3-12-2007

ADSL Router Forensics Part 1: An introduction to a new source of electronic evidence

Patryk Szewczyk
Edith Cowan University

DOI: 10.4225/75/57ad5b8e7ff31
5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2007.

ADSL Router Forensics Part 1: An introduction to a new source of electronic evidence

Patryk Szewczyk
School of Computer and Information Science
Edith Cowan University
p.szewczyk@ecu.edu.au

Abstract

Currently there appears to be a lack of research in the area of developing tools, testing methodologies, and creating standards for ADSL router forensics. The paper examines a wide range of literature and introduces the concept of ADSL router forensics as a new and potential field of research for digital forensics investigators. It begins by examining why there is a need for router forensics by detailing some of the more common threats which consumers may experience while online. An outline will be provided discussing the feasibility, limitations and potential risks of router forensics. The paper will then examine one possible avenue for undertaking router forensics and how this applies to the Linksys WRT54g and finally portrays where the research will continue to hereafter.

Keywords

ADSL router forensics, digital forensics, embedded systems, JTAG, Linksys wrt54g

INTRODUCTION

The demand for Asymmetric Digital Subscriber Line (ADSL) devices has increased considerably as consumers are now offered fast and inexpensive methods to connect to the Internet. The plug and play nature of ADSL routers permits consumers to bypass the tedious configuration process and hence connect to the Internet within minutes. History has shown that the number of published exploits and threats for a particular device or software is generally proportional to the number of individual's utilising that system. In this instance as broadband technology is becoming the predominant method for Internet connectivity the number of published exploits on the more common range of Small office Home office (SoHo) routers is also on a parallel rise. Hence, in order to combat and pursue criminals whom endeavour to maliciously destroy, alter and degrade a consumer's online experience, techniques and standards must be developed to ensure a thorough forensic investigation of the networking device. As there are numerous threats to ADSL routers the number of standards, techniques and frameworks which could be used to forensically investigate a router is non-existent. The paper hereafter will introduce and discuss the necessity for sound ADSL router forensic principles.

THREATS TO ADSL ROUTERS

ADSL routers control the traffic flow between the Internet and the internal hosts on a SoHo network. As broadband technology becomes faster and more reliable consumers may opt to use their ADSL router to share an Internet connection in a home or office, utilise a personal or business internal web server, enjoy the benefits of Voice over Internet Protocol (VoIP) and the convenience of file sharing. In some instances consumers are unaware of the potential security risks and recommended security approaches for ADSL routers (Szewczyk 2006). However, the threats presented hereafter show that a simple and effortless method may disrupt or terminate an entire network connection to the rest of the world (Chang 2002).

Denial of service attack

A Denial of Service (DoS) attack targets routers in a 'reflector' or 'direct' mode and may halt the connection between the router and the Internet Service Provider (ISP). Most recently ADSL routers are predominately becoming victim to 'reflector' based attacks. The attacker transmits numerous synchronisation requests to router 'A' with a preset static source IP address of the soon to be compromised, router 'B'. Router 'A' responds to these numerous requests and sends the numerous acknowledgement packets to router 'B'. Eventually two routers have had their resources consumed as the SYN and ACK packets are constantly transmitted. Alternatively 'direct' attacks also consume the router's resources by flooding it with numerous Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), or User Datagram Packets (UDP) sent directly from the attacker. In this instance, the source IP address is spoofed each time hence leaving half open connections on the targeted router. Due to the resource limitations of the router the device may halt and hence require a power-cycle reboot (Chang 2002).

Access control

Routers are pre-configured to prevent remote management from an IP address outside of the internal network. Research has shown (Stamm et al. 2006) that this security technique can be compromised when an unsuspecting individual accesses a webpage and permits a malicious Java Applet to load. Once the malware is loaded onto a workstation, it begins to ping the other hosts on the subnet in an attempt to discover the location of the gateway/router. After a number of attempts the malware should discover the gateway by detecting which IP address is hosting a web configuration management system. Specific images used in the web configuration management system are unique to each router and hence the make and model of the router may be detected by the type of images retrieved from the default gateway. Once the router type is known, the malware may manipulate configuration settings, alters DNS addresses, enables port forwarding and remote management to a specific IP address, and disables Network Address Translation (NAT) (Stamm et al. 2006).

Software robots

Network address translation (NAT) permits a number of internal workstations to access the Internet simultaneously using a router allocated, private IP address. Essentially NAT provides a level of protection to the internal hosts by not using a public IP address and is enabled by default on many router brands. However, once NAT is purposefully, maliciously or accidentally disabled, the internal hosts may become victim to the control of a BotMaster controlling a collection of BotNets. A BotNet is a collection of hosts under the control of a BotMaster who controls the infectors and infected hosts to carry out various malicious tasks (Rajab et al. 2006a; Rajab et al. 2006b; Ramachandran & Feamster 2006).

A BotNet is instantiated by a BotMaster whom initiates a transmission of a shell code from an already infected host to a newly targeted host. The newly targeted host may become infected through a malware binary download (e.g. through an email attachment). The malware begins to download through the trivial file transfer protocol (TFTP), which once complete, automatically initiates the configuration scripts, allowing the BotMaster to control the victimised workstation. The infected host may then send mass amounts of spam email, install and collect data from key loggers, and launch distributed denial of service (DDoS) attacks. Routers are similar in computational power to the computer of the mid 1990's. Hence, BotMasters are able to abuse the processor cycle and memory resources of both a workstation and a router to undertake a range of tasks including, cracking complex password or encryption schemes.

DNS hacking

The Domain Name Server (DNS) is a dynamic address in most instances is allocated ISP to the router. However, the DNS may be easily changed manually by a non-technical individual through the router's web management interface. A compromised ADSL router, configured with a malicious DNS may have all of its traffic forwarded to a bogus DNS server (Heron 2007). When the unsuspecting user requests to access their bank, email or Microsoft update website they are instead redirected to what looks like the authentic website they would usually visit. The illegitimate website may then be used to capture usernames and passwords entered by the end-user when attempting authentication. It may also be used to send malicious updates to end-user or redirect them to illegal websites.

Voice over Internet Protocol vulnerabilities

Voice over Internet Protocol (VoIP) uses the existing network infrastructure in-conjunction with ADSL routers to conduct voice communication between nodes. VoIP communication can only be permitted by opening specific ports to allow the transmission of packets between the external and internal VoIP hosts (Whitworth 2006). Opening ports on a router increases the number of holes an attacker may use to exploit a system. Furthermore, most VoIP devices are computers with scaled down web-servers allowing them to be queried and exploited like any web-server if not properly configured (Bradbury 2007).

If using NAT on a SoHo network this instantiates a problem when attempting to encrypt VoIP communication using IPSec (Walsh & Kuhn 2005). The problem lies within the header of the packet, which is encrypted by the router on all outbound traffic. This is problematic for the routing device as it is unable to read the destination IP addresses of the sender and receiver. Hence, various publications (Tucker 2004; Walberg 2007) propose a feasible yet dangerous approach that end-users simply disable NAT and hence use public IP addresses for all of the internally networked devices. This approach would permit all internal workstation to be accessible to potential offenders over the Internet.

Embedded System Vulnerabilities

An ADSL router is a scaled down computer system matching the computational power of the desktop workstations of the mid 1990's. Collectively an ADSL router is an embedded system compromising of a processor, memory and embedded software. A single programming error may cause numerous faults to consumers. Acre (2003) discusses that the research department at Core Security Technologies discovered a stack and heap buffer overflow error within many embedded systems. More specifically this error targets routers and may allow an attacker to bypass all authentication techniques thus acquiring effortless access to the router.

Tsow (2006) argues that the reason embedded systems and more specifically embedded software are being targeted within routers is that virus and malware detectors are unable to scan embedded software. More specifically the firmware can be compiled with a static malicious DNS server address. The newly compiled malicious firmware may be uploaded to the router prior to sale. Unless a forensic examination is made, scanning the router's operating system for malicious code or processor activity in not available. Numerous router firmware images are open-source, permitting an attacker to experiment with the software to discover flaws and weaknesses prior to launching an attack (Tsow 2006). Unlike a computer with a new operating system upgrade from Windows XP to Windows Vista, a highly skilled hacker changing the firmware on a router without authorisation should see no difference to the consumer (Tsow 2006). The router is ideally intended to allow trouble free Internet access for the non-technical user.

ADSL ROUTER FORENSICS FEASIBILITY

Digital forensics

Reith et al. (2002) agree that online offenders believe there is still a degree of anonymity when using technology to commit electronic crimes. However, computer forensics which once dealt solely with 'persistent data' (Nolan et al. 2005) now takes on a new stream of evidence acquisition from volatile memory. Forensics investigators have identified that volatile evidence may remain on a computer system a long time after the crime was committed. Hence, because certain electronic devices do not have persistent storage medium does not mean they cannot be forensically investigated. Desktop workstations are no longer the sole means of forensic interest to investigators with offenders breaching laws on cell phones, PDAs and importantly network routers. Researchers have begun developing methods to collect evidence from devices with volatile memory such as Jansen and Ayers (2004) in *Guidelines on PDA Forensics* and also Jansen and Ayers (2006) *in Guidelines on Cell Phone Forensics*. However, researchers have yet to pursue the development of guidelines, frameworks, models and practices on acquiring volatile memory evidence from network routers.

Computer systems with storage mediums such as hard drives and volatile memory may be forensically analysed using pre-tested models, frameworks and techniques. Reith et al. (2002) outline various forensic protocols and argue that these practices are not standardised. Each entity whether it is the Federal Bureau of Investigation (FBI) or US Department of Justice alters these protocols dependant on their needs and requirements. Alternatively these entities may also develop new frameworks depending on the device, operating system and resources available to the forensic investigator although do not release this to the public realm. The numerous digital forensic frameworks and models available (Carrier & Spafford 2003; Department of Justice 2001; Ó'Ciardhuáin 2004; Palmer 2001) provide a set of principles and techniques for acquiring, preserving, analysing and presenting digital evidence acquired from numerous digital devices. Unfortunately neither of these acknowledges ADSL routers as a potential source of evidence. The Department of Justice (2001) does however recognise network routers as a potential source of evidence for forensic investigations– specifically the configuration files.

Volatile memory forensics

Although numerous digital devices have had their volatile memory investigated for potential evidence, viruses and malware are yet to be extracted by forensic investigators. Malicious software such as the Code Red and SQL Slammer work reside solely in volatile memory (Carrier & Grand 2004). Hence, investigating the hard drive may not have recovered evidence of a worm. From a computer forensics perspective, investigating the memory contents may recover the current running processes, unencrypted data such as passwords and current user activity (Carrier & Grand 2004). One such tool which is capable of forensically examining the contents of volatile memory includes WinHex (WinHex 2007). This tools permits investigators to acquire a memory dump which may easily recover unencrypted passwords which have not yet been overwritten in volatile memory (Casey 2004). The tool is specifically designed for desktop workstations although it does show that an extraction of evidence from volatile memory is feasible.

A proof of concept device 'Tribble' has been developed that allows an investigator to perform a forensic analysis on a live workstation (Carrier & Grand 2004). The concept was a Peripheral Component Interconnect

(PCI) hardware based card which is installed in a desktop workstation prior to its usage. If an attack on the target system was undertaken and an analysis was required, Tribble could be used to forensically capture evidence from the volatile memory modules (Carrier & Grand 2004). However, this product requires that it be installed prior to any attack or investigation being carried out. Furthermore, in the context of ADSL routers such a device would require each individual or vendor to attach an additional chipset to their device prior to its sale and usage which may not be feasible for the customer or the vendor from an economical sense.

Typical computer forensic tools may examine a cloned hard disk within an isolated laboratory. However, data of a volatile nature cannot be removed from the location of interest as shutting down the device would erase the non-persistent data. According to Nelson et al. (2006) network forensics would typically follow the systematic process of:

- Closing the network ports or processes that allowed the intruder to carry out the attack.
- Acquire the drive which had been compromised.
- Make an exact replica of the drive with a bit-stream image.
- Verify the duplicate image to the original image.

However, using the procedures detailed is not feasible as closing ports, and making a replica would alter the volatile data and hence erase potential evidence. For this reason, there is a need for sound volatile memory forensic methods which can extract evidence at the scene of the crime within a timely manner, without interfering or overwriting existing evidence (Petroni et al. 2006). Thus, the proposed systematic principles are not ideal techniques for router forensics as each step may potentially alter or erase the evidence within memory.

Difficulties of volatile memory modules

The router's various memory modules are the key to extracting data of forensic interest (Brown 2006). The only persistent component of an ADSL router is the non-volatile Random Access Memory (NVRAM) or flash memory and may be forensically examined without altering key evidence to determine if the firmware or operating system has been altered. NVRAM on all ADSL routers should contain; power on boot procedures and configuration files for the particular network. The Dynamic Random Access Memory (DRAM) or Static Random Access Memory (SRAM) contains; current running processes, routing tables, simplified network logs, network and connectivity statistics (Brown 2006). Any device which can not be switched off is classified in computer forensics as a 'live' device. Investigating a 'live' device follows the scientific principle that any action used to observe the evidence may in essence alter it. Alternatively, shutting down the device may erase the data of forensic interest located in the volatile memory modules. Nikkel (2005) suggests the following assumptions about router forensics whilst attempting to manifest techniques, methods and tools:

- The router where the evidence is stored will not be in full custody of the investigator when carrying out the investigation.
- A forensic image of the router's volatile memory may not be feasible to initiate.
- The evidence on the router is dynamic and may be erased or altered before the forensic examination may take place.
- Verification of the data collected may prove difficult or impossible if the router is switched off hence erasing the volatile memory.

Hence, when forensically examining volatile memory in a device such as a router Petroni et al. (2006) state that in order to decipher the memory status at any point the investigator must thoroughly analyse two main criteria. Firstly, identify how the operating system would generally interact with the memory (i.e. what should be in a specific memory cell in a normal state) and secondly, how the memory cells would have been rearranged or altered during and after an incident occurs (i.e. what the memory cells should contain after the incident occurred).

Industry router forensics

Although Cisco routers encompass the same volatile memory as SoHo routers they have had some publicity on methods to forensically investigate the device after a breach has occurred. Livingston (2005) details what evidence (if any) should be extracted from volatile memory initially if an incident occurs. Although she only details the commands on a Cisco router using the 'show' command, these commands may be replicated on common ADSL routers through the Linux telnet or SSH interface. Ideally a connection would be instantiated using HyperTerminal or the equivalent to allow logging of the session. The follow points detail a list of items of evidence ranked in importance from highest to lowest in conducting a forensic examination (Livingston 2005):

- Router system clock information.
- Firmware type and version.
- IP address of authenticated users.
- Configuration files located in NVRAM – boot sequence, default libraries.
- Routing table information.

To date there is only one router forensic tool available which is constantly undergoing research and testing. All of the evidence above is automatically collected by the evidence collection tool namely the "Cisco Router Evidence Extraction Disk" (CREED) created by researcher Thomas Akin (2002). The tool is a small 1.7MB program which resides on a bootable floppy disk, requiring minimal interaction from the investigator to complete the acquisition procedure. The investigator places the floppy disk into the computer, connects a serial cable from the acquisition computer to the router, and once booted the investigator types 'acquire' in the console and the automated process acquires the evidence (Akin 2002). The tool does however require the serial port on the router as part of the connection process which unfortunately is not standard on ADSL routers. Furthermore, on many of popular ADSL routers, consumers are only presented with numerous Ethernet ports and a Registered Jack (RJ11) telephone line port.

Investigative procedures

Conducting an investigation on an ADSL router is feasible and in many instances is able to acquire evidence which may be of use to an investigator. Table 1 below details a list of commands which may be issued on a Linux workstation. However, since ADSL routers operate under a Linux architecture these commands may also be issued on an ADSL router once a telnet or SSH connection is made (Burdach 2004). However, although an investigation may be of use to an extent, executing each of the commands may in fact overwrite a potential important piece of data in volatile memory.

Table 1 Investigation commands for an ADSL router

Priority	Description	Command
1	Current date and time	date -u
2	Cache tables	arp –an route –n
3	Open TCP/UDP Connections	/proc/net/tcp /proc/net/udp
4	Image of physical memory	/proc/kcore
5	Loaded kernel modules	/proc/modules insmod –f /proc/ksmys
6	Active processes	lsof -n –P –l
7	Useful extra information • Version • Host name • Domain name • Hardware info • Swap partitions • Local partitions • Mounted file systems • Uptime	 /proc/version /proc/sys/kernel/name /proc/sys/kernel/domainame /proc/cpuinfo /proc/swaps /proc/partitions /proc/self/mounts /proc/uptimes

ACQUIRING EVIDENCE USING JTAG

The first principle in undertaking a thorough forensic investigation of any digital device is to ensure that the data of forensic interest remains unchanged throughout the entire process. As detailed previously the number of external ports on an ADSL router is quite limiting in their functionality. A prospective method to acquire evidence from an ADSL router is to utilise the Joint Test Action Group (JTAG) boundary-scan. The JTAG port is generally utilised by manufacturers for testing circuit boards before they are released to the public for sale

purposes (Breeuwsma 2006). However, the same principles which are applied to testing circuit boards can also be used to forensically acquire data and/or an image from a specific embedded system. The following section will briefly outline the potential benefits and methods by which the JTAG boundary-scan may be used.

Potential benefits

Many forensic applications load data into the memory which is then executed by the processor. In the instance of acquiring evidence from a hard disk on a desktop workstation, a boot disk could be utilised where direct write access to the disk is restricted. Only volatile memory and the processor are utilised and data is read from the hard disk and is transmitted over a network (using Net Cat) creating a replicated forensic image. Whilst, data could be retrieved in ADSL routers utilising a direct Ethernet connection, this would in essence load data into memory, potentially leaving a memory footprint which contravenes with the first principle of undertaking a forensic investigation. Secondly, had the user set any passwords, attempting to retrieve or bypass these may also prove difficult (Breeuwsma 2006) and evidence may be lost before access is granted. Utilising the JTAG port permits the investigator to communicate directly with the memory modules acquiring evidence in a sound forensic manner.

In numerous instances ADSL routers halt when a software error is executed or when all available system memory is exhausted. Consumers, whom face these dilemmas and contact their Internet Service Provider, are instructed to power cycle their router, which clears memory. Furthermore, the power cycle will also cause the operating system to reboot and thus resolving any programming error within the software. Unfortunately power cycling a router will clear memory and hence remove all potential evidence. The investigator may not be aware of how long the router has been operating for and hence a sudden exhaustion of memory by loading a forensic tool may again cause the router to come to a halt. Utilising a JTAG port allows the investigator to communicate directly with the processor and hence bypassing the need for memory to be allocated to specific forensic tools for execution (Breeuwsma 2006).

Using JTAG for communication

The JTAG interface is already publicly used amongst the hacker community for imaging firmware onto various ADSL routers but more specifically the Linksys WRT54g. By default the Linksys WRT54g does not have a user accessible JTAG interface as with many of the publicly available ADSL routers (Figure 1). However, resoldering a new 12 pin header onto the board permits the user to connect a pre-purchased or a custom made un-buffered JTAG cable as outlined by the developers of the embedded system operating system ‘OpenWRT’ (OpenWRT 2007).

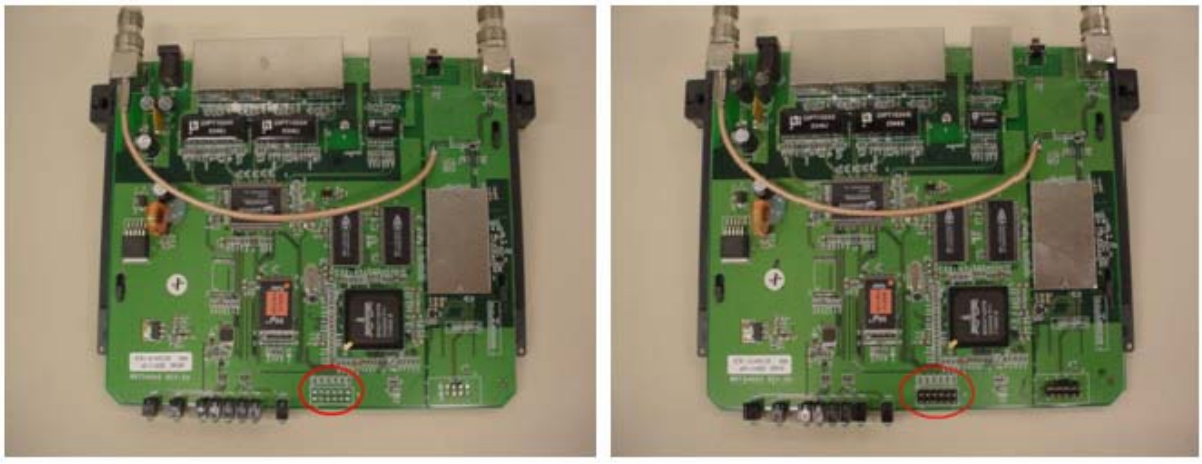

Figure 1 A Linksys WRT54g with and without a JTAG interface header

The JTAG interface cable may either connect to the serial or parallel port of a workstation. Once a connection to the onboard Linksys WRT54g JTAG interface is established, a utility such as the “Hairy Dairy Maid Debricking” utility may be utilised. This tool may be run to debug and program the onboard memory modules. Whilst, the developer of the firmware recovery utility chooses to remain anonymous for legal purposes, the software is not full proof and may damage the router beyond repair. Does utility does permit a user to flash, erase or backup the current operating system stored on the Linksys WRT54g router (HairyDairyMaid 2007).

Whilst the utility does permit an end-user to communicate directly with the processor and hence execute commands it does so in a non-forensic manner. Utilising the same principles of direct processor communications, research will be undertaken into developing and testing a tool which may essentially trick the processor into retrieving the contents from all memory modules and presenting this information in a way which is feasible to understand for a forensic investigator.

CONCLUSION:

The current rate of research on ADSL router forensics is almost non-existent. Research, tools, and methodologies on computer hard disk forensics have exhausted itself over the past few years, and it appears that the era of cell phone forensics is beginning to gain interest. However, many individuals may be underestimating the potential crimes associated with the use of ADSL routers. Until there is a wide interest amongst the forensic computing community, the number and severity of these crimes may only escalate. A forensic acquisition solution for ADSL routers may also apply to a wide range of consumer electronics in the future.

The aim of the paper was to increase knowledge on the yet to become mainstream area of ADSL router forensics. Whilst routers may already be used to commit electronic crimes as detailed in this paper, as technology progresses the rate and publicity of these crimes should also increase. As the cost of manufacturing consumer electronics decreases, the next few years should see ADSL routers with increased memory and processing power for enhanced firewall rule sets, improved VoIP capability and furthermore permit an increase in the number of simultaneous connections.

REFERENCES:

Acre, I. (2003). The Rise of the Gadgets. IEEE Journal, 1(5), 78-81.

Akin, T. (2002). CREED (Cisco Router Evidence Extraction Disk), URL http://web.archive.org/web/20040214172413/http://cybercrime.kennesaw.edu/creed/ Accessed 10 April, 2007

Breeuwsma, I. M. F. (2006). Forensic imaging of embedded systems using JTAG (boundary-scan). Digital Investigation, 3(1), 32-42.

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

Burdach, M. (2004). Forensic Analysis of a Live Linux System, Pt. 1, URL http://www.securityfocus.com/infocus/1769 Accessed 20 April, 2007

Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, 2(2), 1-20.

Carrier, B. D., & Grand, J. (2004). A hardware-based memory acquisition procedure for digital investigations. Digital Investigation, 1(1), 50-60.

Casey, E. (2004). Tool review-WinHex. Digital Investigation, 1(2), 114-128.

Chang, R. (2002). Defending against flooding-based distributed denial-of-service attacks: a tutorial. IEEE Communications Magazine, 40(10), 42-51.

Department of Justice. (2001). Electronic Crime Scene Investigation - A Guide for First Responders, URL http://www.ncjrs.gov/pdffiles1/nij/187736.pdf Accessed 2 April, 2007

HairyDairyMaid. (2007). WRT54G EJTAG DeBrick Guide, URL http://www.ranvik.net/prosjekter-privat/jtag_for_wrt54g_og_wrt54gs/HairyDairyMaid_WRT54G_v22.pdf Accessed 1 September, 2007

Jansen, W., & Ayers, R. (2004). Guidelines on PDA Forensics, URL http://csrc.nist.gov/publications/nistpubs/800-72/sp800-72.pdf Accessed 5 April, 2007

Jansen, W., & Ayers, R. (2006). Guidelines on Cell Phone Forensics, URL http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf Accessed 12 April, 2007

Livingston, O. (2005). Effective Data Investigation on Cisco Routers, URL http://www.securitydocs.com/library/3474 Accessed 23 March, 2007

Nikkel, B. J. (2005). Generalizing sources of live network evidence. Digital Investigation, 2(3), 193-200.

Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). First Responders Guide to Computer Forensics, URL http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf Accessed 22 March, 2007

Ó'Ciardhuáin, S. (2004). An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3(1), 1-22.

OpenWRT. (2007). JTAG Cables, URL http://wiki.openwrt.org/OpenWrtDocs/Customizing/Hardware/JTAG_Cable Accessed 10 September, 2007

Palmer, G. (2001). A Road Map for Digital Forensic Research. Paper presented at the First Digital Forensic Research Workshop, Utica, New York.

Petroni, N. L., Waltersb, A., Frasera, T., & Arbaugha, W. A. (2006). FATKit: A framework for the extraction and analysis of digital forensic data from volatile system memory. Digital Investigation, 3(4), 197-210.

Rajab, M. A., Monrose, F., & Terzis, A. (2006a). On the Impact of Dynamic Addressing on Malware Propagation. Paper presented at the Proceedings of the 4th ACM workshop on Recurring malcode WORM '06, George Mason University, Fairfax.

Rajab, M. A., Zarfoss, J., Monrose, F., & Terzis, A. (2006b). Security and privacy: A multifaceted approach to understanding the botnet phenomenon. Paper presented at the Proceedings of the 6th ACM SIGCOMM on Internet measurement IMC '06, Rio de Janeiro, Brazil.

Ramachandran, A., & Feamster, N. (2006). Understanding the Network Level Behavior of Spammers. Paper presented at the Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '06, Pisa, Italy.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. International Journal of Digital Evidence, 1(3), 1-12.

Stamm, S., Ramzan, Z., & Jakobsson, M. (2006). Drive-By Pharming, URL http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf Accessed 3 April, 2007

Szewczyk, P. (2006). Individuals Perceptions of Wireless Security in the Home Environment. Paper presented at the 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia.

Tsow, A. (2006). Phishing with Consumer Electronics: Malicious Home Routers. Paper presented at the 15th International World Wide Web Conference, Edinburgh, Scotland.

Tucker, G. S. (2004). Voice Over Internet Protocol (VoIP) and Security, URL http://www.giac.org/practical/GSEC/Greg_Tucker_GSEC.pdf Accessed 12 March, 2007

Walberg, S. (2007). How to configure SIP and NAT. Linux Journal, 2007(155).

Walsh, T. J., & Kuhn, D. R. (2005). Challenges in securing voice over IP. IEEE Security & Privacy Magazine, 3(3), 44-49.

Whitworth, M. (2006). VoIP – a call for better protection. Network Security, 2006(4), 11-12.

WinHex. (2007). WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor, URL http://www.winhex.com/winhex/ Accessed 13 August, 2007

COPYRIGHT