Network Forensics: An Analysis of Techniques, Tools, and Trends

Ray Hunt, *University of South Australia*
Sherali Zeadally, *University of the District of Columbia*

Researchers in the growing fields of digital and network forensics require new tools and techniques to stay on top of the latest attack trends, especially as attack vectors shift into new domains, such as the cloud and social networks.

Digital forensics is a science concerned with the recovery and investigation of material found in digital artifacts, often as part of a criminal investigation.[1-3] Digital artifacts can include computer systems, storage devices, electronic documents, or even sequences of data packets transmitted across a computer network.

Network forensics is a branch of digital forensics that focuses on the monitoring and analysis of network traffic. Unlike other areas of digital forensics that focus on stored or static data, network forensics deals with volatile and dynamic data. It generally has two uses. The first, relating to security, involves detecting anomalous traffic and identifying intrusions. The second use, relating to law enforcement, involves capturing and analyzing network traffic and can include tasks such as reassembling transferred files, searching for keywords, and parsing human communication such as emails or chat sessions.

A GROWING FIELD

The evolution of network security, as well as its associated forensic processes and related toolsets, is largely driven by recent advances in Internet technologies. As more aspects of our daily lives migrate to online systems and databases—where they are subject to criminal activity—the need for sophisticated analysis tools is increasing accordingly. Some commonly stated reasons for using network forensics include

- analyzing computer systems belonging to defendants or litigants;
- gathering evidence for use in a court of law;
- recovering data in the event of a hardware or software failure;
- analyzing a computer system after a break-in;
- gaining information about how computer systems work for the purposes of debugging them, optimizing their performance, or reverse engineering them;
- collecting and analyzing live data packets to detect and potentially prevent a malicious attack; and
- learning more about zero-day attacks, particularly through the use of honeypots and honeynets.

This list merely scratches the surface of what network forensics can do as part of risk assessment and data recovery; the following example demonstrates the vital role this technology can play in an investigative process.

The TCP/IP family of Internet protocols carries most of today's online traffic information, and attackers can manipulate these protocols to spoof addresses or embed malware. In particular, they can embed data in unexpected places such as the options field in an Internet Control Message Protocol packet. ICMP messages are used to communicate error information, such as a requested service's unavailability or a host that cannot be reached, or to indicate congestion, such as a downstream router's lack of buffering capacity. There is no expectation that ICMP

Published by the IEEE Computer Society

packets will carry application data, so most firewalls and intrusion-detection/prevention systems do not examine their contents, resulting in a concealed channel that most network security systems simply cannot see.

Some intrusions can be difficult to detect and subsequently analyze—for example, a simple port scan might hide a serious stealthy attack on a crucial system resource. Intrusion analysis and the collection of forensically sound data thus seek answers to the following questions:

- Who generated the (incoming) intrusion or (outgoing) data transfer?
- What equipment and services were involved in gaining entry?
- Where did the intrusion come from, and what parts of the infrastructure were affected?
- Was the attack made possible because by limitations or weaknesses in incoming or outgoing security mechanisms?

This real-time analysis process involves collecting, storing, and tracing data and then recovering the system, all while continuously scanning traffic and logs. As Figure 1 shows, the recovery process starts with security and then moves into forensic analysis—who perpetrated the attack and from where—followed by getting the system going again.

A CONTINUING EVOLUTION

Researchers in the growing fields of digital and network forensics require new tools and techniques to stay on top of the latest attack trends, especially as attack vectors shift into new domains, such as the cloud and social networks.

Several open source tools are available for general forensic analysis of open ports, mapped drives, and open or mounted encrypted files on live computer systems. The currently available open source tools include Sleuth Kit (www.sleuthkit.org), Scalpel (www.digitalforensicssolutions.com/Scalpel), and DEFT Linux (Digital Evidence & Forensics Toolkit, www.deftlinux.net); well-known commercial products include EnCase (www.guidancesoftware.com), FTK (Forensic Toolkit, www.accessdata.com), ProDiscover (www.techpathways.com), and Helix (www.e-fense.com/products.php).

Some important differences

Traditionally, researchers performed computer forensics on stored or static data—for example, the contents of files or images on hard drives. This dead or postevent analysis is also referred to as reverse engineering. But in recent years, there has been an increased emphasis on live system analysis, examining network traffic as it arrives.

Recent network forensics work has taken this one step further, focusing on live packet capture because packets are not normally stored upon arrival at their destination. Other types of live capture focus on attacks that leave no trace on the computer's hard drive because the attacker only exploits information in the computer's volatile memory, including encryption keys.

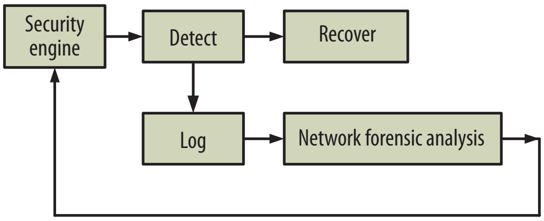

Figure 1. Real-time detection, recovery, and forensic analysis process. The process collects, stores, and traces data and uses it to perform real-time recovery while carrying out forensic analysis to determine the source of an attack.

Network forensics is concerned with monitoring network traffic to see if anomalies exist and whether they indicate an attack or could lead to one. The objective is to determine the attack's nature and then capture, store in a forensically sound manner, analyze, and, finally, present some visual form of it. Because an attacker might have erased all the log files on a compromised host, network-based evidence might be the only material available for forensic analysis.

Unlike digital forensics, which retrieves information from a computer's disks or other storage devices, network forensics retrieves both traffic and information about which ports it used to access the network. Frequently, investigators and adversaries use the same tools: one using the tools to cause an incident and the other using them to investigate it. Current examples include Wireshark, TCPDump, the NetScanTools Pro toolkit (www.netscantools.com/nstpromain.html), and the HENPA framework.[4] NetScanTools includes tools for network information gathering and security testing; IP/MAC address ranges and locations; visible, hidden, and writable shared folders; TCP/UDP port and DHCP analysis; SMTP and SNMP activity; and conventional packet viewers.

It might be possible to trace an attack back to its source—or at least to the ISP that carried the attack—while the attack is in progress, but in many cases, this type of analysis happens after the event. An essential aspect of live network forensics is the ability to collect data from the network fast enough so that no information is lost, which requires very fast processors and I/O devices as well as significant storage capacity. The best way to capture the data is to use a moving window of hours, bounded by the time by which an attack would be expected to be discovered. Sustained attacks of even 10 Gbps make significant demands on both the storage and processing of network forensic data, so, for example,

- 10-Gbps traffic flow with a two-hour sliding window requires 10 Tbytes of storage, and
- 20-Gbps traffic flow with a 12-hour sliding window requires 1 Pbyte of storage.

Because of the sheer sizes involved, only a sample of packets can be stored for subsequent analysis. The processing of network forensic data in real time demands large-scale distributed and parallel processing engines as well as the flexibility to customize the process. Even a sliding window of a few hours covering the duration of real-time traffic of interest could require terabytes of storage. The largest distributed denial-of-service (DDoS) attack on an ISP was recorded in 2010 and reached nearly 100 Gbps.[1] DDoS attacks of this size represent a hundredfold increase over the past 10 years, so current-generation network forensic analysis can require the implementation of parallel processing using supercomputers or Beowulf cluster computing.

It is unlikely that a single tool will suffice for any investigation—more than likely, investigators will use a combination of tools.

A suitable tradeoff between security and performance is also important. Complex tools and techniques could significantly affect the system and have serious consequences—for example, a disruption in communications induced by a network forensic tool's complexity could interrupt the infrastructure's fundamental functionalities due to their strong interrelationships.

Originally, digital and network forensics were viewed as closely related technologies, but in reality, the two are quite different. Digital forensics is driven largely by law enforcement organizations and the need to gain sound evidence to resolve criminal activities. Network forensics has evolved in response to the hacker threat and has strong links with security architecture, including firewalls, port blocking and filtering, threat assessment and surveillance, intrusion detection, and data loss prevention.

In digital forensics, the investigator and the attacker are at two different skill levels, with the investigator supposedly at a higher level. In network forensics, the investigator and the attacker theoretically have the same skill levels. The network forensics specialist uses many of the same tools and engages in the same set of practices as the person being investigated.

Common tools and techniques

Tools to assist with network forensics come in a variety of forms: some are merely packet sniffers, whereas others might focus on fingerprinting, mapping, location identification, email traffic, URLs, traceback services, and honeypots. Table 1 summarizes some of the tools more commonly used to support network forensic investigations, along with their properties.

It is unlikely that a single tool will suffice for any investigation—more than likely, investigators will use a combination of tools. For example, if the focus is on traffic analysis, and the investigators already understand the malware traffic's nature, basic Unix utilities such as Ngrep, TCPDump, or Omnipeek/Etherpeek might be sufficient. But when the investigation merits using a traffic analysis engine, tools such as Wireshark, NetMiner, Driftnet, or Xplico might be required. For commercial organizations, tools such as NetWitness offer a powerful range of analysis options for network monitoring or assessing insider threats, zero-day exploits, and targeted malware.

Cloud computing challenges

To date, although many systems are moving into the cloud, little research has been performed on the tools, processes, and methodologies necessary to obtain legally defensible forensic evidence in that domain.[5] Most investigations require evidence retrieval from physical locations, so cloud network forensic must be able to physically locate data with, for example, a given timestamp and trace network forensic data at a given time period, taking into account the authority at different locations.

Although the live and dead forensics categories still exist, cloud models present new challenges because network data is often difficult to locate, thus acquisition might be challenging or even impossible. Analysis without acquiring network data is impossible, so network forensic tools must evolve yet again, forming an amalgam of current live and dead collection and analysis methods, as well as incorporating the intelligence to find and predict artifacts based on forensic heuristics.

When conventional network forensic tools work, the only aspect that a cloud tool changes is the collection method. For situations in which acquisition is difficult, new network forensic tools will need to visualize physical and logical data locations in a way that indicates both obtainable and unobtainable data and metadata. In addition to visualization, forensic tools will need to use the cloud as a discovery engine for network forensic analysis. So, for example, a network forensic compilation that contains unobtainable data will need to be submitted to a cloud environment for heuristic and signature-based analysis. This is similar to the way network forensics investigators use antivirus engines to converge collections of incomplete data into reliable presentations as the number of submissions increases.[6]

Table 1. Tools commonly used to support a variety of network forensics investigations.

Tool	Features and advantages	Website	Attributes*
TCPDump, Windump	Command-line network packet analyzer that supports network forensic analysis	www.tcpdump.org; www.backtrack-linux.org/backtrack-5-release	F
Ngrep	Simple, low-level network traffic debugging tool	http://ngrep.sourceforge.net	F
Wireshark	Widely used network traffic analysis tool; forms basis of network forensics studies	www.wireshark.org	F
Driftnet	Listens to network traffic and picks out images; used in Backtrack v5	http://linux.softpedia.com/progDownload/Driftnet-Download-15905.html	F
NetworkMiner	Network forensic analysis tool that can be used as a passive network sniffer/packet-capturing tool	www.netresec.com/?page=NetworkMiner	F
Airmon-ng,Airodump-ng, Aireplay-ng, Aircrack-ng	Widely used suite of low-level traffic analysis tools for wireless LANs; used in Backtrack v5	www.backtrack-linux.org/backtrack-5-release	F, L, R, C
Kismet	Network detector, network packet sniffer, and intrusion-detection system for wireless LANs	www.kismetwireless.net	F
NetStumbler	Widely used wireless LAN analysis tool for devices and network traffic analysis	www.netstumbler.com	F
Xplico	Network forensic analysis tool that allows for data extraction from traffic captures; used in Backtrack v5	http://packetstormsecurity.org/search/?q=Xplico	F
DeepNines	Provides real-time identity-based network defense for content and applications, along with basic network forensics	www.deepnines.com	F
Argus	Used for network forensics, nonrepudiation, detecting very slow scans, and supporting zero-day attacks	www.qosient.com/argus	F, L
Fenris	Suite of tools for code analysis, debugging, protocol analysis, reverse engineering, network forensics, diagnostics, security audits, vulnerability research	http://lcamtuf.coredump.cx/fenris/whatis.shtml	F
Flow-Tools	Software package for collecting and processing NetFlow data from Cisco and Juniper routers	www.splintered.net/sw/flow-tools	F, L
EtherApe	Graphical network monitor for capturing network traffic	http://etherape.sourceforge.net	F
Honeyd	Improves cybersecurity by providing mechanisms for traffic monitoring, threat detection, and assessment	www.citi.umich.edu/u/provos/honeyd	F
Snort	Widely used, popular tool for network intrusion detection and prevention, as well as for network forensic analysis	www.snort.org	F
Omnipeek, Etherpeek	Low-level traffic analyzer for network forensics	www.wildpackets.com	F, L, R
Savant	Appliance for live forensic analysis, surveillance, network analysis, and critical infrastructure reporting	www.intrusion.com	F, R
Forensic and Log Analysis GUI	Log file analysis combined with network forensics; Python implementation	http://sourceforge.net/projects/pyflag	L
Dragon IDS	Provides network, host intrusion detection and network forensic capture analysis	www.enterasys.com; www.intrusion-detection-system-group.co.uk/dragon.htm	F, R, L, C
Infinistream, nGenius	Appliance for network forensics, incident analysis combined with session reconstruction and playback	www.netscout.com/products/enterprise/nSAS/ngenius_analysis/Pages/nGenius_Forensic_Intelligence.aspx	F, R, C
RSA EnVision	Provides live network forensics analysis, log management, network security surveillance, data leakage protection	www.emc.com/security/rsa-envision.htm	F, L, R, C, A
NetDetector	Appliance for network forensic analysis, network security surveillance, signature-based anomaly detection	www.niksun.com	F, R, C, A
NetIntercept	Appliance for network forensics, monitoring, and analysis	www.niksun.com/sandstorm.php	F, R, C, A
NetWitness	Addresses network forensic analysis, insider threat, data leakage protection, compliance verification, designer malware, and 0-day detection	www.netwitness.com; www.rsa.com	F, L, R, C, A
Solera DS	Appliance for live network forensics, application classification, metadata extraction, and analysis tools	www.soleranetworks.com/products/appliances	F, R, C, A

* F: filter and collect; L: log analysis; R: reassembly of data stream; C: correlation of data; A: application-layer view

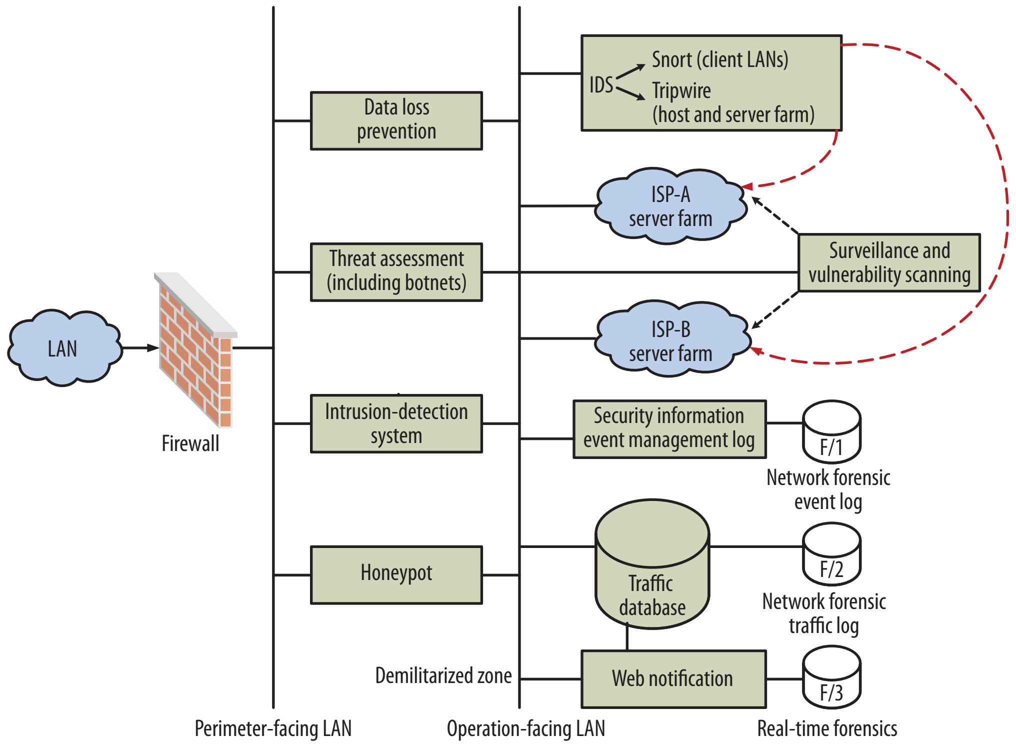
Data loss prevention
Snort (client LANs)
IDS
Tripwire (host and server farm)
ISP-A server farm
Threat assessment (including botnets)
Surveillance and vulnerability scanning
LAN
Firewall
ISP-B server farm
Intrusion-detection system
Security information event management log
F/1
Network forensic event log
Honeypot
Traffic database
F/2
Network forensic traffic log
Demilitarized zone
Web notification
F/3
Perimeter-facing LAN
Operation-facing LAN
Real-time forensics

Figure 2. Real-time adaptive security incorporating network intrusion detection and forensics logging.

New frontiers in network intrusion

Intrusion detection systems (IDSs) monitor network and system activity for malicious behavior or policy violations. Some systems might attempt to stop such an intrusion, but work on developing the ability to dynamically modify firewall rules in the face of an attack is still in its infancy. The combination of network forensics and intrusion detection might be adequate for a user's home system, when manual intervention is appropriate, but most intrusion-detection or prevention systems focus only on identifying possible incidents, logging information, and reporting such attempts. Therein lies the problem: any system of realistic scope or size that supports sensitive client data must include an automated combination of intrusion analysis with network forensic log analysis as well as dynamic feedback to modify access rules in the face of real-time attacks.

Some attackers explore a victim's network prior to launching an attack. A sophisticated IDS might be able to correlate data obtained from the attacker's reconnaissance—possibly along with additional log data—to either forecast the attack or to obtain better forensic evidence during or after the attack. However, although some progress has been made recently with distributed IDS architectures,[7] many IDSs cannot detect complex intrusions and distributed or coordinated attacks.

Figure 2 shows the components required to provide a forensically sound intrusion-detection and prevention system. The combination of such a system with reactive firewalls, traffic storage, and subsequent analysis provides a powerful forensic security architecture.

APPLYING NETWORK FORENSICS IN CRITICAL INFRASTRUCTURES

The critical infrastructures that attackers seek to launch their strikes against include not just the traditional areas associated with cybersecurity attacks, such as the water supply, traffic systems, and power and gas plants, but also any network system that could be considered critical to electronic commerce operations. The secure operations of, for example, banking, airline, communications, weather forecasting, and a host of other business enterprises depend almost entirely on a safe and secure network, which implies significant security issues for the ISPs and telecom operators that provide network infrastructures for these organizations.

Botnets

The environment in which an organization's user base operates continues to grow more hostile with the release of sophisticated and polymorphic malware such as Conficker, Koobface, and Zbot. DDoS attacks from botnets are a particularly serious global threat.[1] Botnets are now available for hire from criminal syndicates and can be used to mount DDoS attacks as well as to harvest identities and financial credentials. Additional attack methods include DNS spoofing and cache poisoning, Border Gateway Protocol (BGP) route hacking, and VoIP infrastructure flooding.

The network forensic process must be able to detect scans and probes outside the firewall and then use this data to inform a security information event management (SIEM) system that includes network forensic analysis tools. Although several SIEM engines are available, only a few include a logging system from which such data can be used later as evidence. A progressive threat assessment requires software monitors to trigger an alert when unusual time-based IP address patterns occur inside the secure perimeter, indicating a potential botnet intrusion.

Network forensics can play a pivotal role in botnet attack threat assessment because the SIEM system not only handles log files in a forensically sound manner, but it also stores a moving window of log data as evidence for potential future activity. Real-time adaptive feedback resulting from this analysis could potentially avert or minimize a real-time attack via firewall rule adaptation.

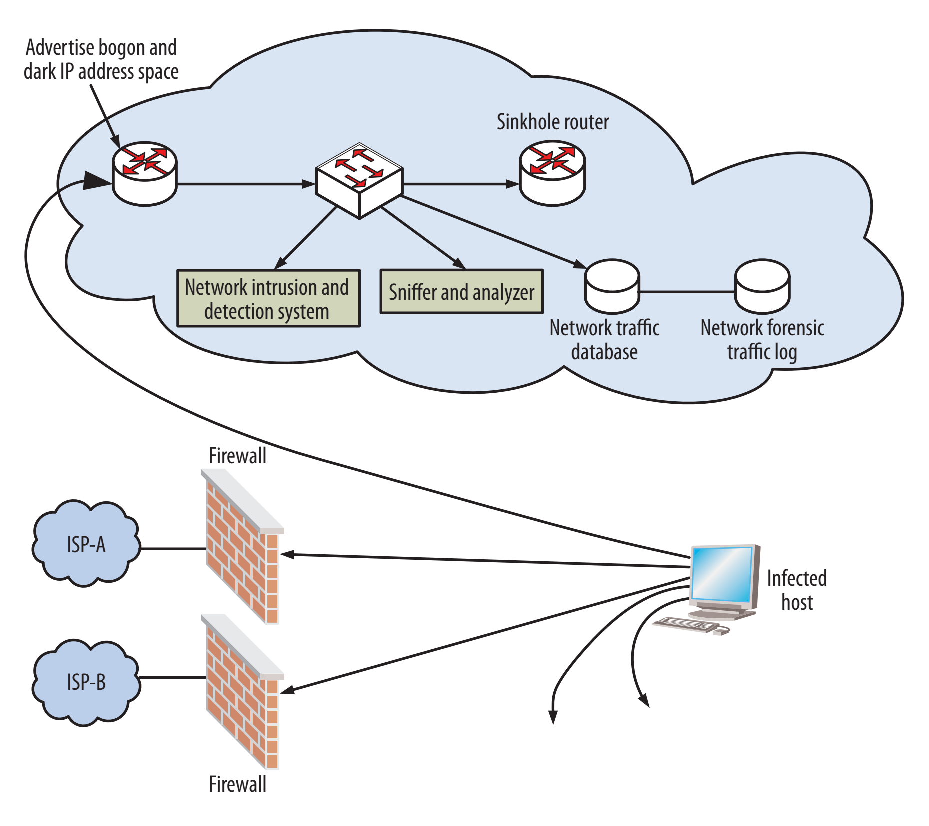
Advertise bogon and dark IP address space
Sinkhole router
Network intrusion and detection system
Sniffer and analyzer
Network traffic database
Network forensic traffic log
Firewall
ISP-A
ISP-B
Infected host
Firewall

Figure 3. Monitoring and analyzing worm propagation using a sinkhole. In this example, an infected host is scanning for others targets to infect. Because it sucks in any internally originated traffic destined for detailed network forensic analysis, the sinkhole can detect a worm's scanning activity.

Wireless networks

Wireless forensics, a subdiscipline of network forensics, provides the methodology and tools required to collect and analyze wireless network traffic. This new area has some techniques in common with fixed networks, along with some differences. Evaluating wireless networks from a forensic computing perspective helps to understand the current state of wireless misuse as well as the various tools and techniques used for identification, containment, and analysis. This research reveals the limitation of current tools and procedures for forensic computing investigations on wireless devices and networks, and highlights various forms of misuse that might escape detection by forensic investigations.

Some commercial players in fixed network forensics also claim wireless capabilities, at least for WLANs. Wireless network forensics requires these tools to analyze 802.11 headers and corresponding protocol data flows. From an open source perspective, there are no well-known, dedicated network forensicsanalysis tool alternatives.

Sinkholes

A sinkhole is a security tool that has the potential to accept, analyze, and forensically store attack traffic. Originally, ISPs used sinkholes to draw attack traffic away from a customer; more recently, they have used them to monitor attacks, detect scanning activity from infected machines, perform a forensic analysis, and generally monitor for malicious activity. Figure 3 shows how the sinkhole gateway router can be used to forward attack traffic to a sinkhole target router via a switch for basic Wireshark and TCP-Dump sniffing, intrusion detection, and forensic analysis.

Figure 3 also shows how a sinkhole can be used to monitor internally generated worm propagation. In this example, an infected host is scanning for other computers to infect. It pulls in any internally originated traffic destined for either bogon addresses or dark IP address space—bogon is unallocated address space, and dark IP space is allocated but unused. Consequently, the worm's scanning activity can be detected at the sinkhole. Monitoring the dark IP address space is essential because future worms might be written to purposely ignore such address blocks.

Additionally, a sinkhole can remove other noise from the network, such as reflector or backscatter traffic, which often indicates the start of a worm or DDoS attack. Backscatter traffic can occur as the result of large-scale DDoS attacks that use spoofed source addresses. A high increase in backscatter traffic could be the first sign of a new worm's release. Forensically sound event logs and network traffic storage of this traffic is therefore crucial.

EMERGING NETWORK FORENSICS AREAS

Network forensics has important roles to play in new and developing areas related to social networking, data mining and digital imaging, and data visualization.

Social networks

Social networking sites such as Google+, Facebook, Twitter, and YouTube have expanded astronomically in recent years, but because the success of such sites depends on the number of users they attract, there is pressure on developers to design systems that encourage behavior that increases both the number of users and their connections. Security has not been a high priority, leading to the emergence of inevitable security risks.

Obviously, there is a need for network forensic tools that address such an important area of usage, but to date, only traditional digital and network forensic tools are available.[8,9]

Data mining

Forensic profiles can be created using data mining technology, which provides a way to discover relevant patterns, thus generating profiles from large quantities of data. Although there has been significant work in the areas of extracting and analyzing digital evidence from physical devices such as hard disks, less work has been reported on data mining in portable storage devices such as flash drives, cell phones, digital cameras, radio frequency identification devices, compact disks, and iPods.[10]

The extraction of historical data from supervisory control and data acquisition (SCADA) systems, which are widely used to monitor and control equipment in various industries such as oil and gas refining, water and waste control, and transportation, is an important area that draws on the combination of data mining and network forensics.

There is currently no generic model for understanding the processes necessary to gather digital evidence from SCADA systems. However, such a model is needed to enable incident response, intelligence gathering, digital evidence collection, and legal action against system intruders. There is a distinct difference between the process of network forensics-based data mining investigations (where time-based data is analyzed to detect potential malware intrusion) and incident recovery and response (where the key purpose is to respond to an alarm and implement recovery).

Some work has been done to incorporate the use of decision trees as well as naive Bayesian, a priori, and neural network techniques.[11] Recently proposed architectures also incorporate mechanisms for monitoring process behavior, analyzing trends, and optimizing plant performance.[12]

Digital imaging and data visualization

Researchers have developed numerous state-of-the-art tools to assist in conducting digital crime investigations. However, digital investigations are increasingly complex and time-consuming due to the amount of data involved. The visualization of data obtained from such investigations is a new and developing area and has the potential to display significant volumes of data where the dimensionality, complexity, or volume prohibits manual analysis.

Data visualization is the graphical interpretation of high-dimensional data, which is particularly appropriate for obtaining an overall view and locating important aspects within a dataset. This is useful in network forensics because the data encountered in digital investigations is often significant in size, multidimensional, and complex. Consequently, obtaining an overall view can help digital investigators obtain a better understanding of the data and identify important aspects to assist in the recovery of appropriate digital evidence.[13]

Well-funded hackers, criminals, and terrorists are hiding data in new ways. Antiforensics tools are now as sophisticated as the tools they endeavor to defeat—Metasploit, for example, has developed three tools that have the potential to devastate automated forensic analysis tools.

Law enforcement agencies strive to both prevent such attacks and catch the perpetrators using the latest security and forensics tools. However, this work requires the design and implementation of a secure and forensically sound architecture. Resource limitations are a problem, and the process of developing innovative solutions will need to include computer software manufacturers, security tools providers, antimalware organizations, forensic tool providers, ISPs, and telecommunications companies. It will also require the dedication and diligence of users themselves.

Regardless of the exact tools used, developers must build forensics capabilities into security systems. Botnet attacks, for example, generate traffic logs, and tracing them in real time requires progressive threat assessment as attacks move through the system. Determining how the attacker gained access or how information leaked out of the organization while simultaneously quantifying the scale and impact of an attack as it happens are the very foundation of cohesive security and forensic processes. C

Acknowledgments

We thank the anonymous reviewers for their constructive comments, which helped us improve the article. We also express our gratitude to Gary Kessler and Ron Vetter for their support and encouragement throughout the preparation of this article.

References

1. D. Anstee, "Worldwide Infrastructure Security Report," vol. 7," *Arbor Networks*, Feb. 2012; www.arbornetworks.com/report.
2. NIST Information Testing Laboratory, "Computer Forensics Tool Testing Program," 2012; www.cftt.nist.gov.
3. NIST, 2012; "Guide to Integrating Forensic Techniques into Incident Response," http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.
4. J. Broadway, B. Turnbull, and J. Slay, "Improving the Analysis of Lawfully Intercepted Network Packet Data Captured for Forensic Analysis," *Proc. 3rd Int'l Conf. Availability, Reliability, and Security* (ARES 08), IEEE CS, 2008, pp. 1361-1368.
5. K. Ruan et al., "Cloud Forensics: An Overview," *Proc. 7th IFIP Conf. Cloud Computing*, Centre for Cybercrime Investigation, Univ. College Dublin, 2012; http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Overview_7th_IFIP.pdf.
6. S. Zimmerman and D. Glavach, "Cyber Forensics in the Cloud," *IA Newsletter*, vol. 14, no. 1, 2011, pp. 4-7; http://iac.dtic.mil/iatac/download/Vol14_No1.pdf.
7. C. Zhou, C. Leckie, and S. Karunasekera, "A Survey of Coordinated Attacks and Collaborative Intrusion Detection," *Computers & Security*, vol. 29, no. 1, 2010, pp. 124-140.
8. J. Cheng et al., "Forensics Tools for Social Network Security Solutions," Pace Univ., May 2009; http://csis.pace.edu/~ctappert/srd2009/a4.pdf.
9. H.V. Zhao et al., "Behavior Modeling and Forensics for Multimedia Social Networks: A Case Study in Multimedia Fingerprinting," *IEEE Signal Processing Magazine*, Jan. 2009, pp. 118-139.
10. V.H. Bhat, "A Novel Data Generation Approach for Digital Forensic Application in Data Mining," *Proc. 2nd Int'l Conf. on Machine Learning and Computing* (ICMLC 10), IEEE, 2010, pp. 86-90.
11. F. Camastra, A. Ciaramella, and A. Staiano, "Machine Learning and Soft Computing for ICT Security: An Overview of Current Trends," *J. Ambient Intelligence and Humanized Computing*, Oct. 2011; doi:10.1007/s12652-011-0073-z.
12. T. Kilpatrick et al., "An Architecture for SCADA Network Forensics," *Proc. IFIP Int'l Conf. Digital Forensics* (IFIP 06), Nat'l Center for Forensic Science, 2006, pp. 273-285.
13. B. Fei, "Data Visualisation in Digital Forensics," Univ. of Pretoria, 2007; http://upetd.up.ac.za/thesis/submitted/etd-03072007-153241/unrestricted/dissertation.pdf.

Ray Hunt *is an associate professor at the University of Canterbury, New Zealand; an adjunct associate professor at the University of South Australia; an honorary associate professor at Deakin University, Melbourne; and an adjunct associate professor at Edith Cowan University, Perth. His research interests include firewalls and security architectures, intrusion-detection systems, networking protocols, quality of service in wireless and mobile networks, broadband wireless technologies, and policy-based management security in heterogeneous mobile networks. Hunt received a PhD in computer science from the University of South Australia, Adelaide. Contact him at ray.hunt@canterbury.ac.nz.*

Sherali Zeadally *is an associate professor in the Department of Computer Science and Information Technology at the University of the District of Columbia, Washington, DC. His research interests focus on computer networks, including wired/wireless networks, network/system/cyber security, mobile computing, ubiquitous computing, multimedia, and performance evaluation of systems and networks. Zeadally received a PhD in computer science from the University of Buckingham, UK. He is a Fellow of the British Computer Society and a Fellow of the Institute of Engineering Technology, England. Contact him at szeadally@udc.edu.*