themselves inadequate. The logging capability is not designed to record security breaches of incidents. The vast majority of exploits attempt to re-configure the ADSL router, hence the configuration data is most applicable in obtaining evidence of value for a forensic examiner.

Brown (2006) suggests that based on the threats currently targeting ADSL routers that the data that would be of most value in aiding a forensic investigation includes:

- Firmware version – This aids in determining if the device in question is utilising an illegal or maliciously altered operating system.

- System time – The ADSL router stores a simple yet effective log of significant system modifications. This may enable the forensic examiner to create a timeline of events which initiated or caused the crime to take place.

- DNS address – Acquiring the DNS address may in-turn allow the investigator to determine if any redirection of traffic is occurring.

- Wireless settings – Bandwidth theft is escalating due to insecure wireless access points. Acquiring the Media Access Control (MAC) allow and deny lists, encryption keys, and determining if the access point is enabled may allow the forensic examiner to construct a scenario of events to do with the wireless network.

- Firewall rule sets – The ADSL router is pre-enabled with a set of firewall rule sets. Acquiring the current rules in place may aid in identifying how vulnerable the device in question was during an incident.

- Remote management – Many attacks attempt to enable remote management to simplify the controlling process. Acquiring remote management settings may aid the investigator in identifying to whom the permission has been enabled.

ADSL ROUTER FORENSICS

The prevalent hardware structure of ADSL routers limits the number of accessible ports to the individual acquiring the evidence. This, in-turn, makes the process significantly more challenging as the device needs to be *broken* into, to physically make contact with the correct onboard interfaces. In addition ADSL routers are typically manufactured with soldered, on-board memory components which are cumbersome to remove, and may result in device malfunction due to improper handling. As a result investigating the device in a non-invasive manner is not always feasible. In "*ADSL Router Forensics Part 2: Acquiring Evidence",* Szewczyk (2009a) demonstrates the two of methods by which data could be acquired from ADSL routers keeping in-line with digital forensic best practices. These methods are practically applied within the procedure, through the use of a Telnet or serial console approach.

One of the limiting factors of acquiring data from ADSL routers is the fact that there is no cryptographic hashing software available on the device by default. This prevents the investigator from checking the integrity of the data before and after an acquisition has occurred. As a result this limits the soundness of the acquisition and instead relies on the precision of the method followed. To validate the integrity of the data acquired the serial and Telnet approach have been stress tested on a series of ADSL routers. The forensic

examiner could load pre-compiled software onto the ADSL router, and utilise the specialised software to create a hash digest of the evidence in question and subsequently transmit this evidence to a secondary storage medium or network path. This approach may not only overwrite existing data and alter configuration evidence, but may also bring the device to a halt due insufficient RAM and processor overload.

According to the "*Good Practice Guide for Computer-Based Electronic Evidence*" (ACPO, 2003) the number one principle of acquiring electronic evidence is "*...no action... should change data held on a computer or storage media...*" which based on the research to date has successfully demonstrated that utilising a serial or Telnet approach on ADSL routers has a continuous assurance on both the integrity of data repeatability factor. As a result, these approaches are in line with not modifying data on the electronic device being investigated.

ACQUIRING EVIDENCE

Unfortunately utilising a serial approach suffers from the problem of vendor's failing to publicly release schematic diagrams and pin outs of their circuit boards. Generally the serial connection is utilised to monitor the networking state of an ADSL router by hobbyists and hackers. Hence, as the demand for methods and tools to monitor system status has increased, the open source development community has succeeded in identifying the serial ports on all ADSL router circuit boards. Upon connection of the serial cable and initialisation of the terminal software, the embedded system will continuously present data being processed by the system kernel. More importantly, the investigator may bypass this monitoring process, and directly interact with the ADSL router's operating system.

To validate the soundness and repeatability of the forensic approach, a series of empirical experiments have been conducted to verify and validate the suitability of the method to a D-Link and Netgear ADSL router. As part of the research process both of these units encompass the Texas Instruments AR7 solution chipset. This chipset is most commonly found within the majority of ADSL router products and has been utilised as the foundation for all forensic acquisitions. A series of steps have been generated to validate the acquisition process;

1. To communicate with the serial console on the ADSL router, the investigator must have access to a specifically designed communication cable. The hardware cable was based on community forum recommendations. The resultant outcome follows the publicly available schematic as demonstrated in Figure 1 (AR7 Firmware, 2009).

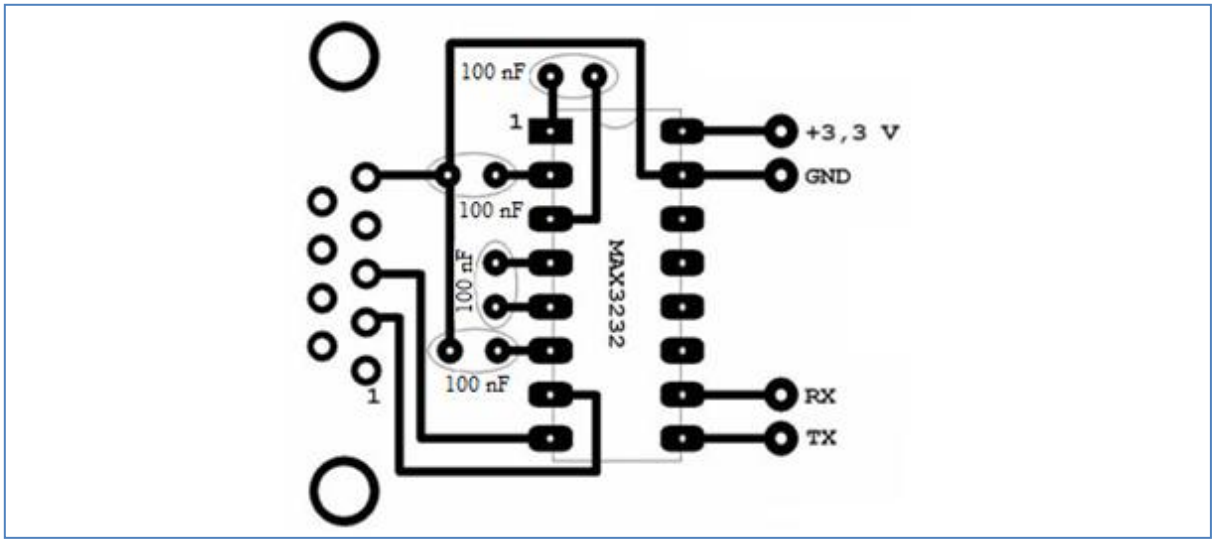


Figure 1 Serial Console Hardware Schematic

2. Upon following and constructing the schematic solutions from Figure 1, a device is constructed as per Figure 2. The devices produces input/output allowing an investigators workstation (via serial) to directly communicate with the onboard serial ports on the ADSL router. As per the diagram, the device encompasses a data transmission and receiving link, a 3.3 volt input link, and a ground link which are directly obtained from the ADSL router.

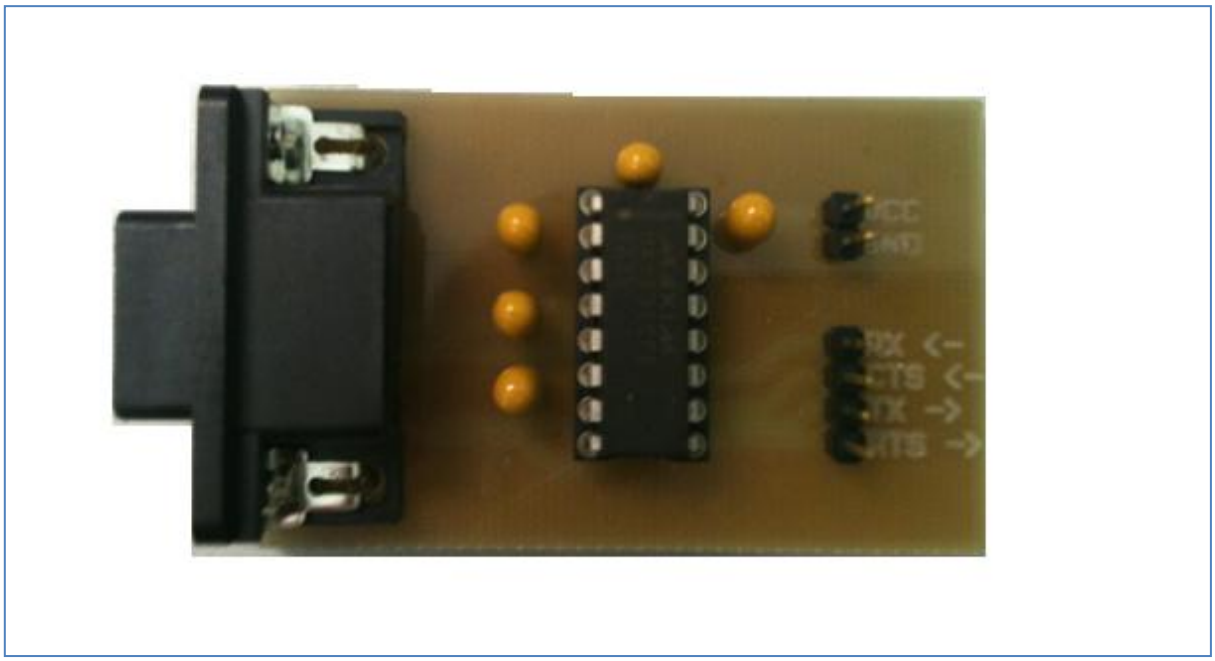


Figure 2 Finalised Serial Console Hardware

3. Both the D-Link G604t and Netgear DG834g were selected due to their market share and popularity amongst both retail chains and ISPs. Each of these devices was patched with the latest firmware directly available from the manufacturer's website. This update was applied through the web management interface of the respectful product.

4. Each ADSL router was disassembled and the serial connectivity points were identified. The serial cable and hardware were connected to each ADSL router in-turn and access via Putty. The serial client (PuTTy) must be configured to communicate with the ADSL router. The serial console settings include; 38,400 baud rate, no parity and flow control, eight (8) data bits and one (1) stop bit.

5. The acquisition method was undertaken as discussed in "*ADSL Router Forensics Part 2: Acquiring Evidence"* (Szewczyk, 2009). A baseline image of a *default* state of each ADSL router was acquired and hashed to produce an md5sum.

   This allows the configuration file to be examined to identify which processes, ports, services and functions are enabled and/or disabled as a result of third party device modification. The process of acquiring a baseline image was re-iterated through the serial based approach over a thirty cycle period. On each re-iteration the device was power cycled and a subsequent image generated.

   The evidence of this process has proven to provide a reliable image during each acquisition. The integrity of each of the acquisitions remained consistent, and the researcher had no reason to believe that the process was in any compromising the integrity of the data during the acquisition. It also became evident that the state of the configuration data is not modified as a result of a power-cycle or reset. This has significant bearing for a forensic examiner. Rather than an investigator having to acquire the device at the premises of occurrence, the device may in fact be seized, acquired and analysed at a remote location – if the configuration data is the only data of evidentiary value.

6. To simulate a compromised router, the settings on the device were altered to mimic the characteristics of a device infected with malware. Specifically, the authentication credentials were altered, Telnet and web management disabled, a random assignment of ports were opened.

7. The resultant state was that the ADSL router became inaccessible. Should a user attempt to utilise the web management facility this would result in inaccessible pages. Further to this, the Telnet facility had been disabled, thus preventing a forensic acquisition from occurring via the Telnet facility.

   Utilising the serial console approach, the device was responsive. Utilising the serial console approach described in previous research (Szewczyk, 2009a) the configuration data was successfully acquired.

8. To validate the soundness of the approach, the process was repeated over a 30 cycle period. In each instance the device was power cycled and a subsequent acquisition conducted. Whilst the device was un-responsive to the Telnet and web management approach in each of the acquisitions – the serial console approach continually proved to be successful. Further validating the process as a useful method by which to obtain data in future acquisitions.

EVIDENCE INTERPRETATION

On conclusion of each of the acquisitions an evidence.xml file is produced depicting the current state of the ADSL router. As it stands there are no elegant methods by which to interpret the data from within this file. Router Marshall (Router Marshal, 2010) appears to present data of evidentiary value in a reporting format. However, the file may still be examined and data of interest extracted by the forensic examiner.

Figure 3 depicts a series of remote management services that could be enabled on an ADSL router. By default, the vendors tend to disable or restrict access to the remote management component of these devices. In the instance of remote configurations, the default state *disabled* is represented by a numerical "1". In this particular instance the Telnet and SSH services have been disabled. However, based on the specific configuration of the ADSL router, the remote web management interface has been specifically enabled. As demonstrated by Figure 3, the state has transitioned to a numerical "0" resembling an *enabled* state.

```
<remote_telnet>
  <state>1</state>
  <RemoteHost>0.0.0.0</RemoteHost>
  <RemoteNetmask>255.255.255.255</RemoteNetmask>
</remote_telnet>
<remote_web>
  <state>0</state>
  <RemoteHost>58.7.255.236</RemoteHost>
  <RemoteNetmask>255.255.255.255</RemoteNetmask>
</remote_web>
<remote_ssh>
  <state>1</state>
  <RemoteHost>0.0.0.0</RemoteHost>
  <RemoteNetmask>255.255.255.255</RemoteNetmask>
</remote_ssh>
```

Figure 3 Remote Management Evidence

As depicted by Figure 4, each configuration file has a populated list of MAC addresses specific to either wireless or wired Ethernet devices. In this particular instance a series of fictitious pre-populated MAC address for wireless devices were placed into the allow list utilising the web management facility of the device. As demonstrated in Figure 4, these MAC addresses are clearly evident and could be extracted for future analysis.

```
<access_list>
  <mac_addr>00-0E-35-00-0E-35</mac_addr>
  <mac_addr>00-15-AF-00-15-AF</mac_addr>
  <mac_addr>00-1F-3B-00-1F-3B </mac_addr>
  <mac_addr>00-22-43-00-22-43</mac_addr>
  <mac_addr>00-23-31-00-23-31</mac_addr>
</access_list>
```

Figure 4 MAC Address Allow List Evidence

The current state of the research is limited to the interpretation of evidence in relation to directly examining the evidence.xml file. As it stands each time the evidence file is extracted and converted from an ADSL router, there are approximately 2,600 lines of data for the forensic examiner to analyse. While the data is of a significant size, the examiner does have the opportunity to directly search through, and manipulate the configuration file to identify evidence of interest, pertaining to the legal case.

Utilising the acquisition and analysis approaches discussed in this paper, ADSL routers are continually purchased from second hand sites such as eBay. Many end-users happily sell their networking devices. However, few to date, have removed their *personal identity* from these ADSL routers. From the series of second hand devices purchased – none of the devices had the Internet Service Provider's account credentials removed. As a result it is simple to identify the ISP and the credentials the seller was utilising to access their broadband service. As many ISPs tend to link the broadband credentials directly to an email or administration account, is it evident that the information could be utilised for malicious purposes.

CONCLUSION

The value of ADSL router forensics will be increasingly important as the number of threats targeting these simplistic devices escalates. The method described within this paper is fundamentally important for investigating the effects of malware on ADSL routers. Each time the "Psyb0t" or "Chuck Norris" malware infects a vulnerable device, the device initiates a lock-out state. A traditional inspection of the device would be defunct in that the ports required to access the device through Telnet, SSH or via the web management interface are blocked as part of the malwares characteristics. Fortunately the malware has no method by which to block the serial console access. As a result an investigator may utilise the approach discussed in this paper whilst still acquiring evidence pertaining to the compromised state of the device which is still operating the specific botnet.

The future of this research will attempt to examine the feasibility of utilising non-solder based contact points on the board of the ADSL router. As with the majority of ADSL routers, there are no actual headers located on any of the boards. As a result each device is prepared through soldering on of a header specific to the JTAG or serial connection to be utilised. This of course would not be a practical method by which to make connectivity in a real life situation and as a result an alternative approach must be investigated to identify suitable approaches to making contact with the appropriate access interfaces.

REFERENCES

ABS. (2009). Internet Activity, Australia, Dec 2009 Retrieved May 9, 2010, from http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/

ACPO. (2003). Good Practice Guide for Computer based Electronic Evidence. Retrieved April 4, 2007, from http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf

AR7 Firmware. (2009). AR7 Based Router Firmware. Retrieved March 13, 2009, from http://ar7.wikispaces.com/Firmware

Baume, T. (2009). Netcomm NB5 Botnet – PSYB0T 2.5L. Retrieved September 10, 2009, from http://users.adam.com.au/bogaurd/PSYB0T.pdf

Brown, C. L. T. (2006). *Computer Evidence Collection and Preservation*. Hingham, MA: Charles River Media.

Hunt, S. R. (2009). New worm can infect home modem/routers. Retrieved October 11, 2009, from http://apcmag.com/new-worm-can-infect-home-modemrouters.htm

Kirk, J. (2010). D-Link issues fixes for router vulnerabilities Retrieved March 22, 2010, from http://www.networkworld.com/news/2010/011510-d-link-issues-fixes-for-router.html

McMillan, R. (2010). Chuck Norris Botnet Karate-chops Routers Hard. Retrieved May 1, 2010, from http://www.pcworld.com/businesscenter/article/189868/chuck_norris_botnet_karatechops_routers_hard.html

OpenWRT. (2010). OpenWrtDocs/Hardware. Retrieved June 12, 2009, from http://oldwiki.openwrt.org/OpenWrtDocs(2f)Hardware.html

Router Marshal. (2010). Router Marshal Digital Forensic Software. Retrieved March 10, 2010, from http://routermarshal.atc-nycorp.com/index.html

Sajdak, M. (2009). *Remoterootshellon a SOHO classrouter.* Paper presented at the Confidence 2009, Krakow, Poland.

SourceSec. (2010). Which Routers Are Vulnerable to the D-Link HNAP Exploit? Retrieved May 20, 2010, from www.sourcesec.com

Szewczyk, P. (2009a). *ADSL Router Forensics Part 2: Acquiring Evidence.* Paper presented at the 7th Australian Digital Forensics Conference, Kings Hotel, Perth, Western Australia.

Szewczyk, P. (2009b). ADSL Router Forensics: Methods of Acquisition. *Journal of Network Forensics, 1*(1), 16-29.

Szewczyk, P., & Valli, C. (2009). Insecurity by Obscurity: A Review of SoHo Router Literature from a Network Security Perspective. *Journal of Digital Forensics, Security and Law, 4*(3), 5-16.

Social Networking: A Boon to Criminals

Tejashree D. Datar and Richard Mislan
Computer and Information Technology Department
Purdue University
West Lafayette IN
tdatar@purdue.edu
rick@purdue.edu

Abstract
With the world getting more and more digitized, social networking has also found a place in the cyber world. These social networking sites (SNSs) which enable people to socialize, and build and maintain relationships are attracting attention of all kinds of people such as teens, adults, sports persons, and even businesses. But these SNSs are also getting unwanted attention from people like sexual predators, spammers, and people involved in criminal and illegal activities. This paper talks about SNSs and how these sites are exploited for criminal or illegal activity. The SNSs are discussed in detail with respect to user profiles, user networks, and privacy and security with respect to these user accounts. The paper also talks about the way available data on these SNSs can be exploited. The paper concludes with a few real life recent criminal cases associated with these SNSs.

Keywords
social networking, social networking sites, Facebook, MySpace, online predators, phishing, social networking crime, social networking models

INTRODUCTION

With the advent of the Internet, it is now very easy to be connected to a number of people, groups, and communities which was not this easily possible before the Internet was widely available. The Internet gave rise to *online* social networking which is mostly done via the use of social networking sites (SNSs) such as Facebook, Twitter, MySpace, Friendster to name a few among the many available SNSs. Today, online social networking has become such a huge phenomenon, that Twitter was declared the most popular English word of 2009 (Parr, 2009). Facebook, one of the social networking sites, ranks third in the overall web traffic in the United States with over 104.2 million users per month (Quantcast, 2009a). MySpace, another social networking site ranks tenth in the overall United States web based traffic with over 55.8 million users per month (Quantcast, 2009b). Online Social Networking has become so much part of our daily lives that it is not uncommon to keep all our contacts posted of what we are doing, if not every minute, but everyday of our life. Social Networking has become a powerful tool for businesses and other things like even the 2008 Presidential Election.

The basic purpose of these SNSs is online interaction and communication and maintaining relationships. SNSs have various models, but the most common model is to present a person's profile and to visualise the person's network of contacts to other people (Gross & Acquisti, 2005). These SNSs allow people to put all kinds of personal information on their

website. When people join these social networking sites, they have to create their personal profile. This profile contains information such as name, which could be real or pseudo, date of birth, address, hometown, gender, ethnicity, religion, spouse's information, workplace details, school details, and the person's personal interest. This profile could also include photographs, videos, and personal messages. Other members can connect by sending friend requests or messages. When a person is added to the contact list or the friend list, this person gets the privilege to access the friend's profile and all the personal information put on this profile. These SNSs also have the privacy option wherein the profile user can hide all of the available personal information from other users except their friends in the friend list, that is, users who are directly connected to the profile owner. Even with all this available privacy, users are least bothered about their profile privacy and are happy to share all the personal information with the online world.

With such personal information as name, address, date of birth, gender, information on children, personal messages like updates, and photos made easily available by the users themselves, it is easy for criminals to gain access to this information. But as per these SNSs models, these criminals also get access to the directly connected contacts of the user. These criminals are commonly referred to as "Online Predators". This paper focuses on three popular social networking sites in the United States, namely, Facebook, MySpace, and Twitter. The paper will describe social networking and its history, and then will describe the above-mentioned three sites in detail concerning the user profile, content, and privacy. It will then describe the possible use of these sites by online predators to conduct their criminal activities.

SOCIAL NETWORKING: EVOLUTION

Until the 1990s, Internet was not so widely and commercially available to the common public. As Internet started becoming more available and more popular, people started viewing it as a useful and commercial application. This was the evolution of online social networking. But does it mean that people did not socially connect to each other before the Internet boom? Human being, in itself is called a social animal. Social networks have been studied and analysed for a long time now. This analysis of social networks is useful in studies of kinship structure, social mobility, science citations, contacts between members of deviant groups, corporate power, international trade exploitation, class structure, and many other areas (Scott, 1998). Internet was a revolution; similar to how telephone was a revolution. As social networking is nothing but maintaining relationships and building new relations, before the advent of the Internet, people used simple methods like snail mail, telegrams, telephones and even actually physically meeting each other to maintain and build new contacts.

In the 1980s and 1990s, a form of social networking called the Bulletin Board System or simply BBS was popular. Here people could send text messages and the BBS ran over the telephone lines (Gigaom, 2008). The first site that could be called as a social networking site came into being in 1997. This was the start of online social networking with SixDegrees.com coming into existence. Users were able to create profiles and list friends using SixDegrees. By 1998, users could also search for friends on SixDegrees. SixDegrees promoted itself as a tool where people could connect with each other and send messages

to each other. But SixDegrees failed as a business and in 2000 was finally closed (Boyd & Ellison, 2007). In 2002, social networking sites finally started blossoming with the introduction of Friendster. MySpace was introduced in 2003, while Facebook was open to the general public in 2006. Twitter was also launched in 2006 (Nickson, 2009). Thus started a new age of social networking that we have now come to know.

USER PROFILE CONTENT OF THE SOCIAL NETWORKING SITE

As stated earlier, this paper concentrates on the three most popular social networking sites in the US, namely, Facebook, MySpace, and Twitter. An account was specifically created for the purpose of this paper on each of these sites. While Facebook and MySpace have more fields as compared to Twitter, all these sites ask for information like name, birth date, photograph, hometown to just name a few. Compared to Facebook and MySpace, Twitter has more concentration on "chat" for social networking. Facebook and MySpace are more oriented towards maintaining and building new relationships. The amount of personal information that could be put up while creating a user profile on Facebook and MySpace is astounding. Apart from the fields mentioned earlier, a user could put in information like gender, sexual orientation, relationship status, movie or music taste, biological data to name a few. Appendix 1 lists and compares all the available fields related to a user profile on all the three sites.

With all this data relating to personal information available on the Internet, privacy is now a huge concern. Most of the user profile fields on these sites have an option of visibility. This means that the user can decide if the specific content should be available to everyone on the network (here network means the entire SNS network) or just the user's personal network of friends. Even with all this form of privacy available, users tend to keep their profiles open to everyone. This has created a huge security concern as crimes related to these SNSs started rising. These crimes could be anything from cyberstalking, social phishing to sexual assault. These sites are even referred to as "Predators Playground" (Schrobsdorff, 2007).

OPERATION OF THE SITES AS A SOCIAL NETWORK

Social networking works in the same way as computer networks. One user is directly connected to a number of users namely contacts or friends and these friends are in turn connected to other contacts. This forms a kind of web or mesh where users act as nodes and every node has multiple branches, which are the user's contacts.

Since every user on these SNSs is unique, the amount of information put out by each user is different. The way these users behave online is hard to define, but this behavior generates out of trust. Fukuyama, and Lewis and Weigert in their respected papers (as cited in Dwyer, Hiltz, & Passerini, 2007) discuss that trust is a critical determinant in personal or face to face relationships. Similarly, Coppola, Hiltz, and Rotter, Jarvenpaa and Leidner, Meyerson, and Piccoli and Ives in their respective papers (as cited in Dwyer, Hiltz, & Passerini, 2007) discuss that trust is also important for successful online interactions. Metzger in her paper write that(as cited in Dwyer, Hiltz, & Passerini, 2007) trust is a precondition for disclosure in interpersonal exchange situations, because of the reduced perceived risks which are involved while revealing private information (Dwyer et al. 2007).

From the above arguments it can be said that relationships on these sites will not be built without trust. To build up a relationship, the user generally adds other users as their friends only if they know each other, even though it was a very brief interaction. The way these SNSs' networks work, once a person is being added into the friend list, this person can access all the information of the user including the users other contacts. This way, it will not be very difficult for an online predator to gain trust of an individual by employing the briefest of interactions and once added to the friend/contact list, exploit this individual's personal data and also maybe search for other potential victims through the now open medium of "Friend List". Crime via social networking is increasing rapidly and criminals are now viewing these SNSs as a tool for committing crimes. If the user account is not open to everyone, the key point of the user information being available for exploitation lies in gaining trust and access to the user profile via Friend/Contact List.

FINDING THE USER INFORMATION FOR EXPLOITATION

There are many ways of finding the user information. The user itself can be found by doing a simple search in search engines like Google or Bing. There are certain privacy features available for users of the SNSs that allow the users to not be found via the search engines. This is called profile searchability. Online predators do not search explicitly for users this way. They prefer to contact potential targets as a user of the SNS. Wolak, Finkelhor, and Mitchell in their paper write that online predators prefer to meet and seduce their victims online. They also say that majority of the victims are aware that they are conversing with an adult (Wolak et al. 2008). In a social phishing study conducted by Jagatic, Johnson, Jakobsson, and Menczer, they found out that students readily give university information to a non-university party. They say that a phisher can mine information about relationships via social networking sites. For this study, Jagatic, Johnson, Jakobsson, and Menczer used freely available user profile data from SNSs for the phishing attack. This data appeared to originate from a friend on the network. They found that the targets were much more likely to disclose personal information to friends than strangers (Jagatic et al. 2005).

So how much information is easily available? Acquisti and Gross in their study found that Facebook users have more trust in the Facebook privacy settings. These users are not much concerned about the information in itself as they think that they can control the information and the privacy controls as to who can view the data. They found out that users are also mildly concerned about who can access their personal data. Another interesting thing Acquisti and Gross found in their study was that users of Facebook, trusted the system and its members more than compared to MySpace (Acquisti & Gross, 2006).

With the users having this attitude towards privacy and trust, with respect to both the SNS and the users in the contact list, it is very easy for online predators to gain access to personal information of the users or for phishers to use phishing methods to collect personal data.

PRIVACY AND SECURITY

SNSs have a lot of privacy features. Users have control over who can search their profile called the profile searchability or who can view their profile called profile visibility. A user's direct network of contacts has exclusive privilege of viewing all of the users content such as

the message posts by the user and by user's other contacts on the user's profile. These direct contacts have access to all of the user's photos, videos, list of the communities, friend/contact lists. These users however, cannot see the messages/mail communication between the user and the user's other contacts.

The privacy issue arises when some user content is seen or accessed by unintended people. This occurs when "friends of friends" or secondary contacts can view the user's content like photos, and videos. A user can be connected to thousands of secondary users or the friends of friends and this potentially increases the risk of personal information being available to users who are not even in the contact/friend list of the user. Acquisti and Gross in their paper write that an online social network lists hundreds of direct contacts/friends and include hundreds and thousands of additional contacts which are just three degrees of seperation from the subject (Gross & Acquisti, 2005).

With these statistics it is very easy to cross reference a particular user via the open friends/contacts channel. If an online predator gained the trust of a teen and gets added to that teen's contact/friend list, this opens a big window for this online predator to search for potential victims via this teen's friend/contact list. This predator will also have access to the teens photos and from there access to any open profiles as well as photos, videos, and personal information of the teen's other contacts, which essentially become the predator's secondary contacts.
Phishers work in different way. They gain unauthorised access into a users account and start sending spam to the user's direct contacts. These messages could be anything like the Nigerian Scam or appear to come from the user and ask to fill information on a third party network or could be even a virus which infects the machine if the link to it is clicked. SNSs are opening new doors for phishers and scammers. One can become a member of these SNSs very easily. Also, most of these sites lack basic security measures like SSL logins. This makes it easy for hackers to access the user data without the site's direct collaboration (Gross & Acquisti, 2005).

EXAMINING THE SNSS FOR INVESTIGATIVE PURPOSES

With the vast amount of data that is readily available on the SNSs, similar to criminals, investigators can also use this data for investigative purposes. The ways of finding user information for investigative purposes is very much similar to what the criminals use. For investigative purposes, a specific user will be targeted to gather information from. Shoemaker in her paper (as cited in Lampe, Ellison & Steinfield, 2006) write about a function called 'surveillance' which allows an individual to track the actions, beliefs and interests of the larger group, to which they belong to (Lampe et al. 2006). Lampe et al. classified this type of surveillance by the goals of users as 'social searching' or 'social browsing'. Social searching is where the site is specifically used to investigate specific people. Social browsing helps to find people or groups with whom the individual wants to connect offline (Lampe et al. 2006). Social searching is the type of surveillance that investigators use as they target specific individuals to gather information.

Just like normal people, criminals tend to keep their profiles open to public. Some criminals go as far as to put status updates about the crimes they have commited. Investigators can

use these SNSs to verify an alibi, or to even just check up the profile of the particular individual. SNSs are used by the investigators as form of resource. They use these sites more reactively rather than proactively (Klein, 2008). Apart from investigators, people like insurance adjustors, insurance attorneys, prosecutors, defense attorneys are also taking help of the SNSs to check out their clients or their witnesses (McKinney, 2010).

SOME CYBER CRIME CASES INVOLVING THE SNSS

With the increase in popularity of the SNSs among general public, there is also an increase of popularity of these SNSs among criminals. These SNSs have actually opened a lot of doors for the crime world and the way crimes are committed. Now-a-days, reports of lots of criminal activities involving the SNSs can be heard. Facebook and MySpace are especially popular in this area. A few cases relating to SNS are listed below.

Recently in the news was John Forehand, who was arrested for allegedly asking his teen daughter for sex over Facebook. John Forehand started communicating with his teen daughter over Facebook. He then told her that he was having inappropriate dreams about her and then proposed sex with her via posting graphic details of the activity on her Facebook account (The Huffington Post, 2009). In this particular case, the teen daughter added John Forehand to her contacts/friend list, as she must have trusted him since he was her father. If we can call John Forehand a predator, then the daughter's other teen contacts could be considered potential victims. John Forehand had easy entry in any open accounts via his daughter's contact/friend list.

In another case, a man named Robert A. Wise was arrested on charges of online solicitation of a minor. Wise was sending explicitly sexual messages to a teenage girl via MySpace. After being contacted the police posed as the 14 year old girl on MySpace and via the MySpace chat arranged a meeting with him. When Wise came to meet the girl at a prearranged spot, he was arrested. The cops also found online evidence against Wise to charge him with the sexual assault of another 14-year-old girl he had allegedly met on MySpace (Schrobsdorff, 2007). In yet another case a Houston man was arrested with sexual assault of a child. This 15 year old teen had been communicating with this man on MySpace and had actually snuck out of the house to meet him in person (Schrobsdorff, 2007).

In yet another incident, Emily Mayhan, a 20 year old Facebook user found that her Facebook account had been hijacked and the password to the account changed due to which she could not access the account. After that several of the contacts in her friend list started getting messages stating that she was stranded in London without cash and in urgent need of cash. Facebook closed her account on account of suspicious activity after a few days but no action was taken on the incident. According to the Federal Bureau of Investigation (FBI), this is a case of online hoax or phishing, which takes place for identity theft or for financial information (Davis, 2009).

In yet another phishing scam on Facebook, Bryan Rutberg's Facebook account had been hacked into and messages appearing from him were being posted saying that he is in urgent need of help. Many of his contacts also received emails saying he had been robbed at gunpoint while travelling in the United Kingdom and he was in need of money. Rutberg

was locked out of his own account and the scammer had even removed his wife from his contact list. The account was de-activated after about 24 hours (Sullivan, 2009).

And lastly but not the least, "Spam King" Sanford Wallace was sued by Facebook for accessing users' accounts without their permission and then sending phony messages and posts. Facebook claimed that Wallace used phishing sites or other similar means to fraudulently gain access to Facebook accounts of the users. After that, he used these accounts to distribute phishing spam throughout the network (cnet, 2009). Wallace was also charged and fined for the MySpace case in 2008 where he sent junk messages to the MySpace users (USA Today, 2009).

CONCLUSION

While social networking sites are a good way of maintaining relationships and building new relationships, a user should be always aware of the existing dangers of using these sites. With the high amount of personal data put on these sites, there is always a risk of this data being exploited. Even with the use of privacy settings, the data is easily accessed through an open account or even through a closed account. Howsoever innocent the personal data is, online predators are always watching and users are targeted via phishing.

REFERENCES

(2009a), 'Profile of Facebook.com', Retrieved from Quantcast: http://www.quantcast.com/facebook.com, November.

(2009b), 'Profile of MySpace.com', Retrieved from Quantcast: http://www.quantcast.com/myspace.com, November.

(2009), *Social Networks, from the 80s to 00s*. Retrieved from Gigaom: http://gigaom.com/2008/01/20/social-networks-from-the-80s-to-the-00s/, November.

(2009), 'John Forehand: Man 'Asked Teen Daughter For Sex On Facebook' (PHOTOS, VIDEO)', Retrieved from The Huffington Post: http://www.huffingtonpost.com/2009/10/12/john-forehand-man-asked-d_n_317148.html, October 12.

(2009), 'Web marketer ordered to pay Facebook $711M damages', Retrieved from USA Today: http://www.usatoday.com/tech/hotsites/2009-10-30-spammer-facebook-damages_N.htm, October 30.

Acquisti, A. & Gross, R. (2006). *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, Retrieved October 2009 from http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf*

Boyd D. M. & Ellison N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication , 13* (1), Article 11, Retrieved from http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

Davis, M. T. (2009), 'Online Predators turn to Facebook', Retrieved from Missourian: http://www.columbiamissourian.com/stories/2009/10/26/social-network-identity-theft-rise/, October 26.

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace*. *Thirteenth Americas Conference on Information Systems*. Keystone, Colorado, August 10-12.

Gross, R., Acquisti, A. (2005, November 7). Information Revelation and Privacy in Online Social Networks (The Facebook Case), Retrieved from http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf

Jagatic T., Johnson N., Jakobsson M., and Menczer F. (2005). Social Phishing. *Communications of the ACM* , Forthcoming (2009).

Klein J. (2008), 'Police: Criminal evidence can be drawn from Facebook, MySpace', Retrieved from Gateway: http://media.www.unogateway.com/media/storage/paper968/news/2008/03/25/NationalNews/Police.Criminal.Evidence.Can.Be.Drawn.From.Facebook.Myspace-3280666.shtml, March 25.

Lampe C., Ellison N., and Steinfield C. (2006). A face(book) in the crowd: social searching vs. social browsing. In *CSCW '06: Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work*, pages 167-170, New York, NY, USA. ACM.

McKinney R. (2010), How Facebook and Social Media Impacts your Case [Video File]. Video Posted to: http://www.nashvillecriminallawreport.com/2010/04/articles/evidence-and-procedure/how-facebook-and-other-social-media-impacts-your-case/

Mills, Elinor (2009), ''Spam king' could face criminal charges in Facebook case', Retrieved from cnet: http://news.cnet.com/8301-1009_3-10264069-83.html, June 12.

Nickson, C. (2009), 'The History of Social Networking', Retrieved from Digital Trends: http://www.digitaltrends.com/features/the-history-of-social-networking/, Janurary 21.

Parr, B. (2009), 'Twitter Declared Most Popular English Word of 2009', Retrieved from Mashable The Social Media Guide: http://mashable.com/2009/11/29/twitter-most-popular-word/, November 29.

Schrobsdorff, S. (2007). 'Predators Playground?', Retrieved from Newsweek: http://www.kidsafecyberspace.com/wp-content/uploads/2009/07/Predators-Playground.htm, October 15.

Scott, J. (1998). Social Network Analysis. *Sociology , 22* (1), 109-127.

Sullivan, B. (2009), ‘Facebook ID theft targets ‘friends’’, Retrieved from http://redtape.msnbc.com/2009/01/post-1.html, November.

Wolak J., Finkelhor D., Mitchell K. J., Ybarra M. L. (2008). Online "Predators" and their Victims. *American Psychologist , 63* (2), 111-128.

1. APPENDIX

1.1 User Profile Fields for Facebook, MySpace, and Twitter

Facebook	MySpace	Twitter
Name/alias	Name/alias	Name/alias
Photograph	Photograph	Photograph
Networks		Lists
Sex	Sex	
Birthday	Birthday	
Sexual orientation	Sexual orientation	
Hometown	Hometown	Location
Relationship status	Relationship status	
Friends list	Friends List	Followers/Following/Lists
Political views		
Religious views	Religious views	
Activities		
Interests		
Musical taste	Musical taste	
Television taste	Television taste	
Movie taste	Movie taste	
Books taste	Books taste	
Quotations		
Email address(es)		Email address
Telephone number(s)		
Instant messenger ID(s)		
Educational history	Educational history	
Employment history	Employment history	
Group affiliations	Networking Categories	
Photo albums	Photo albums	
	Blog entries	Link to online Bio
	Personal 'about me' entry	
	Personal heroes	
	'Who I'd like to meet'	
	Zodiac sign	

	Parental status	
Online status	Online status	
Chat 'wall', including time of post	Chat 'comments', including date and time of post	Chat 'tweets', including date and time of post
	Income	
	Country	
	Postal Code	
	State	
Videos	Videos	
	Intentions (dating, relationships, friendship, networking)	
	Height	
	Body Type	
	Drinker	
	Smoker	
	Ethnicity	
		Time Zone

1.2 Some Recommended Safety Guidelines for Users of SNSs

- Always be aware that any content once put on the Internet always stays there even though it appears to be deleted.
- Always be aware of the content put out on the SNSs.
- Always use the available privacy features on the SNS. Do not leave the user profile open to be accessed by everyone.
- Do not accept friend/contact requests from unknown people.
- Think twice before putting any information on the SNSs.
- Avoid putting photos that might attract unwanted attention from any online predators.
- Avoid putting detailed information of oneself as well as family members like spouses, children, and parents.
- Be aware of any phishing content that might appear to be posted by any of the friends.
- Always be aware of the risks of social networking and different uses of SNSs.

Social Networking Websites as a Tool for Investigators

Bill Harshbarger
Purdue University
harshbwg@purdue.edu

Abstract
Online social networking websites' popularity have grown to the point that hundreds of millions of users have joined in order to make connections to others. Through these sites' information sharing nature, investigators can discover real world relationships and relevant personal information or activities. The purpose of this paper is to present a literature review regarding the nature of online relationships, investigative uses of social networking websites, the types of information available, and some usage examples. It was found that the sites can be a valuable resource for intelligence gathering, and that additional investigation into tools or methods to facilitate information gathering is warranted.

INTRODUCTION

As the growth of Internet availability and the subsequent opportunities and methods for communication have increased, people have started using online social networking websites as a supplement for face to face socialising. The use of these sites to build online representations of real-world acquaintance networks (Lampe, Ellison, & Steinfield 2006), or supplementing existing interpersonal relationships has driven the explosive growth of social networking websites in the past decade. As increasing numbers of people interact on these sites, more and more information about them is requested and collected, often with privacy being an afterthought. Personally identifiable information such as digital photographs, relationship status, friend lists, chats, marital status, birth date, political and religious leanings, as well as tastes in the arts and group affiliations can be revealed (Krishnamurthy & Wills, 2009), (Acquisti & Gross, 2006). Additional information can be directly accessed or inferred by viewing digital photos, videos, or chat postings which may document actions, statements, or locations. Additionally, observation of these sites shows that many activities, such as posting comments or photographs are time stamped. Often through default privacy settings, much of this wealth of information is readily accessible, possibly even by those not directly a member of an individual's social network (Stutzman, 2006).

When one thinks of an online investigation, often the image of an investigator observing or covertly interacting with an online user comes to mind. Many times this investigative target is an individual seeking to build an online relationship or disclose information with a stranger in a semi-anonymous environment, something McKenna, Green, and Gleason (2009) described as "strangers on a train". Instead of seeking or interacting with strangers, what happens if the interactions are explicitly among individuals who already know each other and wish not only to simply connect but do so in an environment that collects information? This building of an online acquaintance directory of sorts, and the ability to

browse and connect with people is the basis for social networking websites usefulness, from a participant's perspective. In nearly the same manner as users browse for people on these sites, so too can investigators navigate the links between people in order to perform reconnaissance (Read, 2006).

Research by Bargh, McKenna and Fitzsimons (2002) has shown that in general, online relationships are perhaps more rapidly and strongly formed than normal social interactions due to facilitating aspects such as implied anonymity or a sense of enhanced self-expression. While social networking sites do promote online relationships, and searching for contact with strangers can occur, the main use is more novel. This additional use is to build or supplement real-world links, however tenuous, to others already known. Instead of seeking relationships with strangers, Lampe, Ellison, & Steinfield (2006) described the term "social searching" or "social browsing" to describe the acts of browsing the social networking website mappings of these real-world links in order to find acquaintances. These browsing functions involve the viewing of social network profiles for the purpose of following people's life activities, or to gather more information or intelligence about friends and acquaintances.

All of this information about a participant's identity and life, which they choose to share, and which is neatly and often publicly compiled by these sites, can be used by law enforcement or the legal or intelligence community. These investigators can browse and search for links between people in a similar manner to the way social searching is done by the users of these websites. Additionally, users and investigators can similarly use the sites to gather information on individuals, determine social connections and mutual friendships, and follow activities. For this paper, online social networking will be described in general terms, but for specific examples three popular US social networking sites will be discussed: Facebook, MySpace, and Twitter. Additionally, the possible advantages of using social networking sites to supplement investigative sources, and descriptions of the types of information available on each will be presented. This mapping of potential information is a first step in providing investigators an index of potentially available information. This is useful, as the more personally identifiable information that can be gathered, the more likely a person can be matched to this information (Gross & Acquisti 2005).

SOCIAL NETWORKING BACKGROUND

The concept of a social network as a way to define and study interpersonal relationships is not a new one. Sociologists have long used social networks and social network analysis as a way to study interactions and relationships among groups of people, and it has been a well-researched field since at least the 1930s (Wasserman & Faust, 1994). Specifically, law enforcement has long realised that the use of social network analysis techniques could benefit investigations by mapping ties between individuals in order to determine relationships (Davis, 1981). Note that sociology defines a social network somewhat differently and in a more formal manner, in order to perform statistical analysis, express relations mathematically, or generate theories on interactions (Wasserman & Faust, 1994). In the context of this paper, social networking is defined as the interactions and web of relationships that are facilitated by websites created specifically for information sharing

among a community of members who are linked by characteristics such as location, affiliations, friendships, families, et cetera.

How did people keep track of friends and acquaintances before computers, the Internet, and specifically social networking websites? The answer is well known, as pre-Internet people kept track of friends and acquaintances through face to face interactions and by using available media technologies of the time, such as written word, telephones, and so on. In reality, social networking websites are performing a similar role as a communications medium. Combined with the specific qualities of online interactions, social networking websites can affect how relationships are formed and information is disclosed. Additionally, the increasingly public nature of disclosure further influences how the information can be accessed (Gross & Acquisti 2005).

Boyd and Ellison (2007) outline the history and growth of social networking sites, from the creation of the first dedicated online social networking website, sixdegrees.com, in 1997. Since that time, twenty-five individual sites have been created or re-launched, many even between 2003 through 2007 (Boyd & Ellison 2007). The growth of these sites can be demonstrated partially by comparing the membership of Facebook, which Gross and Acquisti (2005) estimated to be around 2.4 million in 2005, to a statement from Facebook's founder in September, 2009 that his site now claims three hundred million members. This is a massive number, but definitely not the end of growth for the site, as Facebook's stated goal is to "connect everyone" (Zuckerberg, 2009).

GENERAL NATURE OF ONLINE SOCIAL INTERACTION

The nature of online social interactions also affects the uses of online social networking and also influences tendencies to share information or form relationships. There is no set of rules for how people interact online, however some recurring characteristics have been identified.

Anonymous Environments

One factor is that anonymous, or perceived anonymous environments, including social networking websites can promote the expression of a true self which can influence a person to express ideas or opinions that may not otherwise be accepted in normal society (Acquisti & Gross, 2006), (Bargh, McKenna, & Fitzsimons, 2002), (McKenna, Green & Gleason, 2009). For an investigator, this implies that users of social networking websites may be more prone to express thoughts or opinions that they may normally withhold in real world interpersonal interactions.

Formation of Relationships

Another influencing factor of online social interactions is that the formations of relationships can be facilitated. Some people are simply more comfortable being themselves online than in face-to-face situations. Bargh, McKenna, & Fitzsimons (2002) found through experimentation that online relationships, and specifically the openness of sharing personal information, can depend first on if a participant 'likes' the other person or not. While this initial barrier exists, once openness occurs, online relationships can be built much faster than real world ones. While this poses an initial hurdle to an investigator, it is

similar to building trust with a subject of an investigation or interview. The benefit of being able to quickly connect with people online also has obvious implications for saving time.

Openness and fast relationship building can be an advantage to an investigator and apply in general to online interaction, but the fact still remains that most users of social networking websites will only connect with people they already know, at least in some manner (Lampe, Ellison, & Steinfield, 2006)(Adamic & Adar, 2005). It may only take a brief meeting in a class, or at a conference, or on the street, but for most users of these sites, acceptance into their network may require at least minimal "real-world" interaction.

SOCIAL NETWORKING SITE PROFILE CONTENT

Currently in the United States the three social networking sites given the most attention are Facebook, MySpace, and Twitter. As stated previously, many people use these sites, especially Facebook and MySpace, to supplement, build, or extend existing relationships with family, friends, coworkers and acquaintances (DiMicco & Millen, 2007), (Lampe, Ellison, & Steinfield, 2007). While Twitter contains similar profile elements, it has many less profile fields compared to Facebook or MySpace at the time of this writing, as exhibited in Appendix A.

As asserted previously, there is a wealth of personal information on these sites, but what exactly is available? For each of the three sites, an account was created and the available fields to complete a profile were observed. Appendix A details the names of some of the fields available to be filled out in a user's profile. While sites use varying terminology, analogous entries are listed on the same row. Even though these fields represent the defaults available for a profile on the social networking website, this information, and much more can be disclosed through the openness of chat posting on a profile. In other words, there is no restriction as to what a user can enter into their profile, chat about, or post to other's profiles. One could say that this profile information is just the starting point of what is potentially available.

VIRTUALLY LOCATING THE SOCIAL NETWORK PARTICIPANT

Using Open Privacy Settings

If the user of a social networking site leaves their privacy settings open, then anyone can use that website's search feature to locate them, primarily based on name, known friends, or other profile information. Additionally, these open profiles are often indexed by Internet search engines, which allow all content of the profile to be searched. Essentially, to find any participant, the same techniques that people intuitively use when searching for their friends is used. There really isn't a high-tech methodology to locating someone, rather it is by using existing online search methods that people may be found.

Exploring Known Relationships

Another method to find individual profiles is to explore known relationships of the target, usually provided in some manner by the sites, and note common friends. To most investigators, it is common sense to cross reference people who are friends or acquaintances with an investigative target. However, there are some surprises to this method. As described by Adamic and Adar (2005), so-called "short paths" exist in the

degrees of separation among people, and these short paths are often facilitated by well connected individuals with many members in their personal networks. (Adamic & Adar 2005) demonstrated that with personal network memberships of three hundred, it would be possible to link any two people in the country in three intermediary relationships. This implies that it may be possible to discover connections to an investigative target that may not have otherwise been easily detectable. Finally, Adamic and Adar (2005), explain that by narrowing down similar traits, or in a social networking terms, profile elements, navigation of a broad social network to an individual can be accomplished. In a sense, this is the same concept as matching enough data points to find an exact person, assuming each person has at least one unique characteristic.

In a practical sense, searching for a person means starting with what information is known, mapping that to profile fields, and searching along those traits. For example, if the target of an investigation liked a certain movie or musical act, there is a chance that they would somehow be associated or linked to related content on the social networking site. The end result could then be to gain access to the target's profile , at least to a degree at which the target's personal information is viewable and less restricted by privacy controls (Gross & Acquisti, 2005). This can depend on many factors, but mainly group or network memberships and privacy settings.

CORRELATION OR INFERENCE OF INFORMATION

Some information may not be explicit in the profile, or the profile may not be accessible. However, useful information can still be obtained from these sites. For example, if a target is not a user of a social networking site they may, for example, attend a birthday party of a friend or relative who is a user of these sites. Often these events or activities are documented through video, photography, or depicted through text describing the event. This is important because even if a person doesn't participate on a social networking site, it seems plausible that at least some of their friends or family or classmates or coworkers do. It is then possible that participants may post this information which may have content including the non-participating individual, though the reliability of this method was not determined in this research. This hypothetical example is where the power of the popularity of social network sites may be able to play a huge role. In these instances the tendency to post online about people with whom there are real-world connections, even if the second party doesn't participate, benefits the investigator. Many people who do not use or object to using these sites may not realise that non-participation is not a guarantee that information about them is exempt from being disclosed. Additionally, given that the number of degrees or hops between people can be surprisingly small (Adamic & Adar, 2005), it may be possible to find content in unexpected places.

Other data may also be inferred. For example, a target could post to their profile that they attended a movie with two friends. This post will more than likely have a timestamp, and possibly a method of posting, such as from a mobile phone as described in Appendix A. With this information, it may be possible to infer the time and location, as well as the activities of the target. Even if one such post does not provide all of this information, observing several posts can lead to a pattern of activities. For example, if a target often posts on Mondays that they are going to a local bar to watch football, one could safely

assume that they could be found there on a subsequent Monday around a certain time. These hypothetical examples go to illustrate not just that the sites contain useful data, but that correlating the same data could possibly provide insights or information that wasn't explicitly divulged.

PRIVACY CONTROLS ON CONTENT

Each of the sites provides an outlet for a user to interact with their friends, acquaintances, or the public. At the same time these interactions are happening in an increasingly public sense. For instance, conversations that may have taken place over emails or SMS messages may now appear on users' profiles or chat space, which at a minimum are viewable by their first-degree circle of linked relationships, and potentially open to the world if privacy controls are lax or not applied. This can be equated to the information sharing properties of the sites and users' propensity to post information openly as described by Gross and Acquisti (2005).

Each of these sites is allowing unprecedented access to view relationships, opinions, actions, and anything else a person may be inclined to disclose, and as demonstrated previously may in fact be more apt to do so. By their design and nature these sites are set up for the sharing of information and therefore the privacy controls are weaker than one may expect (Acquisti & Gross, 2006). Additionally, Acquisti and Gross (2006) stated findings that privacy concerns over a particular site do not necessarily deter participation.

Although the privacy implications of these sites is beyond the scope of this paper, one interesting consequence of the openness of these sites is that data leakage through advertisements, website applications, and games could potentially provide a vector for access to profile information (Krishnamurthy & Wills, 2009). For example, Krishnamurthy and Wills (2009) found that advertising referrer headers contained user IDs and friend information, regardless of privacy control settings. These demonstrated "leaks" of information imply that it may be possible for a 3rd party to obtain much profile information simply by having a user view an advertisement. Combine this with the amount of targeted advertising on these sites and in some cases built in advertising tools, the potentials for access becomes apparent.

BENEFITS TO AN INVESTIGATOR

There are several ways in which using social networking sites can benefit an investigation or intelligence gathering. First and perhaps surprisingly, non-participants information may still exist on a participating friends' profile. Additionally, searches of these sites can reveal real-world relationships which can potentially be discovered much faster than traditional methods. Novel relationships can be discovered through short paths, and may provide contacts for questioning that may not have been found otherwise.

Although Acquisti and Gross (2006) argue that usefulness to those outside a network will predictably diminish as users learn about privacy controls, it is still trivial to become a participant, and the research by Krishnamurthy & Wills (2009) indicates that privacy controls may not play as large a factor as is perceived.

Another investigative benefit, implied in the research by Lampe, Ellison & Steinfield (2007) found that at Michigan State only 3% of Facebook users felt that law enforcement or school administration were actively viewing profiles. This could be compared to the feeling of anonymity, and may promote a more cavalier attitude in disclosing information on illicit acts.

Krishnamurthy and Wills (2009) also suggest that data remnants of social network browsing should specifically be targeted in the forensic investigation of a seized computer. This implies that the data in a profile is not just limited to the website, but is useful even beyond intelligence gathering and may play an additional evidentiary role.

Another interesting application could be to use so-called crowdsourcing techniques, which would allow an investigation to leverage the participants to find fugitives or possibly missing persons in much the same way that television and Amber Alerts are used to notify people of situations and encourage their assistance.

Gross and Acquisti (2005) stated that the use of face recognition in searches could potentially be used to find people in digital photographs on these sites.

As discussed previously, the nature of these sites means that people may be more prone to build relationships or divulge information more readily than in face to face interactions. Additionally, in real world covert investigations, targets may expect to be able to connect on a social networking site, and not doing so may be suspicious to the target of the investigation or detrimental in forming a relationship. This is inferred from the fact that participants in social networking prefer to connect with people they already know(Lampe, Ellison & Steinfield, 2006).

EXAMPLES OF USE OF ONLINE CONTENT IN INVESTIGATIONS

Although it seems that news reports of the use of social networking sites in criminal or administrative investigations occurs almost daily, a few examples of recent uses provides some context into how the sites can be used:

Recently, in Clark v. State of Indiana (2009) an Indiana appeals court found that evidence collected from a MySpace profile of Ian Clark and presented in his murder trial had been admissible. This evidence not only played a part in the conviction of Clark for murder, but the court also upheld the opinion on appeal that the evidence gathered was admitted properly (Clark v. State of Indiana, 2009). The evidence in question had been a posting on his MySpace profile which the prosecution had admitted as character evidence.

Read (2006) describes how a postgame riot at Penn State was documented photographically and posted to a Facebook profile specifically created for the viewing of these pictures. This open posting of pictures of rioters resulted in two arrests, and fifty administrative referrals. Read (*ibid*) also describes how MySpace was used in a missing persons case regarding a VCU student. Finally, Read (*ibid*) explained how several campus police departments used social networking sites to perform reconnaissance on where parties may occur.

Finally, in October 2009, Topping reported that fugitive Maxi Sopo was located in Mexico and apprehended based solely on information in his Facebook profile. This case is a prime example of the powerful nature of social networking and novel connections among people. The fugitive Sopo's profile was set to private. However as is often typical, his list of friends was not. The investigator noted that Sopo had a friend in his network who in turn had a connection to the US Justice Department. Although this connection was not represented online it proved to be useful. Through this connection, investigators were able to locate and apprehend Sopo in Mexico without actually having to make any direct connection with him or his profile.

WHAT NEXT

While the argument that there is useful information on these sites should be clear, what may not be are the next steps in forming methods or tools for investigators to use to access this information. The first steps would be to map what sites exist, the membership ranks, and study which combination of factors such as profile completeness, privacy settings, posting frequency, etc. are likely to provide results. A list of available profile fields was started by creating accounts on Facebook, MySpace and Twitter and observing what was available at the time of this writing. This is provided in Appendix A, however a list alone has limited practical value.

Additionally a prototype compilation of a quick checklist for investigators to refer to when performing investigations is provided. This sort of quick reference to techniques that may facilitate investigators' use of social networking sites to gather intelligence. It seems fitting to provide results of further study in such a checklist in order to provide investigators with sound recommendations.

Further research into the success rates of locating non participating individuals through participating individuals' postings may also prove beneficial. If this technique proves to be feasible, it could mean that searching for intelligence on a non participating individual should become commonplace, and social network searching should be performed in all instances and not just when an investigative target has a profile.

RECOMMENDATIONS

Proposed are a few additional research topics that may facilitate the use of these sites by investigators. First, an easily accessed, published compilation of contact information, procedures, and policies regarding legal requests for each popular social networking would benefit investigators who may ultimately need to access information via these methods.

Next, an investigation into the usefulness of built-in tools such as querying interfaces or languages, advertising mechanisms, or other site-specific tools should be performed. This research could produce procedures, software, interfaces, or resources for investigators to more easily search or access profile information through novel means. Determining what sorts of social methods, such as crowdsourcing, that can leverage the user community itself as a resource to assist in finding individuals or information may possibly benefit investigations.

Finally, each of these areas of practical knowledge seem to be well suited for presentation on an online resource to the investigative community, and this online resource is ultimately one goal for providing investigators what they need to effectively use these sites.

CONCLUSION

In summary, social networks have become well-established online collection points for several types of personally identifiable information as well as mapping interpersonal relationships. As these relationships are typically indicative of real-life relationships, the browsing and searching of these sites in order to gather intelligence in investigations becomes apparent. Since the kinds of information posted by users of these sites is known and willfully provided by the users, new tools and methods of lawfully accessing this information should be researched.

APPENDIX A: PROFILE FIELDS FOR FACEBOOK, MYSPACE, AND TWITTER

Facebook	MySpace	Twitter
Name/alias	Name/alias	Name/alias
Photograph	Photograph	Photograph
Networks		Lists
Sex	Sex	
Birthday	Birthday	
Sexual orientation	Sexual orientation	
Hometown	Hometown	Location
Relationship status	Relationship status	
Friends list	Friends List	Followers/Following/Lists
Political views		
Religious views	Religious views	
activities		
Interests		
Musical taste	Musical taste	
Television taste	Television taste	
Movie taste	Movie taste	
Books taste	Books taste	
Quotations		
Email address(es)		Email address
Telephone number(s)		
Instant messenger ID(s)		
Educational history	Educational history	
Employment history	Employment history	
Group affiliations	Networking Categories	
Photo albums	Photo albums	
	Blog entries	Link to online Bio
	Personal 'about me' entry	
	Personal heroes	
	'Who I'd like to meet'	
	Zodiac sign	
	Parental status	
Online status	Online status	
Chat 'wall', including time of post	Chat 'comments', including date and time of post	Chat 'tweets', including date and time of post
	Income	
	Country	
	Postal Code	
	State	
Videos	Videos	
	Intentions (dating, relationships, friendship, networking)	
	Height	
	Body Type	
	Drinker	
	Smoker	
	Ethnicity	
		Time Zone
Posting method (mobile phone)	Posting method (mobile)	Posting method(software name)

REFERENCES

Acquisti, A., & Gross, R. (2006), 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. ' Springer Berlin / Heidelberg

Adamic, L., & Adar, E. (2005). "How to search a social network" Social Networks, Volume 27, (Issue 3): Pages 187-203

Bargh, J., McKenna, K., & Fitzsimons, G. (2002). "Can You See the Real Me? Activation and Expression of the "True Self" on the Internet." Journal of Social Issues, Vol. 58(1) Page 33.

Boyd, D., & Ellison, N. (2007). "Social Network Sites: Definition, History, and Scholarship." Journal of Computer-Mediated Communication. Vol 13(No. 1) Pages 210-230.

Clark v. State of Indiana. Kosciusko Circuit Court, No. 43C01-0705-FA-127(2009) Retrieved from http://www.in.gov/judiciary/opinions/pdf/10150901rts.pdf

Davis, R. (1981)." Social Network Analysis - An Aid in Conspiracy Investigations."[Abstract] FBI Law Enforcement Bulletin Volume:50 Issue:12 , Pages11-19.

DiMicco, J. M. & Millen, D. R. (2007). "Identity management: multiple presentations of self in facebook." 2007 international ACM Conference on Supporting Group Work, November 04 - 07, 2007. Sanibel Island, Florida, USA.

Gross, R., & Acquisti, A. (2005). "Information Revelation and Privacy in Online Social Networks." Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society November 07, 2005Alexandria, VA, USA

Krishnamurthy, B. & Wills, C. (2009). "On the Leakage of Personally Identifiable Information Via Online Social Networks." Proceedings of The Second ACM SIGCOMM Workshop on Online Social Networks, August 2009. Barcelona Spain.

Lampe, C., Ellison, N., & Steinfield, C. (2006). "A face(book) in the crowd: social Searching vs. social browsing." 2006 20th Anniversary Conference on Computer Supported Cooperative Work November 04 - 08, 2006. Banff, Alberta, Canada.

Lampe, C. A., Ellison, N., & Steinfield, C. (2007). "A familiar face(book): profile elements as signals in an online social network." SIGCHI Conference on Human Factors in Computing Systems. April 28 - May 03, 2007. San Jose, California, USA.

McKenna, K, Green, A., & Gleason, M. (2009)." Relationship Formation on the Internet: What's the Big Attraction?" Journal of Social Issues.Volume 58 (Issue 1) Pages 9-31.
Chronicle of Higher Education

Read, B. (2006). "Think Before You Share: Students' online socialising can have unintended consequences." Chronicle of Higher Education. January 20, 2006.

Stutzman, F. (2006). "An Evaluation of Identity-Sharing Behavior in Social Network Communities." International Digital and Media Arts Journal, Volume3. (Issue1).

Topping, A. (2009). "Fugitive caught after updating his status on Facebook", The Guardian (UK) October 14,2009.

Wasserman, S., & Faust, K. (1994). Social Network Analysis: Methods and Applications. Cambridge, Cambridge University Press.

Zuckerberg, M, (2009, September 15). '300 Million and On. http://blog.facebook.com/blog.php?post=136782277130 Accessed November 2009.

2011 secau Security Congress
Call for Papers

"Building a Resilient Future"

The 2011 secau Security Congress incorporates a continuum of new ideas and research ranging from digital to physical security and from highly technological solutions to human factors using scientific and socially embedded frameworks. The Congress aims to draw together competing and complementing areas of security as part of a holistic engagement with the wider security discourse.

This is the first call to submit full academic papers for the 2011 secau Security Congress. Submitted papers must be in English, should be typed in a single column, single-spaced format, and must adhere to the maximum word limit of 3500 words. All submitted papers will be double blind peer reviewed and high quality papers will be considered for publication in selected journals. The secau Congress will incorporate the following conferences from **Monday 5 December to Wednesday 7 December, 2011**

12th Australian Information Warfare Conference
9th Australian Digital Forensics Conference
9th Australian Information Security Management Conference
4th Australian Security & Intelligence Conference
2nd Australian Counter Terrorism Conference

Full papers for review should be submitted by the 30 September, 2011

2nd International Cyber Resilience conference
Call for Papers

Monday 25 July and Tuesday 26 July, 2011

The aim of the International Cyber Resilience Conference is to bring together practitioners, academics and Government agencies to discuss and explore issues relating to cyber resilience of information systems and critical infrastructures. The conference is meant to not only consider technical cyber security issues, but also the human factors that impact the risks associated with the secure management of critical infrastructures. In addition, how all factors in combination can impact the timely response and recovery of systems and critical infrastructures.

The conference is across four main themes:

- Incident Response and Recovery
- Human Factors
- Cyber Security
- Risk Management

Full papers for review should be submitted by the 29 April, 2011

For further information contact the Conference Coordinator Lisa McCormack on +618 6304 5176 or email secau@ecu.edu.au . For detailed information regarding paper submission please refer to the main conference website found at http://conferences.secau.org/

Notes for Contributors

The secau -Security Research Centre is constantly searching for good publishable material within the domain of network forensics. The centre promotes a broad continuum of security research and is always keen to consider conference papers, journal submissions or any other proposals that further the security research envelope. http://www.secau.org/

Journal papers will be accepted in two major categories:
Academic papers follow the accepted international standards. An international panel of recognised experts in this field will ensure the very highest standards are maintained by refereeing all papers. A double-blind peer review process is adopted to ensure fairness and quality. A limited number of contributions, of a less rigorous nature, are welcomed. These are items which are considered to indicate significant trends of special interest to subscribers. While these papers are still refereed, a more relaxed standard is applied, with the emphasis on interests and potential significance rather than academic rigor.

Standard Journal submissions should be 3000 – 6000 words in length, although there can be flexibility in some circumstances. Papers should not have been previously published. Amended and augmented conference papers will be considered as long as copyright is cleared. Copyright remains with the author(s) although the Journal of Network Forensics reserves the right to re-publish the paper for instance, in a collection of papers.

Receipt of papers will be acknowledged. The reviewed papers will normally be returned within eight weeks. Accepted papers should be amended and returned to the editor within four weeks. Please do not use auto-formatting or any other style. Please adhere to the style as specified by the editorial panel. A copy of the specific formatting requirements can be requested from the secau - Security Research Centre by emailing Lisa McCormack at secau@ecu.edu.au

Length of Papers
Papers (title, abstract, main text) must normally not be more than 6000 words in length. Papers may be rejected if they are longer than the word limit.

Author's Responsibilities & Copyright
Authors are to ensure the accuracy of their own papers. This journal does not accept any responsibility for statements made by authors in their written papers. Where relevant, authors are to ensure that the contents of their papers are cleared for publication, for example, by their employer, their client, the funding organisation and/or copyright owner of any material which is reproduced. Authors retain their copyright of the paper.

Publication
The referees reserve the right to refer papers back to authors for correction, or to edit papers before publication in the published proceedings.

File Types
Please send the following by the deadline:

1. Final paper to the specifications above in Word Format.
2. Author Declaration Form.
3. 150 Word Biographical Statement for each author.

Submissions should be made via electronic mail to Lisa McCormack at the secau - Security Research Centre secau@ecu.edu.au