Dept of Computer Science, P B SIDDHARTHA COLLEGE OF ARTS & SCIENCE, VIJAYAWADA.
UGC SPONSORED NATIONAL SEMINAR ON "CYBER SECURITY WITH SPECIAL FOCUS ON CYBER CRIMES & CYBER LAWS (NSCS 2014)" on
15th & 16th November 2014-IJDCST SPECIAL ISSUE, PAPER –ID: IJDCST-06
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Network Forensics

V.Chandrika, M.Sc. (CS), Ch.Pavani,MCA,MTeach
Lecturer, dept. of Computer Science, K.B.N College, Vijayawada.
vutukurichandrika@gmail.com, chitrapu.pavani@gmail.com

Abstract: Research in the field of network forensics is gradually expanding with the propensity to fully accommodate the tenacity to help in adjudicating, curbing and apprehending the exponential growth of cyber crimes. However, investigating cyber crime differs, depending on the perspective of investigation. This paper presents the findings on the critical features for each perspective, as well as their characteristics of Network forensics. The paper also presents a review of existing frameworks on network forensics. Furthermore, the paper discussed on Network forensics: Tapping the Internet.

Keywords: Network forensics, Tapping, Internet.

Introduction

Computer forensics is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European court systems.

The F.R.E.D. family of forensic workstations consists of integrated forensic processing platforms capable of

handling the most challenging computer case. Available in mobile, stationary and laboratory configurations, these systems are designed for both the acquisition and examination of computer evidence. F.R.E.D. professional forensic systems, and the Digital Intelligence UltraBay 3d universal write protected imaging bay, deliver the ability to easily duplicate evidence directly from IDE/SAS/SATA hard drives, USB devices, Firewire devices, CDs, DVDs, LTO-4 tapes and PCCard/Smartmedia/SD-MMC/Memory Stick/Compact Flash media in a forensically sound environment.

C-DAC developed indigenous tools for collecting digital evidence pertinent to different areas like disk forensics, network forensics, device forensics, live forensics, enterprise forensics, photo forensics and virtualized environment forensics.

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Cyber Forensic Solutions

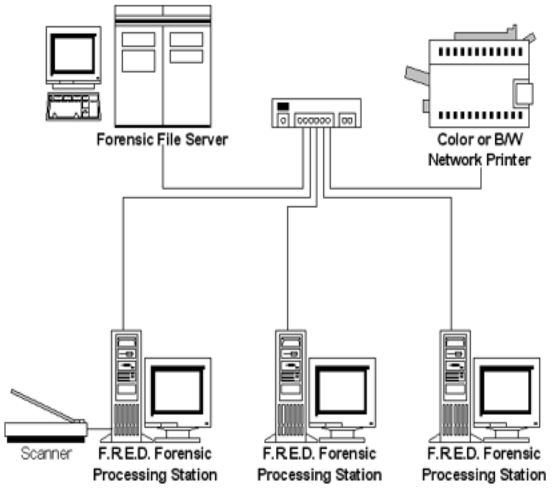
- Disk Forensics Tool: Suite with Disk imaging (True Imager), Data recovery and analysis (Cyber Check), S/W for tracing sender of e-mail, Forensic Data Carving (F-DaC), Forensic Registry analysis (F-Ran) and Forensic Thumbnail extraction (F-Tex) tools

- Network Forensics Tool: Suite with Network Session Analyser (NeSA), Forensic Log Analyser and S/W for tracing sender of e-mail

- Mobile Device Forensics Tools: Software solution for acquisition and analysis of mobile phones, smart phones, Personal Digital Assistants (PDA) and other mobile devices (Mobile Check), s/w for analyzing Call Data Records of various service providers (Advik) and forensic solution for imaging and analysing SIM cards (SIMXtractor)

- Live Forensics Tool (Win Lift): Software solution for acquisitions and analysis of volatile data present in running Windows systems

- Portable Forensics Toolkit: TrueTraveller is a portable forensics toolkit.



What is a Forensic Network?

Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.

A Forensic Network is a series of processing and imaging computers connected and integrated directly with a high-speed, high-capacity server to share resources. The file server operates as the backbone of the Forensic Network and is used as a central storage facility for Forensic Images as well as applications software for use by the client processing and imaging stations. Workstation clients on the network perform the actual imaging and processing tasks, while the central file server stores the images and case work. High speed scanners and color printers can also be made available as shared resources on the network. Multiple forensic clients can access case and image files simultaneously without duplicating information on several workstations. File and image storage space is centralized at the file server reducing the localized storage requirements at the workstation clients.

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Forensic networks are typically physically isolated from other networks (including the Internet) due to the sensitive nature of the data being stored. This means that the forensic network must also have its own network services such as DNS, DHCP, and user account management. Lastly, there must be support for the long-term archival of evidence utilizing removable media - typically tape backups.

How Can a Forensic Network be Used?

The client workstations in a forensic network are used for the actual acquisition of forensic images. However, rather than storing those images locally on each client, the images are recorded directly to the high-capacity fault-tolerant storage array on the file server over the network. These workstations can be pre-configured to access the network directly from DOS or Windows operating environments. Only a minimum of local storage is required on each client processing station for the operating system(s) and temporary work space. In fact, CD and network PXE boot disk images are provided such that each station can be brought completely onto the network requiring absolutely no hard drive facilities at all!

The forensic file server maintains a high capacity RAID6 storage array. Each RAID module hs two redundant power supplies as a dedicated power source for the RAID array itself. This online storage is used for maintaining forensic images as well as application and forensic software and utilities. The file server is also configured with a Robotic Tape Library for system backups and offline storage of case information and images once online access to the information is no longer required. This file server comes pre-configured and installed with a highly optimized SUSE Linux Enterprise Server. Microsoft Certified (MCSE, MCPS) and Novell Certified (CNA, CNE) personnel on our staff ensure that these network operating systems are properly configured and installed prior to delivery.

Once the forensic images are recorded directly on file server storage space, any forensic client workstation on the network can be used to process the information. Images can be restored directly from the network to work drives on each client or processed in place on the file server. Multiple clients can be used to process a single image simultaneously from the network without requiring local storage at the workstations. One or more shared printers may be installed on the network in order to provide print services to all the client workstations.

The file server can also be used to store "functional" images of operating environments for testing and analysis. Symantec Ghost images can be pre-configured and stored on the file server and then restored to any of the network clients as needed. Want to see how a particular piece of software behaves in Windows? Deployment of pre-configured functional images can be a tremendous time saver when needed to research or test the behavior of multiple operating systems!

The forensic file server not only serves as a centralized facility for the storage of forensic images, case information, and functional images, but also a resource for the production and printing of reports and other day-to-day operational requirements. Furthermore, this centralized resource can also be

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

used to allow or deny access to any of the forensic images or information on the laboratory network as your organization's requirements dictate.

Why a Forensic Network?

Faster Than a Local Hard Drive

Image a hard drive directly to a Forensic File Server 25% faster than you can image to a local mechanical hard drive... DIRECTLY to the server over standard Copper Gigabit Ethernet. There's no need to image to your workstation and then copy it up to a slow server.

Significantly Faster Than a Windows Server

A Forensically Optimized Network Operating System is 30% faster than Windows Server running on the same hardware!

12.1 GB/Minute Imaging Speeds From Four Workstations Simultaneously

Real-world forensic benchmark utilizing Tableau Imager (TIM) to image drives connected to the UltraBay III on our FRED Workstations.

Keep Your Existing Clients

Use the same Operating Systems on your desktop as always (i.e. Windows 7). Our Forensic Network Operating System integrates seamlessly with your existing clients - no additional client software is required.

Centralized File Storage

Consolidate your storage investment. No need to buy lots of standalone hard drives to pass around your lab. No wondering where that case data is. Stop wasting money on individual hard drives or portable RAID arrays.

Centralized Access Control/Security

Decide who has access to what evidence from a single vantage point. Determine which investigators have access to which cases.

Centralized File Sharing

Allow multiple investigators to work on a single case using a single set of Data Files.

Centralized Data Backup

Backup and Restore data from a single vantage point into a single offline repository using a 16 tape LTO-5 robotic tape library. Maintain your data in two separate locations at all times (online and offline).

0 to 60 in Two Days

FREDC equipment is typically installed in 2 days. Equipment assembly and configuration on Day 1, and your orientation/training on Day 2. Take your lab from an outdated workstation centric environment to a fully optimized forensic network in 2 days. (Your MIS / IT guys have been relying on networks since the late 80's - now its your turn to blow them away.)

Completely Configured

It's a complete network in a rack including all TCP/IP services (DNS / DHCP). Just connect your workstations with Cat 5e or Cat6 Gigabit Ethernet and you're ready to go! We establish a proven storage architecture that makes your access control simple

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

and your backup activities manageable. We even set up your backup jobs and establish your automatic drive mappings for you. Instead of imaging to a local hard drive (i.e. "D:") you simply use your network drive letters instead (i.e. "R:").

Easy to Maintain

We provide approximately a full day of orientation/training for the person(s) who will be managing the server. Since our server runs like an appliance (no blue screens, no weekly patches), the routine tasks are minimal. Adding/Removing Investigator accounts, performing Backups, and modifying access control (if required) are essentially all that needs to be done.

Easy to Use

The only thing your investigators (users) will notice is new (network) drive letters. Everything else stays the same!

What Options Should be Considered When Designing a Forensic Network:

How much online RAID6 storage do you require?

How many Forensic Clients would you like in your network?

Would you like a Shared Network Printer?

Digital Intelligence installs the Network at your facility.

Digital Intelligence configures your network to meet your security, administration, or functional requirements.

Digital Intelligence provides training on the day-to-day use and administration of your Forensic Network.

Digital Intelligence provides support to assist in the day-to-day administration and use of your Forensic Network.

Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. According to Simson Garfinkel, author of several books on security, network forensics systems can be one of two kinds:

"Catch-it-as-you-can" systems, in which all packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage, usually involving a RAID system.

"Stop, look and listen" systems, in which each packet is analyzed in a rudimentary way in memory and only certain information saved for future analysis. This approach requires less storage but may require a faster processor to keep up with incoming traffic.

Both approaches require significant storage and the need for occasional erasing of old data to make room for new. The open source programs tcpdump and windump as well as a number of commercial programs can be used for data capture and analysis.

One concern with the "catch-it-as-you-can" approach is one of privacy since all packet information (including user data) is captured. Internet service

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

providers (ISPs) are expressly forbidden by the Electronic Communications Privacy Act (ECPA) from eavesdropping or disclosing intercepted contents except with user permission, for limited operations monitoring, or under a court order. The U.S. FBI's Carnivore is a controversial example of a network forensics tool.

Network forensics products are sometimes known as Network Forensic Analysis Tools (NFATs).

Network forensics: Tapping the Internet

During the Gulf War, computer hackers in Europe broke into a UNIX computer aboard a warship in the Persian Gulf. The hackers thought they were being tremendously clever -- and they were -- but they were also being watched.

Just before penetrating the PACFLEETCOM computer and reading the Navy's email, the hackers hopped through a computer at Los Alamos Laboratory. And unknown to the attackers, every packet in or out of Los Alamos over the Laboratory's Internet connection was recorded and preserved for later analysis on magnetic tape.

The incident in the Persian Gulf became a cause celebre in the years that followed. Tsutomu Shimomura bragged about the incident in his book Takedown. Many experts in the field of computer security used the story as proof, of sorts, that the U.S. military was asleep at the switch when it came to computer security.

One of the more dramatic outcomes of the incident was a videotape played at the annual meeting of the American Association for the Advancement of Science in February 1993 -- a video that showed each of the attacker's keystrokes, replete with mistakes, and the results, as he systematically penetrated the defenses of the ship's computer and scavenged the system.

In the decade that followed the Gulf War, Moore's law had its way not only with processors, but with bandwidth and storage as well -- but each unequally. While the clock on the average workstation surged from 25 Mhz to 1.1 Ghz, and while the typical "big" hard drive jumped from a few hundred megabytes to 160 GB, bandwidth increased at a comparatively modest rate -- from 28.8 kbps to 384 kbps for many homes and small businesses. Even today, few businesses have more than a T1's worth of Internet bandwidth.

These trends are accelerating. For the foreseeable future, both the amount of information that we can store and our ability to process that information will far outpace the rate at which we can transmit information over large distances. As a result, where it once took the prowess of a national laboratory to systematically monitor all of the information sent over its external Internet connection, now this capability is available to all.

Today some organizations are following Los Alamos's precedent and routinely recording some or all of the traffic on their external Internet connections. Little of this information is actually analyzed. Instead, it is collected in expectation that it might be useful at some future point. After all, if you want to be able to review the information moving

over your Internet connection at some point in the future, you must record it now -- fast as they are, today's processors still can't travel back through time.

Capturing everything moving over the network is simple in theory, but relatively complex in practice. I call this the "catch it as you can" approach. It's embodied in the open source programs tcpdump and windump, as well as in several commercial systems like NIKSUN's NetVCR and NetIntercept, which my company, Sandstorm Enterprises, recently brought to market.

Another approach to monitoring is to examine all of the traffic that moves over the network, but only record information deemed worthy of further analysis. The primary advantage of this approach is that computers can monitor far more information than they can archive -- memory is faster than disk. So instead of being forced to monitor the relatively small amount of network traffic at the boundary between the internal network and the external network, you can actively monitor a busy LAN or backbone.

A second advantage of this approach is privacy -- captured traffic almost invariably contains highly confidential, personal, and otherwise sensitive information: if this data is never written to a computer's disk, the chances of it being inappropriately disclosed are greatly reduced.

In some circumstances, it may not even be legal to record information unless there is a compelling reason or court order. Call this the "stop, look, and listen" approach. This approach, pioneered by Marcus Ranum in the early 1990s, is now the basis of Ranum's Network Flight Recorder (NFR) as well as Raytheon's SilentRunner, the open source snort intrusion detection system, NetWitness by Forensics Explorers, and even the FBI's "Carnivore" Internet wiretapping system (since renamed DCS 1000).

Recently, Information Security magazine coined the term Network Forensic Analysis Tool (NFAT) to describe this entire product category. (Ranum coined the term "Network Forensics" back in 1997.)

With the heightened interest in computer security these days, many organizations have started to purchase monitoring appliances or have set up their own monitoring systems, using either commercial or open source software. If you are charged with setting up such a project, or if you are just curious about the technical, ethical, and legal challenges these systems can cause, read on.

Build a Monitoring Workstation

In many ways, a system that you would use for monitoring a computer network looks a lot like any other high-end Windows or UNIX workstation. Most run on a standard Intel-based PC and capture packets with an Ethernet interface running in promiscuous mode.

"Catch it as you can" systems immediately write the packets to a disk file, buffering in memory as necessary, and perform analysis in batches. As a result, these systems need exceptionally large disks -- ideally RAID systems. "Stop, look and listen" systems analyze the packets in memory, perform rudimentary data analysis and reduction, and write selected results to disk or to a database over the

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

network. Of course, no matter which capture methodology is employed, the disks eventually fill up, so all of these systems have rules for erasing old data to make room for new data.

How much attention you need to give the hardware you use for network monitoring depends to a large extent on the complexity of your network, the amount of data at the points you wish to monitor, and how good a job you want to do. If you are trying to capture packets as they travel over a 384kbps DSL link, a 66Mhz 486 computer will do just fine. If you are trying to make extended recordings of every packet that goes over a fully-loaded gigabit link, you will find it quite a challenge to build a suitable capture platform and disk farm.

To explore the differences between different operating systems and hardware platforms, Sandstorm Enterprises purchased two identically-configured Pentium III-based dual-processor systems with removable disk drives. One system was set up as a packet generator using a program that transmitted individually serialized Ethernet packets of varying sizes. The second system was set up with rudimentary capture software -- either tcpdump on the UNIX systems, or windump for Windows.

We then wrote an analysis package that examined the recorded dump files and calculated both the percentage of dropped packets and the longest run of dropped packets under varying network load. By holding the processor, bus, and Ethernet cards constant and loading different operating systems onto different hard disks, we were able to determine effects of different operating systems on overall capture efficiency. Once we found the best operating system, we were able to swap around Ethernet adapters and disable the second CPU to determine the effects of different hardware configurations.

The results of our testing were more reassuring than surprising. Over the six operating systems tested, FreeBSD had the best capture performance and Windows NT had the worst. Under FreeBSD, we found that Intel's EtherExpress cards had the best packet capture performance. Finally, we found that FreeBSD did a somewhat better job capturing packets when run with a single processor than when run with two processors, although if additional analysis work was being done at the same time on the same computer, having two processors was vastly preferable. The reason for this is that no process can dominate both processors at the same time, and thus one processor ends up doing packet capture, and the other processor ends up doing analysis.

Sandstorm used the results of this testing to choose the hardware configuration for its NetIntercept appliance, although the results are applicable to any organization setting up a monitoring system. Of course, for many installations the choice of hardware and software will largely be determined by available equipment, training, and the supported hardware or software of the monitoring software to be used.

For example, organizations with significant Linux experience will almost certainly prefer using Linux-based systems for their packet capture systems, rather than acquiring experience with FreeBSD. And unless you are on a heavily loaded 100BaseT network, the

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

overall packet capture differences between FreeBSD and Linux are probably irrelevant.

If you intend to record most or all of the traffic moving over your network, you need to spend as much time thinking about your disk subsystem as your processor and Ethernet card. Last year Sandstorm spent several months comparing IDE drives with the UDMA100 interface to SCSI LVD-160 drives. We also explored a variety of RAID systems. The conclusion: today's IDE drives are significantly faster than SCSI drives costing two or three times more per gigabyte stored.

This is not the result we were expecting, and it goes directly against the conventional wisdom that says SCSI is inherently better than IDE. Nevertheless, it does seem to be the ugly truth, at least for straightforward read/write tests in a single-user environment. Although we saw the highest performance with a hardware-based RAID 5 system manufactured by Advanced Computer & Network Corporation, we saw nearly the same performance with a RAID 5 system based on the 3Ware Escalade 7000 RAID controller.

Long-term storage of captured data is another problem entirely. Although you can build a terabyte RAID system for less than $2,000, backing this system up will set you back $4,000 for the AIT II tape drive and $120 for each 100GB cartridge. Absent extraordinary requirements, most users will elect not to back up their capture disks, and instead archive specific capture runs to CD-R or DVD-RAM drives.

Analyzing the Data

After you've taken measures to collect the information, your next big decision will be the analysis tools that you can bring to the table. If you have built your own system, your primary analysis tools will be tcpdump and the strings command. You can use tcpdump to display the individual packets or filter a few packets out of a large data set. The strings command, meanwhile, will give you a rough transcript of the information that passed over the network. Snort will allow you to define particular conditions that generate alarms or traps. If you purchase a commercial system, your analysis will be pretty much limited to the capabilities the system provides. That's OK, though, because analysis is really the strength of the commercial offerings.

In a world in which strong encryption was ubiquitous, the monitoring performed by these network forensics systems would be restricted to what's called "traffic analysis" -- every IP packet contains the address of its destination and the address of its sender. By examining the flow of packets over time, it's possible to infer when a person is working, who they are communicating with, what Web sites they are visiting, and other sorts of tantalizingly vague information. Traffic analysis is the stuff that a lot of military intelligence is built upon, and it can be very powerful.

Unfortunately, we do not live in a world in which strong encryption is ubiquitous. Largely as a result of the U.S. government's war on encryption in the 1980s and 1990s, the vast majority of personal, sensitive, and confidential information sent over the Internet

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

today is sent without encryption, open to eavesdropping, analysis, and misuse.

Using a network forensics tool you can spy on people's email, learn passwords, determine Web pages viewed, even spy on the contents of a person's shopping cart at Amazon.com. The tremendous power these systems have over today's networks makes them subject to abuse.

If you install a monitoring system, you should have a policy regarding who has access to use the system, under what circumstances it should be used, and what can be done with the information collected. In fact, you should have such policies even if you do not install an NFAT, since every UNIX workstation is a potential network wiretapping tool.

Indeed, none of these network forensics tools -- not even the FBI's Carnivore -- provide capabilities that are fundamentally new. Back in the 1980s, packet capture programs were available for DOS and UNIX. Using these programs, it was possible to eavesdrop on people's email, learn passwords sent without encryption, and otherwise covertly monitor information sent over networks. This vulnerability to covert monitoring is a fundamental property of most communications systems, including telegraph wires, long-range microwave links, and even semaphore.

But while monitoring was always possible in a networked environment, NFAT tools make monitoring considerably easier than ever before. On a gigabit network it is simply not possible for a human to examine each passing packet to see if it contains useful information. The power of these tools is their ability to rapidly distill down a large data set into manageable chunks.

As such, these systems are a double-edged sword for security and privacy. On the one hand, a powerful NFAT makes it possible to put a spotlight on a particular subject. You can, for example, covertly monitor all of the email messages sent between a pair of users. But on the other hand, these systems also make it possible to conduct surveillance of a network being used by thousands of people and limit the information captured and disclosed to external intrusions, system glitches, or one or two individuals under surveillance. Of course, this selective capability makes it far more likely that these surveillance capabilities will actually be used.

For example, in 1996 the FBI obtained its first Internet search warrant for the Internet backbone at Harvard University. The FBI was investigating a series of computer break-ins all over the world; they were all originating at Harvard from a variety of different machines belonging to the faculty of Arts and Sciences. But rather than record the contents of every TCP/IP connection, which would have subjected Harvard's entire community to unacceptable monitoring, the FBI used a program called I-Watch (developed by the Automated Systems Security Incident Support Team at the Defense Information Systems Agency in Washington, D.C.) that could be programmed to only capture TCP/IP connections that contained a particular keyword.

It turned out that the hacker was breaking into other computers and setting up a program called "sni256."

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

So by only recording TCP/IP connections that contained the letters "sni256," the FBI was able to restrict the data collection to those TCP/IP connections made by the attacker.

Ultimately, the monitoring capabilities made possible by an NFAT are not a tremendously big deal to anyone who has spent time working as a system administrator, since these are exactly the same sort of capabilities granted to a person with UNIX "root" or Windows System Administrator privileges. Most system administrators regard being able to read people's email and look into their files more as an unwanted responsibility than a right. It is a necessary capability that occasionally needs to be used, but generally administrators have better things to do than to nose around through other people's business. And while there are exceptions, generally people who abuse positions of trust do not retain those positions.

From a legal point of view, your right to monitor (or to be free from monitoring) depends on who you are, where you are working, and who is doing the monitoring. Corporations generally have free rein to monitor their own networks, provided that employees and network users are told in advance that the monitoring may be taking place. (It is not necessary to inform the employees before each specific instance of monitoring, however, so most corporations generally inform their employees with a posted policy and leave it at that.)

ISPs are required under the Electronic Communications Privacy Act (ECPA) to protect the privacy of their customers' electronic communications -- they can't eavesdrop on communications or disclose intercepted contents -- unless one of the parties to the communication has given consent, or if the monitoring is needed to maintain system operations, or in cases of a court-authorized intercept.

Generally speaking, most ISPs require their users to give implicit consent to any and all monitoring as part of their "terms of service" agreement, so for most practical purposes the ECPA doesn't give ISP users any privacy at all. Law enforcement agencies have the right to monitor without the consent or the knowledge of the individuals being monitored, provided they can obtain authorization from a court. However, they have the added restriction of minimization -- they can only capture and record information specified in their warrant.

Today there is gaping disconnect between the level of privacy that most users expect and what is both technically possible and legal. That is, most users expect that their computer use is largely anonymous and untracked. At the same time, computers are getting better at monitoring, more products are being introduced specifically for the purpose of monitoring, and legislation such as the USA PATRIOT Act is making monitoring even easier than it was in the past.

CONCLUSIONS

Full-content network monitoring is no longer the province of spooks and spies -- it's increasingly a practice that serves a variety of goals for both computer security and overall network policy. These days the underlying hardware is certainly up to the

ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

task, and some of the software that's out there, both commercial and free, is exceedingly good.

What hasn't caught up is our understanding of what to do with this technology -- what it is good for, and what uses should be declared out of bounds. In particular, few of the commercial or free offerings have facilities for watching the watchers -- that is, for logging the ways the systems have been used in an attempt to prevent misuse. Likewise, few organizations have developed policies for the appropriate use of this technology, other than catch-all policies that simply allow the organization to monitor anything for any purpose whatsoever.

Although there has been a lot of public opposition about monitoring technology in general, and about the FBI's Carnivore project in particular, ultimately these systems will be used by organizations because organizations need to understand what information is moving over their network connections. As such, it behooves us as technologists to understand how these systems work, to publicize their capabilities and their limitations, and to develop standards for their ethical use.

REFERENCES

1. Natarajan Meghanathan, Sumanth Reddy Allam and Loretta A. Moore, "Tools and Techniques for Network Forensics", International Journal of Network Security & Its Applications (IJNSA), Vol .1, No.1,April 2009

2. Yong Guan, "Network forensics", chapter 20, Computer and Information Security Handbook, Publisher: Morgan Kaufmann, Pub. Date: May 22, 2009, Print ISBN-10: 0-12-374354-0,WebISBN-10: 0080921949

3. Sriranjani Sitaraman, Subbarayan Venkatesan, "Computer and Network Forensics", chapter III, Digital crime and Forensic Investigation in Cyberspace Book, Edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos, 2006, ISBN-10: 1591408725.

4. Andrew Case, Andrew Cristina, Lodovico Marziale,Golden G. Richard, and Vassil Roussev. Face: Automateddigital evidence discovery and correlation.Digit. Investig.,5:S65–S75, September 2008.

5. Advanced automated threat analysis system. http://www.threatexpert.com.