

The Greatest Information Survivability Threat: The Undetected Barbarian within the Gates

Andrew P. Snow
Department of Computer Information Systems
Georgia State University
asnow@gsu.edu

Mark Longworth
Forensics Explorers Division
CTX Corporation
mlongwth@forensicexplorers.com

Abstract --There is an increase in the incidences of financial, intellectual property, and trade secret theft using information systems. In addition, these thefts often involve insiders, such as current or past employees and contractors. A new genre of information system monitoring has evolved which can be used to help combat this type of Cybercrime, and is dubbed here as a DataCam capability. Such commercially available capabilities can be thought of as providing a non-disruptive 100% audit log which can be used for posterior information security forensic investigations triggered by insider or outsider behavior. Although the ability of businesses to deploy such tools appears to be legal in the US, the capability has significant privacy concerns, which may be potential barriers for deployment. If combined with procedural and technical privacy safeguards, the DataCam appears to offer a formidable tool in combating Cybercrime.

Introduction

By now, It is very clear that the line of defense offered by firewalls and intrusion detection systems is not doing the job. The firewalls are porous and the intrusion detection systems (IDS) reactionary. As quickly as means are developed to prevent firewall penetration, determined hackers and crackers develop other techniques. Also, reactionary IDS means high alarm volumes and the concomitant false alarms, which must be attended by security operators. As a result penetrants do significant damage, a lot of which is coming to our attention. More worrisome however, are not the information damage we detect, but that which goes undetected.

The Threat

Undetected damage or theft comes from two sources. The first is that of the outside penetrant who must run the firewall and IDS gauntlet without detection. The second is the trusted insider. Either of these undetected players are in a position not only to do damage or steal, but to do so repeatedly. Since these players are undetected, we have no way to measure frequency of these acts, or the amount of damage an enterprise has sustained.

When a security fault is detected, the security error can be addressed, and depending upon the seriousness of the breach, an investigation triggered. The amount of resources spent on the investigation is related to the magnitude of the damage or theft. If significant, investigators are left with the unsettling problem of determining WHAT ELSE has been damaged or stolen. At this point, the investigation becomes a forensic exercise. Security logs for firewalls and all enterprise servers must be investigated one by one. In large, complex IT infrastructures, this is a daunting task. First, consider security log content. It is possible that the event log has not recorded the information necessary to detect a perpetrator, as the more information collected real time by the security log, the more this action affects the IT mission of the device (resources and

capacity). Second, it is possible that the perpetrator could have penetrated the servers and defeated the log. At this point, the investigators might have to resort to individual computer forensic examinations - reconstructing what was on the hard drives over time and hoping that one can determine if the logs were changed. If log review is hard... computer forensics is even harder.

To combat Cybercrime more effectively, organizations need more intelligent alarming, and more complete archiving of information system transactions. Alarms more geared to content and destination, using more intelligent triggers, are needed to decrease the amount of false alarms. In addition, any increase in audit trail logging cannot come at the expense of user responsiveness.

New Monitoring Capabilities: the Datacam

Since all traffic in an enterprise traverses over local area networks, the natural question is why not place a passive probe on the network and capture everything? From a technological perspective, the capability to do just this exists:

1. Network Interface Cards (NIC) running in promiscuous mode have been used since the 1980s primarily for network control capabilities.
2. Server speed (bus and processor) is no longer a bottleneck for accepting multi-Mbps streams.
3. Low cost processors can be cost effectively equipped with the memory necessary for caching real time multi-Mbps flows.
4. The price and capabilities of storage (magnetic or optical) are no longer a barrier for capturing massive amounts of data.

The real question is what to do with such large amounts of raw information if it were collected? The answer is re-segmentation and logical storage for easy query and analysis by information security analysts.

In effect, the monitoring capability must perform re-segmentation functions of not only all protocol layers, but also the actual application. This is a tall order because there might be thousands of different transactions traversing the network among tens of different servers, and possibly thousands of different users. However, this can be done in the following steps:

1. Read all asynchronous datalink layer frames or cells traversing a network (e.g. Ethernet, Token Ring, ATM)
2. De-encapsulate each frame capturing the datagram, revealing such information as the source/destination IP addresses.
3. De-encapsulate each datagram capturing TCP/UDP segments, revealing TCP/UDP source/destination socket addresses.
4. De-encapsulate each segment capturing application data, and determine the application type (such as emails with attachments, TELNET sessions, FTP, etc.)
5. Associate application data units of the same application transaction, reconstructing the session and data exchanged.
6. After completing a synthesis of the transactions, store the results along with such information as user (or hacker/cracker if known), date/times and IP addresses.

The transactions can now be analyzed (real time by an algorithm or by a security analyst who was alerted by the tool or an external factor such as an employee separation). This is an extraordinary capability given that the networks might be running 100 Mbps Ethernet or ATM at

OC-3. Remarkably, these capabilities have been rapidly evolving for the last three years, but have not gained widespread acceptance or penetration in organization IT infrastructures. The analogy for such a capability might be a Videocam in a bank, so here we coin the capability as “Datacam”.

Examples of Datacam Capability

Four commercially available “existence proofs” of Datacam capabilities are identified and briefly discussed here:

1. FBI’s “Carnivore”
2. Raytheon’s “Silent Runner™,”
3. NIKSUN’s “NetVCR™”
4. CTX’s “NetWitness™,”

The FBI’s Carnivore capability has received a lot of publicity, most of it negative. The tool probably operates in the general fashion outlined above, with an important caveat. The tool apparently provides filtering, permanently capturing only the transactions of a particular target. This is effectively a Title III court-ordered wiretap. Privacy organizations and civil libertarians have been withering in their criticism of Carnivore because of what they see as potential for abuse by law enforcement officers. Critics do not seem to question whether Carnivore is a useful and effective tool for lawful use by law enforcement, but rather what safeguards (procedural and technological) exist to prevent abuse by law enforcement. Carnivore also can operate in a “pen” mode where it collects only transactional data about the network – recording network transactions and certain (e-mail and web) application data. (www.epic.org/privacy/carnivore)

Silent Runner™ is sold commercially by Raytheon, apparently from a shrink-wrap product sale approach, and appears geared to highly specialized and trained information security analyst. Silent Runner™ collects all of the data on a network and provides statistical insight to its composition as well as two additional tools – Link Analysis and n-gram clustering of the raw content of the datagrams. Further information regarding Silent Runner™ can be found at its website (www.silentrunner.com).

NetVCR™, sold by NIKSUN, is an appliance capable of recording activity on networks operating in excess of 100Mbps. It uses a modified LINUX operating system and libpcap (the basis for the tcpdump sniffer). NetVCR™ is capable of storing up to 1 TeraByte of raw traffic in its appliance and offers limited analytical tools to conduct forensics. Further information regarding NetVCR™ can be found at its website (www.niksun.com).

NetWitness™ is sold by CTX Corporation’s Forensics Explorers division, also as shrink-wrap tool. NetWitness™ concentrates on business analysis capabilities, and is geared towards typical information security users. NetWitness is the only product that produces log data about the majority of protocols (layer 3 and up) seen on a network and provides the tools for analyzing these logs. Further information regarding NetWitness™ can be found on CTX’s website (www.forensicexplorers.com).

Barriers for Use

It is widely accepted in the US that since employers own their information systems, employees should have no expectation for privacy regarding their usage of these systems. Favorable Federal Court rulings have established this precedent, based upon the 1986 Electronic Communications Privacy Act:

“Under the 1986 law, a network operator can intercept or disclose a user’s message ‘in the normal course of his employment’ to protect the rights and property of the network’s owner – even without giving a warning, though experts frequently advise companies to do so.”¹

However, some businesses may be reluctant to do so, examples of which are:

1. Some business managers are squeamish about “spying” on their employees, or concerned about abuse of the information collected
2. As a result of Microsoft’s email use as a primary evidentiary source in its antitrust case, some businesses are permanently purging email after say 30 or 60 days.

With respect to squeamishness, executives must be presented with facts regarding the detected frequency and magnitude of financial, intellectual property, and trade secret theft. For example, according to the American Society for Industrial Security:

“..regarding intellectual property loss, potential known losses to all American industry could amount to as much as \$63 billion, with current losses occurring at a rate of \$2 billion a month. The high-tech industry has an average loss per incident reported of \$19 million”²

With respect to destroying information for fear of legal liability, the executive must be educated as to value of archival information in determining the amount of loss sustained, detecting the means of the thefts, attributing theft to outsiders or insiders, and finding those responsible. The executive must weigh the threat of lawsuit against the threat of losing valuable information or property, possibly without knowing it. Without archival information, organizations will be left wondering what else was stolen if they do catch a perpetrator. Also, if industry hides such events because of fear of publicity, it will only create other victims.

Conclusion

New powerful network and information system security monitoring and archiving tools are available and rapidly evolving. So far, market penetration has been minimal. The key to using such systems for more effective insider and outsider monitoring would seem to be executive and employee education. First, the threat must be understood, and second, important privacy concerns must be addressed. Most people have no problem with a VideoCam in the bank, in department stores, or at the entrance of a business. After all, the large majorities of people are honest and do not engage in crime. However, almost everyone would object to VideoCams in restrooms or locker rooms. Education as to need for analogous capabilities in information systems and management sensitivity to valid privacy safeguards are in order, if these new capabilities are to join in the struggle against Cybercrime. Without them, we will be left to wonder about the threat of an undetected enemy within the gates.

¹ “Judges’ Ire Stirs Debate on Web Monitoring”, Wall Street Journal, August 8, 2001

² Neil Gallagher, Deputy Assistant Director, Criminal Division, Federal Bureau of Investigation, “Cybercrime, Transnational Crime, and Intellectual Property”, Statement for the Record before the Congressional Joint Economic Committee, Washington, D.C., March 24, 1998.