Simplicity and Awareness – Keys to Network Security

a report by
Richard Bejtlich

Senior Engineer, Managed Network Security Operations, Ball Aerospace & Technologies Corporation

Richard Bejtlich is a senior engineer, responsible for the Managed Network Security Operations at Ball Aerospace & Technologies Corporation. He runs the network security operations, process development, incident response and technical training. He began his computer security career as a captain in the Air Force in late 1998. He served as the Chief of Current Operations at the Air Force Computer Emergency Response Team (AFCERT), supervising a 60-person global network security monitoring unit. He has published several papers, such as *Interpreting Network Traffic: A Network Intrusion Detector's Look at Suspicious Events* and *Network Intrusion Detection of Third Party Effects*. Mr Bejtlich is a 1996 graduate of Harvard University and a 1994 graduate of the US Air Force Academy.

Few people believe that maintaining a sound network security posture is easy. Those who do are deluding themselves, unless they practice two fundamental tenets of security: simplicity and awareness. Simplicity facilitates abstraction, which is the basis of all computing. Abstraction is the ability to imagine and evaluate processes and data with no equivalent in the physical world. Awareness is an augmentation to abstraction, giving a better idea of exactly what processes and communications must be manipulated mentally. For example, a company must be aware of users from Hungary mounting drives remotely on its file server. This may violate its security policy. Unfortunately, the modern networking environment is destroying both simplicity and awareness. The purpose of this article is to explain how security professionals can deal with this hostile situation.

Simplicity takes many forms. In one sense, a home user operating a single machine with dial-up Internet access has a simple security task. He or she must protect the computer from exploitation. Nevertheless, many home users are not equipped to recognise the vulnerabilities that are present in the default configuration of their personal computers. A simple case of defending a single computer has been made complex by the obscurity of that machine's operating system (OS).

Uniplexed Information and Computer System (UNIX)-based OSs, with their general reliance on text-based configuration files, give greater transparency to knowledgeable users. It is simple to eliminate services that are started by the inetd daemon. The inner workings of Windows OSs, despite their 'friendly' graphical environment, can be more difficult to decipher. Terminating some dangerous services in Windows NT requires unbinding protocols, modifying the registry and altering object properties. Sadly, the majority of home users run opaque Windows platforms, largely negating their initial simplicity advantage.

Beyond home users, corporate networkers defy simplicity at every turn. The home office paradigm of a single machine with a single OS is shattered. Many corporations run dozens to hundreds or thousands of machines, with a variety of functions being performed by multiple OSs. Small businesses might run simultaneously Oracle databases on Solaris, Microsoft Office suites on Windows 2000, Sendmail mail agents on Red Hat Linux and Apache Web servers on FreeBSD. A single administrator may be responsible for every application, OS and platform.

Some argue that simplicity in small networks is served by running the same OS on every host. Homogeneous environments may be easier to maintain, but they suffer a dangerous flaw. If a crippling exploit was introduced, every machine would be at risk simultaneously. For example, the next Melissa virus will plague everyone who is running the same vulnerable configuration of Microsoft Outlook. An entire enterprise can be destroyed in the same way that a virus can slaughter a genetically identical species. Diversity, but not complexity, facilitates survival.

One strategy with which to establish a secure networking environment when simplicity is at risk is to reduce the number of workstations while balancing the risk of strict homogeneity carefully. Information appliances, such as Sun Microsystem's Sun Ray, provide computing power to users and centralised control to system administrators. Of course, the malicious insider may find it easy to access an entire office's files from within a single compromised Solaris Enterprise server. While useful within the boundaries of the corporate network, this appliance deployment tactic does not reduce the threat to systems with Internet exposure.

Systems that are at risk from external threats reside in demilitarised zones or 'perimeter networks', acting as external routers, firewalls and e-mail, Web and domain name servers. Some vendors do offer this functionality in appliance form, promising 'hardened' configurations with specialised settings. Often, these devices are endangered by the same lack of transparency as the inner workings of Microsoft platforms.

As it is safe to assume that the obsessive, incredibly skilled attacker is intimately familiar with the design

of his or her target's defensive systems, any obscurity harms the security professional. Since the very nature of pure hacking is learning every detail of a system's operation, openness is the best way to counteract the skilled adversary's knowledge of closed systems. However, transparency compensates for complexity only to a certain extent. Other measures must be taken.

Awareness is the best way to promote security in a complex environment. Cultivating awareness is not easy, as complexity can make gathering critical information difficult. Managing the flood of vendor bulletins, computer emergency response team advisories and security mailing list postings can be a full-time job. In addition, an insidious aspect of the awareness principal makes matters worse. For example, there is the problem of being aware of – and defending against – a vulnerability in a local server if the existence of the server is unknown. It is difficult for system administrators to maintain complete and current network maps, and to prevent others from bringing new systems online.

of network protocols, and especially the growth of protocols within protocols, makes recognition increasingly challenging. Decoding raw Microsoft's NetBIOS/Server Message Block traffic, even with the aid of analysis software such as Ethereal, is difficult. Recognising Simple Object Access Protocol (SOAP) riding through Hyper Text Transfer Protocol (HTTP) is not any easier. No less important is the increasing use of encryption across enterprise boundaries. While encryption can deny intruders access to transmitted data, it can also mask attackers who tunnel their activities through legitimate encrypted channels. Foundstone began demonstrating these techniques publicly about two years ago, compromising Web servers while hiding within Secure Sockets Layer (SSL) traffic.

A way in which to best serve the three elements of awareness must be identified. The first and second elements, awareness of the existence of hosts and their services, are met by two strategies. First, system and network administrators can keep careful

It is vital to remember that security itself cannot be 'outsourced'. Rather, tasks that contribute to enhanced security can be outsourced. Security professionals should seek to implement as much simplicity and awareness as their positions allow.

From a network security perspective, awareness takes several forms. First, there must be an awareness of the workstations and servers that are active in the enterprise. When confronting external threats, there are concerns about servers with direct exposure to the Internet. Typical enterprises supply multiple public targets: external routers and firewalls, as well as e-mail, Web and domain name servers that offer suitable exposure.

Second, the services that are offered by these systems must be known. Improperly configured or 'unhardened' servers may give attackers vectors with which to exploit systems that are unrelated to the target's main purpose. For example, an e-mail server may afford access to its line printer daemon, inviting exploitation of a service that is not required for transmitting e-mail.

Third, the traffic that is traversing the enterprise network boundary must be observed, recognised and understood. This point, and especially the recognition element, is crucial. The proliferation

inventory of their assets. Network discovery and logging tools that are configured properly will help. Second, and more significantly, administrators can hire outside help. This assistance takes three forms:

1. auditing;
2. vulnerability assessment; and
3. penetration testing.

Auditing is the process of measuring an enterprise's compliance with its security policy. Vulnerability assessment is the process of examining computing assets for configuration and operational weaknesses that could result in a loss of confidentiality or integrity/availability. Penetration testing is the next step beyond vulnerability assessment. It is the active exploitation of vulnerable assets to determine the likely extent of a successful enterprise intrusion. Typical penetration tests will result in multiple compromised machines, each leveraged to gain deeper access in accordance with the rules of engagement that are set by the client enterprise.

'Outside help', a form of 'outsourcing', is standard practice in many fields that are unrelated to computing. In order to preserve and demonstrate the integrity of their finances, publicly traded companies must hire outside accountants to audit their books. Failure to perform this task properly has serious consequences. In June 2001, the accounting company Arthur Andersen paid US$7 million to settle federal charges after filing false and misleading audits of Waste Management Inc. During the last few years, hiring companies to provide auditing, vulnerability assessment and penetration testing has become a routine practice. Government regulation, such as the *Health Insurance Portability and Accountability Act 1996* (HIPAA) and the *Gramm-Leach-Bliley Act 1999* (GLB) are prodding medical and finance companies towards outsourcing these security tasks.

The third element of awareness is the observation, recognition and understanding of network activity. Experienced network engineers may have trouble with the subtle security-related aspects of suspicious traffic. In addition, the employment of multiple OSs, offering numerous services collectively, raises the stakes. If it is difficult to be skilled sufficiently in proper configuration of Windows, Linux, Solaris and FreeBSD platforms, it is harder to understand how each OS and application communicates with its peers. The straw that breaks the camel's back is the attacker's tendency to manipulate protocols and processes outside of their documented and expected forms.

The consequences of not observing, recognising and understanding network activity are plain: long-term, undetected and increasingly damaging compromises. As reported in July 2001 by Ned Stafford of www.newsbytes.com, Switzerland's third largest Internet service provider (ISP) discovered attackers had access to thousands of user names and passwords, including some for the embassies of France, Sweden and Israel. The perpetrators roamed SwissOnline for months, with the capability to read, alter, delete or copy e-mail at will. The infiltrators were only detected when they announced their presence by sending SwissOnline a CD-ROM containing 185,000 accounts and 250,000 e-mail addresses.

An increasingly accepted way in which to meet the challenge of detecting and reacting to suspicious network activity is managed network security monitoring (NSM). The analogue equivalent of this service, the manned security camera, is found in increasing numbers of banks, convenience stores, restaurants and other places of business. In addition, casinos require experienced observers to detect the most subtle of cheats. Similarly, well-equipped, managed NSM operations leverage their expertise for the benefit of all client enterprises. The best NSM providers offer expertise across multiple OSs and architectures, with knowledge of protocols and services and ways to defeat them. Managed NSM companies also offer early warning services within their field of view, which can far exceed that of each individual client. For example, if the NSM operation detects a new exploit in use against a client in Boston, it can ensure that its other clients prepare for probable attack.

For small to mid-sized enterprises, managed NSM operations are far cheaper to hire than the equivalent in-house capability. In a sense, hiring a managed NSM provider is similar to investing through mutual funds. Serious researching, purchasing and performance monitoring of stocks could be a full-time job for the individual investor. Alternatively, for a miniscule fee, individuals buy the expertise of a fund manager with a wide view of the investing landscape, and the time and skill to make informed financial decisions. Larger enterprises with numerous points of Internet presence and the resources to hire the dozen or so skilled professionals that are needed for constant staffing may elect to pass on managed NSM companies. Such large companies are similar to wealthy families who can afford to hire personal accountants, lawyers, tax advisors and investment assistants.

As the modern networking environment will only become more complex, security professionals must compensate for the lack of simplicity by seeking increased awareness. Since staying responsive to developments in applications, protocols and OSs is progressively more difficult, enterprises are recognising the need to employ specialists selectively to enhance their security posture.

In the same way that the division of labour has helped modern society to achieve greater prosperity and productivity, so outsourcing can further enhance security postures. It is vital to remember that security itself cannot be 'outsourced'. Rather, tasks that contribute to enhanced security can be outsourced. Security professionals should seek to implement as much simplicity and awareness as their positions allow.

While one focus of this article has been on the administrator's attentiveness to his or her enterprise's traffic, awareness should also be a required skill for users. The demystification of computing will undoubtedly continue as people who are born after the creation of the World Wide Web (WWW) reach the corporate workforce in the coming years. ■