ASSESSING AND COMBATING THE SNIFFER THREAT

E. Eugene Schultz

INSIDE

The Nature of the Threat; How Sniffers Work; Types of Sniffers; The Concern Extent of the Problem; Case Studies; Solutions; Policy; Encryption, Employ One-Time Password Authentication; Use Secure Ethernet Technology; Implement Secure E-mail; Educate Users; Responding to Sniffer-Related Incidents

INTRODUCTION

To say that determining the real origins and magnitudes of threat is one of the most challenging problems facing information security (InfoSec) professionals is a gross understatement. The media, net news, and a myriad of other sources constantly remind us just how diverse the range of potential threats is. Internet security, intranet and extranet security, operating system-based security, information warfare, personnel security, and other important topics have all at one time or another received a disproportionate amount of attention in the 1990s, forcing InfoSec professionals to deal with these issues more than with many other competing issues. Addressing these issues is a sound strategy, but the proverbial winds of hype continually shift. All things considered, deciding what the real, relevant sources of InfoSec threat are, then assessing the resulting risk, and, finally, planning how to effectively control that risk have become more difficult than ever.

The inevitable result of all this justified attention on these diverse, sometimes sensational sources of InfoSec-related threat has been diminished attention to less dramatic, more seemingly routine sources of threat. One such source, the focus of this article, is network snooping or sniffing in which network traffic is captured without authorization. Although most InfoSec professionals understand that such a threat exists, it is easy to fall into the trap of thinking that somehow the magnitude of

PAYOFF IDEA

The greatest potential loss due to unauthorized access to systems results from the use of unauthorized sniffers. The nature of the threat is discussed in terms of how sniffers work and the types of sniffers. The countermeasures to this increasingly challenging threat are described in detail.

Auerbach Publications

this threat pales compared to the other, more exciting sources of threat. An organization is likely to have provisions in an InfoSec policy that prohibit the use of sniffers without proper authorization and that may even require periodic inspections to determine whether unauthorized sniffers exist. Furthermore, unless one works in a unit whose responsibilities include networking, one is not likely to be aware of the extent to which sniffers are deployed and exactly who has access to the data that sniffers capture. Of all the sources of potential loss due to unauthorized access to systems, illegal data transfers, etc., however, none is greater in most operational environments than the deployment of unauthorized sniffers. This article explores the nature of the sniffer threat, presents solutions for combating the risk, and suggests strategies for dealing with sniffer-related incidents should they occur.

THE NATURE OF THE THREAT

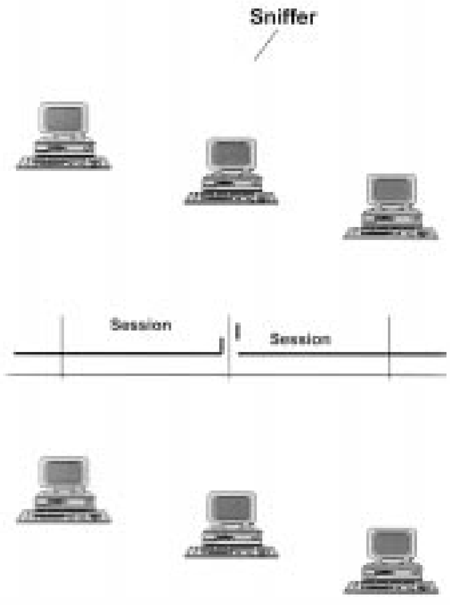
How Sniffers Work

To understand the threat that sniffers present first requires understanding how sniffers work. The manner in which sniffers operate depends on the type of network. In a shared media network such as a standard Ethernet, packets sent along a network segment travel everywhere along the wire. Any host connected to a segment is capable of capturing all sessions within that segment. For example, Exhibit 1 depicts a sniffer-capable host. It is able to capture any traffic that goes through the network segment, regardless of the particular neighboring host or other remote host to which that traffic is destined. In other types of networks (e.g., token-ring networks), sniffers are capable only of capturing sessions sent to or through a specific device or host, that is, either the physical sniffer itself or the host that houses a logical sniffer. Exhibit 2 depicts this scenario in a token-ring environment. Note that only the traffic traversing the side on which the sniffer is located can be captured by the sniffer.

Types of Sniffers

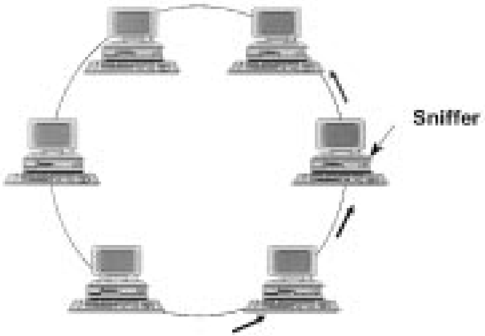
The two types of sniffers are physical sniffers and logical sniffers. Physical sniffers are devices with built-in network interface hardware such that when they are installed on a network, they record all traffic. Logical sniffers are programs that run on host machines that also capture data traversing a network. In order for logical sniffers to function, the host machines that house them must have a network interface card that not only provides a physical interface to the network, but also provides packet capture functionality. This type of interface card, commonly known as a promiscuous network interface card, is built into some off-the-shelf systems, but must be installed in others.

EXHIBIT 1 — A Sniffer in a Shared Media Network



Two types of promiscuous network interface cards exist. One can monitor all traffic going across a network segment. The other is capable only of capturing the traffic bound for or going through the host on which it is installed.

EXHIBIT 2 — A Sniffer in a Token-Ring Network



The Concern

Why do unauthorized sniffers pose such a high degree of threat? When in the hands of legitimate network administrators and other technical personnel, sniffers are an immensely valuable tool; sniffers help substantially in diagnosing and fixing networking problems (such as broadcast floods and locating points in a network in which traffic flow is disrupted). When in the hands of unauthorized persons, however, sniffers are a potential security-related catastrophe waiting to happen because:

1. Many logins across networks in typical operational environments involve transmission of cleartext passwords. An intruder with access to a sniffer can quickly learn the login names, passwords, and IP addresses of host machines on which login accounts exist by examining the first portion (the "header") of each log-in packet. The intruder can then establish a telnet or a similar connection to that host and attempt to log in. Unless captured passwords are obsolete (because, for example, the user whose password has been captured recently changed the password), the probability of the intruder's success in breaking into legitimate user's accounts is very high. Once the intruder breaks into an account, the intruder will have the access rights of the user whose account is now compromised, leading to the possibility of reading and copying files to which the user has access. Worse yet, the intruder now has a foothold (namely, user-level access) within a system and can attempt to use cracking tools and other methods that provide superuser access on this system. With superuser access, the attacker is able to read and copy any file stored on that system, and is in addition very likely to find attacking other machines with the network considerably easier.[1]
2. Data (including text within e-mail messages) is constantly sent from host to host within a typical network; sniffers can capture this data. If the data is not encrypted, unauthorized persons can read and copy the data. A reasonably high proportion of transmitted data in typical corporate network environments is business critical. The compromise of data such as information about pending patents, original engineering data, marketing and lease bid data, and other information can result in immeasurable loss if in the hands of a competitor or other potentially hostile party. Consider also that this type of data compromise may not directly result in direct financial loss — a competitor may obtain critical information but not use it. The media may, however, learn of the incident involving data compromise or some other negative outcome, and then release stories that can damage an organization's image. The result may be substantial indirect loss through outcomes such as lowering customer confidence in products and services offered by that organization, stockholder lawsuits, etc.

EXTENT OF THE PROBLEM

The full extent of unauthorized deployment of sniffers is (like so many other types of InfoSec-related problems) unlikely to be known or even reasonably estimated. The meaning of “unauthorized deployment” is in fact ambiguous at best; an intruder can, for example, gain access to a legitimately installed sniffer. Whereas the installer and others may have legitimate access, someone else’s access to that sniffer may be unauthorized. In addition, sniffers for the most part are by nature clandestine — discovering them requires additional analysis and work that many organizations neglect. Despite complications such as these, data about deployment of unauthorized sniffers is available. The following two case studies exemplify the range of incidents that can occur as a result of unauthorized sniffers.

Case Study 1: Outbreak of Sniffer Attacks on the Internet

A widespread series of sniffer-based attacks on the Internet occurred between 1993 and 1995.[2] Attackers initially broke into host machines using automated attack scripts widely available over the Net, then exploited other vulnerabilities to gain superuser access using additional scripts. Superuser access allowed them to put unauthorized network sniffers in place. The intruders then connected to the hosts on which the logical sniffers were installed to gather log-in names and passwords, enabling them to break into additional hosts throughout the Internet. What was most noteworthy, however, was the fact that the intruders compromised hosts used by Internet service providers. These hosts were within subnets to which hub routers used in routing large volumes of Internet traffic were placed. In addition, these subnets had numerous leased line and dial-up connections. By placing sniffers on a host within the same network segment to which hub routers were connected, the attackers were able to capture all traffic that went in and out of the routers. Sniffers were often embedded in hacking toolkits that also removed indications of the intruders’ activities from system logs.[3]

These attacks were devastating in that an organization could have a relatively secure, sniffer-free network that nevertheless could be compromised because of sniffers outside the network. A single user simply had to log in remotely to a machine within the network from a machine outside the network. When the traffic passed through a compromised Internet service provider’s network, one or more sniffers captured passwords and other critical information. The practical significance is that sniffers within an organization’s networks are only part of the total sniffer threat; sniffers *outside* an organization’s network(s) can pose a significant security threat to that organization’s security.

Case Study 2: An Unauthorized Gateway-Based Sniffer in a Large Corporation

Several years ago, a technical staff member for a U.S.-based Fortune 100 company discovered an unauthorized physical sniffer. Unauthorized sniffers almost always spell trouble, but the location of this particular sniffer posed an especially high risk — -it was attached to a high throughput link to the Internet immediately before (i.e., outside of) a firewall that screened incoming traffic. Whoever had planted this sniffer had the ability to capture all traffic coming into and out of this business-critical network. Soon after the sniffer was discovered and removed, an investigation ensued. Investigators determined that it had been installed by an employee who was working in collusion with another outside person in a scheme to sell corporate information. The sniffer had been in place for approximately three months before it was discovered.

The moral of this story is that physical sniffers placed anywhere can cause catastrophic results. Sniffers placed at gateways to critical networks, however, can potentially cause the greatest loss because they can capture all traffic (inbound and outbound) through the gateways. Sniffers attached to a network's backbone also entail significantly elevated risk because so much traffic traverses through the backbone.

Which pose a greater overall threat — physical or logical sniffers? Although physical sniffers pose a serious threat, they are separate, identifiable hardware devices that can be seen by someone who is physically present. Additionally, someone who is physically present at a location where network cabling (to which a physical sniffer must be attached) is accessible must install them. Someone who installs an unauthorized sniffer might be observed and subsequently reported. Furthermore, physical sniffers tend to be somewhat (but not prohibitively) expensive, making their purchase by the typical user somewhat unlikely. A more likely scenario, therefore, is unauthorized access to a physical sniffer purchased and installed legitimately by an organization, rather than the purchase and installation of such a device by a dishonest employee or contractor (although the latter possibility is nevertheless real and potentially catastrophic).

Logical sniffers in many respects comprise a more serious threat than physical sniffers. Many systems have built-in promiscuous interfaces; more commercial system administration tools than one might expect have built-in network traffic capture capabilities. Someone with access (authorized or unauthorized) to these tools could read or copy captured network traffic. Access to such tools is, however, not necessary; a perpetrator can simply gain remote access (in most cases, superuser access) to a target host, install a sniffing program, then wait until a sufficient amount of passwords or data is captured, and finally harvest the captured data. In many incidents, intruders have gone even further; they have replaced the entire kernel of a compromised system with a new, promiscuous kernel, thereby making discovery of the fact that the compromised system is now in promiscuous mode very difficult.[2]

For all practical purposes, however, the greatest threat associated with the use of logical sniffers is an everyday desktop user buying a promiscuous interface card and a sniffer program at a local computer store, then installing both on a desktop machine that connects to a corporate or other network. Commercial sniffer programs that run in environments such as DOS and Windows 95 now often cost less than $20. Sniffing in Macintosh environments is even easier; a sniffer program, Traffic Peek, is built into every Macintosh host. Windows NT 4.0 Server also offers a built-in logical sniffer, the Network Monitor (NM). Fortunately, access to this program is limited by default to administrators and also requires entry of a password.

In summary, the sniffer threat is indeed more serious than might superficially be apparent. Sniffers can be installed virtually anywhere network wires go.[4] Not only are there physical sniffers, but there are also logical sniffers, many of which can be installed by an average user without elevated privileges. In so many corporate, government, and academic environments around the world, passwords and data traverse networks in cleartext, making them perfect targets for sniffer attacks. Worse yet, only one sniffer installed in the proper location can capture a voluminous amount of data.

SOLUTIONS

The sniffer threat is insidious. It should come as no surprise, therefore, that choosing suitable control measures is by no means easy or straightforward. The following solutions are the best currently known solutions.

Policy. Policy is the basis for all effective InfoSec measures. The first and most essential step, therefore, in dealing with the sniffer threat is to ensure that one's InfoSec policy contains provisions that prohibit the installation or use of sniffers (physical or logical) on any system or network without the written approval of cognizant management. Cognizant management may possibly include line management, business unit managers, InfoSec management, or some other management function. This policy should also specify who (employees only, employees and contractors, etc.) is allowed to install sniffers and read sniffer data; include provisions for protecting sniffer data from unauthorized disclosure; and specify consequences in case someone does not adhere to it.

Encryption. The most powerful, single technical solution to the sniffer threat is the widespread deployment of network encryption. Encryption forces those who deploy sniffers without authorization to be capable of breaking the encryption to read the contents of captured packets. Tragically, the major question with respect to deployment of encryption too often centers on the strength of encryption (e.g., 40-bit versus 128-bit encryption). The result is that encryption solutions are postponed, leaving systems and data at risk. Some encryption (no matter how weak) is better than none. Relaxation of United States encryption export policies makes implementing some kind of network encryption feasible in nearly every country.[5]

Implementing virtual private networks (VPNs) is an increasingly popular method of achieving encrypted network traffic flow. Sessions between hosts can be encrypted using either private or public key encryption, thereby establishing a secure "tunnel" between them. VPNs between firewalls or routers are now used routinely in corporate intranets and in other critical network deployments. Although VPNs are generally effective in controlling the sniffer threat, the type of VPN deployed makes a significant difference in the overall effectiveness. VPNs that provide link encryption (as from one firewall to another) are not so effective in that transmissions are sent in cleartext everywhere but between the hosts that provide the link encryption (see Exhibit 3).

In contrast, VPNs that provide point-to-point (also known as end-to-end) encryption are more effective in that network transmissions are encrypted over every part of the route they traverse (see Exhibit 4).

Additionally, a problem common to both types of VPNs is that some vendors have deviated from the mainstream by developing their own, proprietary Point-to-Point Tunneling Protocols (PPTP — the protocol that provides the encrypted sessions). Consequently, two hosts that support different implementations of PPTP cannot establish a secure tunnel.

Employ One-Time Password Authentication. In one-time password schemes, a password for a user is sent across the network once, and then changed the next time a password for that user is transmitted. Several dif-

EXHIBIT 3 — A VPN with Link Encryption Between Firewalls

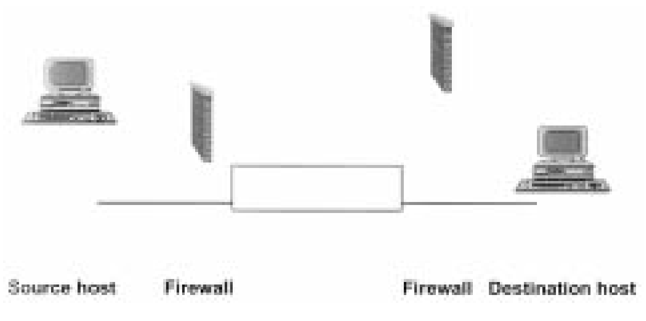
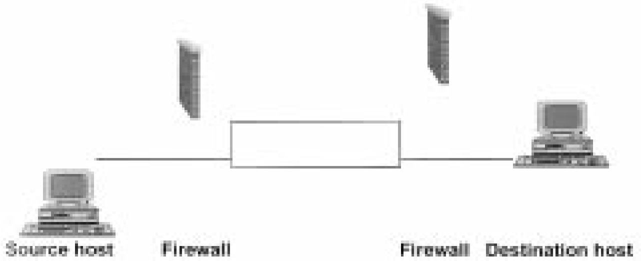


EXHIBIT 4 — A VPN with End-to-End Encryption



ferent one-time password programs exist, but one of the most effective versions is Bellcore's commercial S/KEY tool. S/KEY allows the user to choose a particular password for a given number of log-ins, but never allows a cleartext password to be sent over the network. Instead, it encrypts every password transmission. Better yet, it encrypts each password differently[6] during each log-in attempt. Even if a sniffer captures passwords, the passwords will be encrypted. The encrypted versions will be very difficult to crack because no two cyphertext passwords sent over the network will be identical.

Use Secure Ethernet Technology. As mentioned previously, standard Ethernets are shared media networks. As such, they are ideal for perpetrators of sniffer attacks. Fortunately, a relatively new development — the secure Ethernet — limits the distribution of data sent over a network. Secure Ethernets send data only to the host that each packet header indicates is the destination host. In a secure Ethernet, an attacker would have to plant a sniffer on every host within a network segment to capture all sessions. The major limitation of secure Ethernet technology is that it works only locally; once network transmissions are sent outside of the local network in which this technology is implemented, the traffic may be subject to sniffer attacks if the destination networks have not implemented secure Ethernets. Still, secure Ethernet technology offers substantial improvement in ability to defend against the sniffer threat.

Have System Administrators Regularly Inspect Hosts for Unauthorized Logical Sniffers. In particular, have them look within gateways — -routers are often the hosts on which logical (as well as physical) sniffers are installed without authorization because such a large volume of traffic generally goes through routers. Logical sniffers are often installed in public directories (including temporary directories) where anyone can add files and where the sheer number of files can make finding the executable and data files for the sniffer unlikely. Using integrity checking tools such as Tripwire (for UNIX hosts) can be helpful in identifying changes to existing files if someone replaces a legitimate file with a sniffer executable. Other clues that unauthorized logical sniffers may be in place are the presence of hidden files (such as . files in UNIX hosts and $ files in Windows NT hosts), often with unfamiliar names such as ., .., .X, or others. A well-known logical sniffer program in the UNIX arena is named "rootkt," although an attacker is likely to change this name to some name that is not so easily recognized. Entries in audit logs may show that a sniffer has been installed; similarly, checking for current processes that are running on each system may reveal the presence of unknown processes that capture network or host sessions. Scanning programs such as CPM (Check for Network Interfaces in Promiscuous Mode[7]) are useful in that they can be run on Sun Microsystems hosts to determine whether they are in packet-capturing mode. Remember, however, that measures such as these help only with respect to the sniffer threat in local networks.

Frequently Inspect for Unauthorized Physical Sniffers. These sniffers can sometimes be very easy to detect. The fact that a desktop computer bearing a well-known sniffer manufacturer's name, such as Network General, is attached to the network is, for example, a dead give-away that the computer is a sniffer. The presence of a hardware device that connects to a network cable via a vampire clamp — a type of interface that penetrates the cable's insulation where the clamp is attached — is a high probability indicator of the presence of an unauthorized physical sniffer. The most significant problems in discovering unauthorized physical sniffers are that homemade sniffer devices may not be so easily recognizable and also that sniffers can be hidden in difficult-to-access locations such as wiring closets and subflooring.

Implement Secure E-mail. Secure e-mail programs can protect the privacy of e-mail messages by encrypting the contents. Both commercial and freeware programs of this nature are widely available. As mentioned previously, United States encryption export restrictions have recently been relaxed sufficiently to allow sufficiently strong encryption throughout the world.

Prepare for and Plan to Use the IPv6 Protocol. This emerging protocol consists of an authenticating header (AH) and encrypted session payload (ESP). The ESP portion keeps cleartext data from being transmitted over networks, making data safe from sniffers. IPv6 is currently an emerging technology; however, to use this technology requires that network applications be programmed to utilize it. As a real solution to the sniffer threat, therefore, this technology is still several years away. Nevertheless, initiating efforts to investigate and utilize IPv6 as soon as possible is an excellent strategy for dealing not only with the sniffer threat, but also a wide range of other threats.

Employ Third-Party Authentication. This type of authentication requires users to authenticate to an authentication server (usually through presenting some kind of token such as a smart card), then to authenticate using the normal system authentication procedures (namely by entering a log-in name and password). With third-party authentication, even if a perpetrator captures a user's cleartext password and attempts to log in using it, the log-in attempt will fail because the perpetrator will not possess the necessary token. As strong as this measure is, unfortunately, it provides only a partial solution to the sniffer threat in that it protects against password sniffing, but does not protect data transmitted over the network.

Educate Users. Educates users about the sniffer threat and help them understand the policy the organization has in place concerning sniffers. The education and awareness effort should enable them to recognize and report illegal sniffers through proper channels. This effort can go a long way in the battle to combat unauthorized sniffers. The time and resources spent in training system and network administrators usually also have great benefits; the "gung-ho" administrator who installs sniffers with good intention but without proper authorization is in many respects the greatest source of danger.

RESPONDING TO SNIFFER-RELATED INCIDENTS

Schultz and Wack[8] maintain that responding to incidents requires six distinct phases of activity, including:

- preparation
- detection
- containment
- eradication
- recovery
- follow-up

Of these stages, detection and containment are usually the most critical in a sniffer-related incident. Detection is critical because, as mentioned earlier, any system within a network can be capturing packets without anyone's knowledge other than the person who installed it. Additionally, sniffer incidents are often extremely difficult to contain. As in Case Study 2 above, a sniffer may be running for months before it is finally detected. By the time the sniffer is found, it may have captured tens of thousands or more cleartext passwords to systems that are now subject to immediate, unauthorized access.

If an unauthorized sniffer is discovered, the first thing one should do, if at all possible, is to perform a full backup of the system on which the sniffer runs. The backup will serve as evidence in case the organization initiates prosecution of the perpetrator(s). Additionally, by including all the sniffer's executables and data files, the backup may be useful in determining how the sniffer works, what data the sniffer has captured already, and (if one is lucky) clues concerning the identity of the person(s) who have written and installed the sniffer.[9] If the sniffer is a logical sniffer, one may be able to inspect the code to determine the file(s) to which the sniffer is writing data. Inspecting log-in IDs and passwords in such files will allow one to know which accounts in which systems are most likely to have been compromised. Have the system administrators of these systems inspect logs, log-in messages, etc. to determine whether these systems have been accessed without authorization; then take any necessary evasive measures (including, if circumstances warrant, initiating system shutdown procedures) to protect these systems and the data they store. Be sure at this point to also delete any sniffer-related files within any compromised system to prevent them from being accessed and used by others.

If an unauthorized physical sniffer is discovered, handle this device as you would any other piece of physical evidence.[10] Fingerprints on the sniffer device may enable law enforcement personnel to identify the perpetrator; be sure, therefore, to have someone who is an expert in computer forensics or law enforcement be in charge of evidence handling. As in the case of logical sniffers, inspecting the output of a physical sniffer may also enable one to determine the accounts and systems that are currently most at risk.

The next step is also an extremely important one. One should now initiate an effort to change all passwords on all hosts within any network on which a sniffer has been found or through which remote log-in traffic has passed. Although the user community is likely to be less than enthusiastic about this measure, it is the only logical course of action. One sniffer may have captured passwords for any other host in the entire network, allowing the perpetrator(s) easy and immediate access. Changing all passwords is the only way to be sure that any passwords that any perpetrators have "stockpiled" are now invalid and useless.

Performing incident response procedures correctly for sniffer-related incidents may not be as easy as it seems. Consider the following case study.

Case Study 3: A Lesson Learned in Responding to a Sniffer Incident

During the massive outbreak of Internet sniffers from 1993 to 1995, a member of a national emergency response team traveled to a site in which several unauthorized logical sniffers were found. After analyzing the problem, this investigator deleted the sniffer programs, then logged in remotely as root (superuser) to a system at the site from which this team operated. Shortly afterward, this system — in addition to scores of others at the response team's site — was compromised. The investigator did not realize that additional, as yet undiscovered sniffers had been installed at the site at which the investigation was being performed. The root password to the investigator's system was transmitted in cleartext across a network segment in which an undiscovered sniffer had been installed. A perpetrator harvested this password, broke into the investigator's system as root, and planted still another sniffer on this system. This enabled the perpetrator to gather many passwords for machines at the investigator's site (in addition to a number of additional sites). The lesson learned from this series of unfortunate events is that sniffer attacks are not as easy to handle as one might suspect. One mistake, such as the one discussed in this case study, can proliferate these incidents out of control. Although the speed of response is critical, it is most important to carefully think through every step and action to avoid making the situation worse. This "lesson learned" is particularly applicable to organizations with many intranet and extranet connections.[11]

Finally, one should engage in a follow-up process to determine how the sniffer-related incident occurred and what measures (e.g., scanning hosts more frequently to see if they are in promiscuous mode) might have made the occurrence of such an incident less likely. One should also evaluate the response to the sniffer incident, identifying steps that could have been performed more efficiently and additional resources that would have been useful. One should revise incident handling procedures accordingly and, finally, write a report on the incident for future reference.

CONCLUSION

The threat of unauthorized sniffers has long been recognized in the InfoSec community. Amid all the confusion generated by the news of new, more sensational threats, it is easy to overlook the sniffer threat. Overlooking the sniffer threat is a major mistake; in many respects, a well-placed, unauthorized sniffer could easily result in more loss and disruption to an organization than any other type of incident. The proliferation of logical sniffers on many platforms represents a serious escalation in the sniffer threat. Network attackers cannot only install sniffers on remote hosts, but even the most casual, inexperienced user can now buy an inexpensive logical sniffer and install it on a desktop machine to capture critical data and passwords transmitted across network segments.

Many potential control measures for unauthorized sniffers exist. These include getting the appropriate policy provisions in place, encrypting network transmissions, using one-time passwords, implementing secure

Ethernet technology, regularly inspecting for both logical and physical sniffers, installing secure e-mail, implementing network applications that utilize the IPv6 protocol, using third-party authentication, and establishing an effective user education and awareness program that helps both users and system administrators understand and combat the sniffer threat. The appropriate subset of these measures depends on the particular business and other needs of the organization. However, ensuring that an appropriate policy exists is imperative, no matter what other measures are appropriate. Encryption is the best (although not necessarily the most feasible) technical solution. Additionally, the potential for a widespread outbreak of sniffer attacks dictates that an effective incident response program that includes the appropriate procedures for combating sniffer attacks be put in place.

Notes

[1] Many system administrators set up trusted access mechanisms that allow them to easily move from one machine to the other in a network without having to authenticate themselves to each machine. These mechanisms often require that those who use them have superuser privileges on the machine from which trusted access is initiated. Although advantageous from the perspective of convenient access for system administrators, a perpetrator who gains superuser status in a single machine may also be able to exploit these mechanisms to gain unauthorized access to many other systems within the same network.

[2] Schultz, E.E. and Longstaff, T.A. (1998). Internet Sniffer Attacks. In D.E. Denning and P.J. Denning (Eds.), *Internet Besieged*. Reading, MA: Addison-Wesley, p. 137–146.

[3] Van Wyk, K.R. (1994). Threats to DoD Computer Systems. Paper presented at *23rd International Information Integrity Institute Forum* (cited with author's permission).

[4] Sniffers could also, in fact, be used to attack wireless networks if they are planted in any host connected to such networks.

[5] Laws within countries such as France and Russia restrict the use of encryption within these countries.

[6] The change in encryption is the same for both the sending and receiving host, so authentication is not disrupted.

[7] Available from ftp.cert.org and other ftp and Web sites.

[8] Schultz, E.E. and Wack, J. (1996). Responding to Information Security Incidents. In M. Krause & H.F. Tipton (Eds.), *Handbook of Information Security Management: 1996–97 Yearbook*. Boston: Auerbach, p. S-53–S-68.

[9] Authors of a sniffer tool will, for instance, write the sniffer code in a manner that manifests a particular style of programming. Software forensics experts may accordingly be able to identify the authors. In addition, the code may contain Internet addresses and other information that may enable investigators to determine the identity of any perpetrator(s).

[10] Bernstein, T., Bhimini, A., Schultz, E.E., and Siegel, C. (1996). *Internet Security for Business*. New York: John Wiley & Sons.

[11] An intranet is, for the purposes of this article, considered a group of internal networks that connect with each other. An extranet is a group of external networks that are linked together.

E. Eugene Schultz is a program manager at SRI Consultants in Menlo Park, CA.