Network Security: It’s Time to Take It Seriously

Let’s face it. Security is usually discarded when it contends with performance. But as the world becomes more tightly interconnected, organizations are feeling a greater need to rediscover network security.

Patrick W. Dowd
University of Maryland
Laboratory for Telecommunications Sciences

John T. McHenry
National Security Agency
Laboratory for Telecommunications Sciences

Network security is the most important thing on the planet.” We have heard these words uttered with great conviction many times. However, the first time it causes any inconvenience to system owners, administrators, or users, the same people hasten to add “except when it impacts performance, system complexity, or cost.” Let’s face it. Security is usually discarded when it contends with performance. The reason is simple, and at one time it may have even been valid: Performance directly contributes to the bottom line while security provides only indirect benefits. But as the world becomes more tightly interconnected, organizations are feeling a greater need to rediscover network security.

WHY BOTHER?

There are plenty of reasons. The massive surge of interest in the Internet, along with the emerging use of low-cost residential broadband networking for homes and small enterprises, has given rise to a concentrated study of network security practices. The explosive growth of networking technology continues to redefine the rules for maintaining the privacy and integrity of electronic data. There is a staggering amount of personal, commercial, governmental, and military information in the various networking infrastructures worldwide. This vast connectivity also poses monumental risks. Almost anyone can reach out to the network, which often means almost anyone can reach in. In short, network security is an issue that can no longer be postponed.

Fortunately, security measures do not have to be expensive or complicated—a reality the networking community has only recently taken to heart. Network security itself, however, must be better understood and embraced, preferably before a compromise occurs. The articles in this issue are intended to alert you to the risks and some solutions and to encourage you to develop and implement security methodologies and strategies before—rather than after—an incident.

ESTABLISHING A PLAN

A thread that spans most definitions of network security is the intent to consider the security of the network as a whole, rather than as an endpoint issue. A comprehensive network security plan must encompass all the elements that make up the network and provide five important services:

• Access. Provides users with the means to transmit and receive data to and from any network resources with which they are authorized to communicate.

• Confidentiality. Ensures that the information in the network remains private. This is typically accomplished through encryption.

• Authentication. Ensures that the sender of a message is who he claims to be.

• Integrity. Ensures that a message has not been modified in transit.

• Nonrepudiation. Ensures that the originator of the message cannot deny that he sent the message. This is useful for both commercial and legal reasons.

An effective plan is also built on a thorough understanding of security issues, including the potential attackers, the needed level of security, and the factors that make a network vulnerable to attack. This understanding helps you define the level of security that is appropriate for the information the network contains and the environment in which it operates.
Know your attackers

Before you can determine how much time and effort to spend on your security strategy, you must identify your potential attacker. Is it a 14-year-old looking for a moment of fame or a well-financed organization with specific economic objectives? Are you the only target or are you in a class of targets, such as banks? If the target is you specifically, protection will be more difficult, since one-on-one attackers are not often easily discouraged. If the objective is to attack a class of targets, you may need only enough security to motivate the attacker to move to another target in the class.

Determine the pain thresholds

You will need to estimate the threshold of pain you and your potential attackers are willing to tolerate—the threshold representing the resources you and your potential attackers are willing to commit. As a system owner, you need to know what you are protecting, what its value is to you, and what its potential value is to others. The statement “when you have nothing, you have nothing to lose” rarely applies to networks. Consider the world’s vast network infrastructure—personal information within homes, technical and marketing information on corporate systems, and political and military information on government systems. Clearly there is much to lose. Intellectual property is a valuable asset. The protection of marketing information, product announcements, and pricing plans is often crucial to a company’s financial success.

There are also more subtle consequences of an attack. Depending on the type of business, the subsequent publicity about the attack can cause both investors and consumers to lose confidence in the company. For example, customers may be reluctant to provide sensitive personal information to a company if they know its infrastructure has been successfully attacked. Such a loss may stall electronic commerce and other activities that require sensitive or private information.

Network security strategies, methods, and devices are used to raise the level of pain your opposition must endure to punch a hole in your system. It is impossible to ensure absolute security. You can ratchet up the level of effort an attacker will need to expend, but the amount of investment and level of defensive effort committed to security should be guided by the threat profile. You must understand this trade-off before your plan can incorporate the right balance between the level of security and the threat.

Understand the sources of risk

Probably the most common risk is a poorly administered system. System administrators have ignored or disabled security features when the security product or facility implementing these features is complicated. System users often circumvent security procedures if the procedures degrade performance. In such cases, designers of the security strategy think the network is secure, but it has been fundamentally compromised because people are not following through with its implementation.

Social engineering is another common problem that leads to system vulnerabilities. It is not a technical assault on the network components, but a direct or indirect effort to learn about the characteristics and potential vulnerabilities of a system through social means: A person leans over your shoulder to observe your password, learns about a targeted system by...
Computer security devices may generate enormous logs for later analysis, but the analysis may be performed only when some specific problem is encountered. The logs may be deleted or trimmed before the data analysis is complete. Too little logging, too much logging, and too little analysis are still important problems.

Apathy is another source of risk. Network owners often do not take the business of providing network security seriously. They make excuses when it becomes inconvenient. It's "too hard" because of the administrative burden; it's "too expensive" because devices such as firewalls must be purchased and supported. Another popular excuse is "we don't have anything intellectual property within their systems generally fail to treat its security seriously.

SECURITY DEVICES AND MEASURES

Once you have shaped your network security plan, you can begin to incorporate the appropriate technology to provide a secure environment. Several items may be common to many plans, but not all the elements we describe here must be in place. What you use should be based on a thorough assessment of the risks present and your plan's objectives. Many security devices—from stand-alone products to protocols incorporated into network elements—have been developed. The brief description of firewalls and intrusion detection we offer is only a sample of popular devices.

Firewalls

Firewalls enforce an access policy by operating as a gateway between two networks. There are two major classes. Packet filter firewalls examine endpoint identifiers in datagrams passing through a link to determine if each packet should be allowed to proceed. For example, an IP packet filter can examine the source and destination IP addresses, the port being used, and the specified protocol field. Depending on the firewall's degree of sophistication, it might also...
maintain the state associated with each IP flow so that flows can be statistically analyzed.

Proxy firewalls act as a mediator between two devices attempting to communicate through the firewall. They terminate a flow at one side of the firewall, provide some proxy service to examine the data within the flow, and then re-create the flow in the network at the other side of the firewall. As an example, a telnet or ftp session from a network endpoint within a protected enclave to an external network element would be staged at the firewall as an intermediate flow.

Network intrusion detection

Network intrusion detection devices try to detect and call attention to odd and suspicious behavior. Anomaly detection devices use statistical methods to try to detect activity that deviates from normal behavior. These devices generate logs and alert system

Figure 1. How public-key cryptography works.
en. In similar ways, systems people may be at risk of being encouraged to provide access to their networks either through force, threats, or enrichment. Physical access to network elements must be protected, and access provided only to trusted people.

No system is absolutely secure. With a field so vast and vague, no one can anticipate all the possible breaches.

The goal of the network security articles in this issue is to give you a deeper understanding of the fundamentals of an effective network security plan must address. Cryptography, for example, provides the fundamental mechanisms for privacy, authentication, and integrity that are at the heart of most security plans. The sidebar “Simplified Example of Public-Key Cryptography” shows how this mechanism works. Communication protocols are also fundamental, enabling the current explosive growth in network connectivity.

The problems and solutions for both Internet and Web users are complex and still developing. Some of the articles we’ve included describe current problems and propose solutions. Others describe future challenges and the technology envisioned to meet them. We hope these articles will serve as an additional resource for those who are ready to take network security seriously. Our capacity to protect information worldwide will grow only when more network owners begin to plan for and consider these complex issues.

References

Patrick W. Dowd is an associate professor of electrical engineering at the University of Maryland, College Park, and a senior research scientist in the U.S. Department of Defense’s Advanced Networking Research Department. His research interests are in network security, high-speed networks, cluster-based computing, and mobile and optical communication. Dowd received a BS in electrical engineering and computer science from the State University of New York at Buffalo, and an MS and a PhD in electrical engineering from Syracuse University. He is on the editorial boards of International Journal in Computer Simulation and Cluster Computing and is an associate editor of SCS Transactions on Simulation and editor of the electronic journal Computer Simulation: Modeling and Analysis. He is a member of the IEEE and the ACM, is on the program committee of many IEEE and ACM networking conferences, and serves on the executive committee of ACM SIGCOM.

John T. McHenry is a senior electronic engineer with the National Security Agency, where his research interests include ATM networking, high-speed network firewalls, reconfigurable computing architectures, and FPGA design. He received a BS, an MS, and a PhD in electrical engineering from the Virginia Polytechnic Institute and State University. He is a member of the IEEE and serves on the program committee of the IEEE FPGAs for Custom Computing Machines (FCCM) Conference and the Reconﬁgurable Architecture Workshop, is a co-chair of the 1998 SPIE Conﬁgurable Computing Workshop, and is a participant in the DARPA Adaptive Computing Systems Program.

Contact Dowd at EE Dept., University of Maryland, College Park, MD 20742; p.dowd@ieee.org or McHenry at National Security Agency, US Dept. of Defense, Ft. Meade, MD 20755; mchenry@ieee.org.