Journal of
INDUSTRIAL
TECHNOLOGY

Volume 17, Number 1 - November 2000 to January 2001

Internet and Network Security

By Dr. James H. Yu & Mr. Tom K. Le

KEYWORD SEARCH

Administration
Internet
Legal Issues
Management

Reviewed Article

The Official Electronic Publication of the National Association of Industrial Technology • www.nait.org

Internet and Network Security

By Dr. James H. Yu & Mr. Tom K. Le

James H. Yu is a professor of Electronics and Computer Technology at San Jose State University. His current research includes microprocessor architecture, management information systems, computer networking and security, and electronics manufacturing technologies.

Tom K. Le is a technical account manager at Acclaim Technology in San Jose. He received his Bachelor of Science degree from University of California at Berkley. He has implemented numerous system network configurations, including network security measures for corporations and business.

Introduction

Although the history of the Internet is relatively short, its growth has been dynamically explosive. The number of Internet users worldwide has grown from 95 million to 130 million in 1998, and it is projected that there will be 350 million users in the year 2003 (eMarketer, 1998). The Internet is a worldwide collection of networks that links together millions of computers by various means, such as modems, fiber optic lines, routers, and servers. It provides connections to businesses, the government, industries, educational institutions, and individuals.

Each of these organizations has become increasingly dependent on networks and distributed computing and processing systems. Furthermore, because they possess a critical and integral asset of information, internetworking security and what measures to protect this information has become a major area of concern. In this paper we will address the key concepts of network security, common network vulnerabilities, network security threats and attacks, security measures and tools, and the development of a network security policy and proper violation response plan.

Network Security Architecture

The Internet is a worldwide collection of networks that is based on open protocols. Hence the network and Internet security are moving targets. Network security is setup to guard against unauthorized access, alteration, or modification of information, and unauthorized denial of service. A well-established network security and a well-implemented security policy can provide a highly secure solution so that only authorized people gain access to the system, that communications on the network are kept private from outsiders, and that data being communicated is kept safe. The following are the key components of network security architecture:

Authentication

Authentication is the action of verifying information such as identity, ownership or authorization (RSA Data Security, 1998). It verifies that a user requesting access is the one who he or she claims to be prior to being allowed access to the network and network services.

Access Control (Authorization)

Access control is a security measure that defines who can access a computer, when they can access it, and what actions they can take while accessing the computer (Shelly, Cashman, Vermaat, & Walker, 1999). There are numerous approaches in providing access control, ranging from password protection to token-based mechanisms to biometric encryption technologies.

Privacy

Privacy is the state or quality of being secluded from the view and or presence of others (RSA Data Security, 1999). The goal of privacy is to ensure that unauthorized users on the network cannot see the contents of the message being sent. Privacy is synonymous with confidentiality and secrecy (Sun Microsystems, 1999).

Integrity

Integrity includes the security of the network periphery, security of the network devices, and security of the flows of information between them (Cisco Systems, 1999). It addresses the unauthorized manipulation or destruction of data. Data integrity is ensured by encryption. If information is received that cannot be decrypted properly, then the recipient knows that the information has been tampered with during transmission.

Network Management

Network management keeps track of detailed records of user identities, all the communications on the network, which network services users are accessing, and the network resources they are utilizing. It provides all this information for billing, auditing, reporting, and subsequent reviews of related security events.

Hierarchy of Network Security Systems

The United States Department of Defense has classified four hierarchies of network security systems. At the top of the hierarchy is A, which provides the most security and at the bottom is D, which provides minimal or non-existent security. Each hierarchy has a number of levels as well, totaling seven. The layout and description of the hierarchy is documented in a publication known as the Trusted Computer System Evaluation Criteria (TCSEC), otherwise known as the Orange Book (United States Department of Defense, 1996). Another publication, the Red Book, provides subsidiary information that enables the Orange Book guidelines to be applied in a network environment. The Red Book was initially published as the Trusted Network Interpretation (TNI) of the TCSEC. The Orange and Red Books have begun to set a standard in network security. More corporations are requiring their purchases to satisfy a specific level of security as defined by these books. The following is the classification of network security systems, as defined in the Orange Book, in terms of access control, accountability (identification and authentication), operational assurance, and system architecture:

- D1 class has the minimal protection. A D1 rating system is untrusted and provides no security at all. It fails to meet the requirements for a higher evaluation class.
- C1 class has the discretionary security protection. It is suitable for allowing users to be able to protect project or private information and to keep other users from accidentally reading or destroying their data.
- C2 class has the controlled access protection. Systems in this class make users individually accountable for their login procedures, and provide auditing of security-related events and resource isolation.
- B1 class provides labeled security protection. This class supports multi-level security and mandatory access control in which access permission can only be assigned by authorized users.
- B2 class supports structured protection. Authentication mechanisms are strengthened, trusted facility management is provided, and stringent configuration management controls are imposed. The system of this class is relatively resistant to penetration.
- B3 class provides the security domains for the system. A security administrator is supported; audit mechanisms are expanded to signal security-related events, and system recovery procedures are required. A B3 class system is highly resistant to penetration.
- A1 class has a verified design protection and is the highest level of security validated through the Orange Book. It uses formal verification methods to ensure that the security controls employed in the system can effectively protect classified or other sensitive information stored or processed by the system. All hardware and software must be protected during shipment to prevent tampering.

Network Security Threats and Attacks

When a network is connected to the Internet to increase information sharing, communications, or productivity, the network is vulnerable to potential intrusions and attacks. Areas where potential intruders can enter may be dial-up access points, network connections, or misconfigured hosts. Misconfigured hosts, frequently overlooked as points of network entry can be network systems that (1) use unprotected login accounts (such as guest accounts), (2) employ extensive trust in remote commands, (3) have illegal modems attached to them, or (4) use easy-to-break passwords (Cisco Systems, 1997).

Security threats are classified as passive or active (Stallings & Van Slyke, 1998). Passive attacks involve eavesdropping on, or monitoring, transmissions without actually disturbing the network. The main concern of the point of vulnerability in the network is eavesdropping by another employee or unauthorized user. Data is transmitted in the form of frames or packets containing the source and destination address, and other related information. An eavesdropper can monitor the traffic of this information on the network. Individuals who attempt to read privileged data, perform unauthorized modification to data, or disrupt the system, on the other hand, carry out active attacks.

There are many ways in which to attack the network security. These security attacks target the key elements of the network security architecture as aforementioned:

Authentication Attacks (Unauthorized access)

These types of attacks occur when a user manipulates system resources or gains access to system information without authorization by either sharing logins or passwords or using an unattended terminal with an open session.

Password attack is a frequently used method of repeating attempts on a user account and/or password. These repeated attempts are called brute force attacks (Cisco Systems, 1999). They are performed using a program that runs across a network and attempts to log into a shared resource, such as a server.

Confidentiality Attacks (Network Snooping/Sniffing)

Because network computers communicate serially (even if networks communicate in parallel) and contain limited immediate buffers, information and data are transmitted in small blocks or pieces called packets. The attackers use a variety of methods known collectively as social engineering attacks (Cisco Systems, 1999). With the use of dozens of freeware and shareware packet sniffers available, which do not require the user to understand anything about the underlying protocols, the attackers would capture all network packets and thereby the users login names, passwords, and even accounts. The intruders usually take advantage of human tendency, e.g. using a single, same password for multiple accounts. More often they are successful in gaining access to corporate sensitive and confidential information. Some snooping attacks place the network interface card in promiscuous mode, while other packet sniffers capture the first 300 bytes of all telnet, file transfer protocol (FTP), and login sessions.

Integrity Attacks (Message Alteration, Delay, and Denial)

In this type of attack, data or information is added, removed, or modified in transit across the network. This requires root access to the system or a router. If a program does not check buffer limits when reading or receiving data, this opening can be exploited by an attacker to add arbitrary data into a program or system. When run, this data gives the intruder root access to the system.

Integrity attacks can create a delay, causing data to be held or otherwise made unavailable for a period of time. The attackers flood the network with useless traffic, making the system extremely slow to serve the customers, and in the extreme case, causing the system to crash. They could also cause the data to be discarded before final delivery. Both delay and denial attacks can result in the denial of service to the network users.

Access Control Attacks (Address Masquerading)

An attacker "listens" to the network traffic, finds the Internet Protocol (IP) address of a trusted host or system, configures his/her own network interface, and transmits the message as if from the trusted host. This is called IP address masquerading or IP spoofing. Like packet sniffers, IP address masquerading is not restricted to people who are external to the network.

Network Security Technologies

With the explosive growth in the Internet, network security has become an inevitable concern for any organization whose internal private network is connected to the Internet. New tools that probe for network system vulnerabilities, such as the Security Administrator Tool for Analyzing Networks (SATAN), assist in network security efforts. However, these tools can only identify points of risk and areas of weakness in the system. They cannot provide a means to protect their networks. The following are some of the widely used strong tools for securing computer networks:

Firewalls

A firewall system is a hardware/software configuration, physically located between an internal and external network that protects the internal network from unwanted intrusion from the outside network (Sun Microsystems, 1999). Firewalls restrict information entering and leaving at carefully controlled points. If implemented properly, they are very effective at keeping out unauthorized intruders and stopping unwanted activities on the internal network. There are many different ways to implement the firewalls: (1) packet-level authentication – access by protocol, (2) address-based authentication – access by IP address (both source and destination), (3) user authentication by login/password over Secure Socket Layer (SSL), (4) performing IP address translation, and (5) point-to-point encryption at IP-level in Virtual Private Networks (VPNs). Firewalls can also be used for intranet access control.

Encryption

Encryption is the process of transforming plaintext into unreadable form (called ciphertext) using a mathematical process (RSA Data Security, 1998). An encryption system includes four elements: (1) the plaintext, the raw data or message to be encrypted, (2) the cryptographic algorithm, a mathematical method that determines how plaintext is to be combined with a key, (3) the key, a string of digits, and (4) the cipher text, the encrypted message. The longer the key string digits, the more difficult the encrypted data is to break.

In theory, trying all possible keys in sequence can break any cryptographic method with a key. If a brute force is used to attack the cryptographic algorithms, the required computing power increases exponentially with the length of the key.

There are two classes of key-based mechanisms, symmetric (private-key or secret-key) and asymmetric (public-key) algorithms (SSH Communications Security, 1999). The difference between the two is that private-key algorithms use the same key for encryption and decryption, whereas public-key algorithms use a different key for encryption and decryption, and the decryption key cannot be derived from the encryption key. In general, symmetric algorithms are much faster to execute on a computer than asymmetric ones. In practice, however, they are frequently used together. Asymmetric algorithm is used to encrypt a randomly generated encryption key, and a random key is used to encrypt the actual message using a symmetric algorithm.

Cryptographic algorithms, both asymmetric and symmetric, are widely used in network security. The followings are some of the popular algorithms:

Public-Key Algorithms.

- RSA (Rivest-Shamir-Adelman) encryption is the most commonly used public-key algorithm. The security of RSA relies on the difficulty of factoring large integers. With the advancement of computing power, currently 512-bit keys are considered weak against brute force attacks, 1024-bit keys are secure enough for most purposes, and 2048-bit keys are likely to remain secure for decades (SSH Communications Security, 1999).
- Diffie-Hellman Algorithm involves two-way communications across the Internet without exchanging keys. Each party obtains the public key for the other from a certificate authority and performs a special calculation using a discrete logarithm with their own private keys. The result of the algorithm will be the same for both parties.
- Pretty Good Privacy (PGP) is an emerging encryption mechanism for protecting the privacy of network files and e-mail. It provides the means for encrypting the files and e-mails, creating public and private keys, maintaining a database of public keys, adding digital signatures to documents, and certifying keys and obtaining keys from key servers (Sun Microsystems, 1999). PGP runs on virtually every operating system, such as UNIX, Windows, DOS, OS/2, and MacOS.
- Elliptic Curve Cryptography (ECC) is an emerging network security technology that allows

longer key size while decreases overhead and latency. ECC uses an algebraic system that is defined on the points of an elliptic curve to provide public-key algorithms. These algorithms can be used to create digital signatures, and provide a secure means to transmit confidential information. More applications of ECC algorithms have been identified, such as financial transfers and wireless data transmissions that require intensive use of signing during the process of authentication. They are performed at high-speed and with limited bandwidth (Sun Microsystems, 1999).

Private-Key Algorithms.

- Data Encryption Standard (DES) is a symmetric cipher, which encrypts a message by breaking it down into blocks and encrypting each block (RSA Data Security, 1998). DES algorithm uses 56-bit keys out of a 64-bit block size. It was developed in the 1970s and has been adopted by the U.S. government. With today's computing power, DES is easily breakable. A variant of DES, triple DES or 3DES, uses DES algorithm three times and follows an encrypt-decrypt-encrypt sequence with three different, unrelated keys. With three iterations of DES algorithms, the effective key length is 112 bits, which is much more securing than plain DES.
- RC4 is a cipher algorithm designed by RSA Data Security. RC4 is essentially a pseudo random number generator, and the output of the generator is logically exclusive-ored with the data stream (SSH Communications Security, 1999). It is essential that the same RC4 key never be used to encrypt two different data streams. The U.S. government approves this type of algorithm with 40-bit keys only for export. The security is very weak for its key length even though the algorithm is very fast.
- International Data Encryption Algorithm (IDEA) is a fairly new algorithm developed at ETH Zurich, Switzerland. It uses a 128-bit key and is considered very secure.

Security Protocols

Currently, public-key and private-key algorithms are being implemented in the network security protocols. These protocols are necessary because more and more companies are doing business on the Internet, and the issue of secure payments over the Web has become a greater network security problem. Merchant servers are developed to provide secure measures for electronic commerce applications. The following are some of the widely used protocols for performing secure transactions on the web.

- Secure Socket Layer (SSL) protocol employs a private-key encryption nested within a public-key encryption, authenticated through the use of digital certificates (Netscape Communications, 1999). Netscape Communications based on RSA public key cryptography developed SSL. It allows private information, such as Credit Cards and purchase orders, to remain private while traveling across intranets and the public Internet. SSL is currently the most widely used method and particularly suitable for use in e-commerce applications due to the following features: (1) privacy is ensured through encryption, (2) integrity is ensured through decryption, and (3) authentication is provided through the use of digital certificates (Netsavvy Communications, 1999).
- Secure Electronic Transaction (SET) protocol was developed by Visa and MasterCard for enabling secure credit card transactions on the Internet. It employs RSA public key encryption technology and DES single-key technology (Stallings & Van Slyke, 1998). SET uses digital certificates to ensure the identities of all parties involved in a transaction and encrypts credit card information before sending it across the Internet.

Developing an Effective Network Security Policy

A study reported by the U.S. General Accounting Office (GAO)(1996) found that the U.S. Department of Defense network computers are extremely vulnerable. A series of security attacks conducted by the Defense Information System Agency (DISA) revealed that of 38,000 attacks DISA could penetrate the protection and gain access to the network computers 65% of time. Of those successful attacks only 4% (988 attacks) were detected by the target organization. Furthermore, of those detected, only 27% (267 attacks) were actually reported to the appropriate security authority. Given the sophisticated computer network at the Department of Defense and the number of computer personnel involved, the statistics are alarming.

The goal of network security is to provide maximum security with minimum impact on the user accessibility and productivity. The network security policy developed must conform to the existing organization policies, rules, and regulations. Security policies should reflect constant organization changes in its new business directions, technological changes, and resource allocations.

When developing an effective network security policy, the following 11 areas should be addressed (Cisco Systems, 1997):

1. Identify the Network Assets to Protect

The first step is to understand and identify the organization's network assets and determine the degree to which each of these assets must be protected. Items to be considered include hardware, software data, procedures, personnel and users, documentation and supplies.

2. Determine Points of Risk

Risk analysis includes what you need to protect, what you need to protect it from, and how to protect it.

You must understand how and where potential intruders can enter your organization’s network or sabotage network operations.

3. Determine the Cost of Security Measures

Security measures invariably cause inconvenience, particularly to certain personnel or users. They can consume significant computing resources and require dedicated hardware. Another cost of security measures is that they can also delay work and create expensive administrative and educational overhead. If the cost of implementing security measures outweighs its potential benefits and the actual dangers, then it is a disservice to the organization to implement them.

4. Limit the Scope of Access

Too much security can be as counterproductive as too little security. Organization can provide higher levels of security to the more sensitive areas of the network. Create multiple barriers within networks such that any authorized access to a part of the system does not automatically grant access to the entire infrastructure.

5. Identify Assumptions

Every network security system has underlying assumptions. For instance, an organization might assume that its network is fairly secure, that its network is not tapped, that intruders are not knowledgeable, that attackers use standard software, or that a locked room is safe. It is essential to identify, examine, and justify your assumptions. Any unassumed or hidden assumption may turn out to be a big security hole.

6. Consider Human Factors

It is optimal that a network security policy strikes a balance between productivity and protection. If security measures interfere with the essential use of the system and the users are not fully informed, the users almost always resist the change. These measures then are either ignored or even circumvented. All users should be educated on the proper use of their account or workstation, the proper procedure of the security, the detection of unauthorized access, and the accidental release or revelation of passwords or other secrets over unsecured telephone lines.

7. Control the Number of Secrets

A properly designed network security policy relies only on a limited number of secrets. The more secrets there are, the more difficult it becomes to keep them all.

8. Limit Your Trust

You should know which network devices you can trust and which software you can rely on. Under no circumstances should an assumption be made that all software are bug-free.

9. Understand Typical Network Functions

Understanding how a network system normally functions, being aware of what is expected and unexpected, and knowing how network devices are usually utilized will help you detect any security problems. System software auditing tools can help detect, log, and track any unusual events.

10. Realize Physical Security

Often times, the most obvious element of security is the one most easily overlooked, such as security guards, closed-circuit television, and card-key entry systems. It is essential that physical security, such as the server room or the network administration station be taken into consideration because they are the controlling center to the most sensitive, confidential information.

11. Implement Pervasive and Scalable Security

All personnel and users need to realize the security implications of every change they make. The goal of a network security policy is to create an environment that is not susceptible to every minor change.

Violation Response Plan

An organization needs to devise a response plan to a security violation. When a violation is detected, the immediate course of action or series of actions should be pre-defined to ensure prompt and proper enforcement. An investigation or analysis should be conducted to determine how and why the violation happened. Then, an appropriate corrective action should be executed. The violation response plan should also be prepared to answer the following questions:

- What outside agencies should be contacted, and who should contact them?
- Who may talk to the press?
- When do you contact law enforcement and investigative agencies?
- If a connection is made from a remote site, is the system manager authorized to contact that site?
- What are our responsibilities to our neighbors and other Internet sites? (Sun Microsystems, 1998)

Summary

Developing a network security policy comprises of identifying the organizational assets, threats, and risks as well as evaluating and implementing the tools and technologies available to meet these risks. When all these factors are accounted for, a usage policy is then developed. In addition, an auditing procedure that reviews network and server usage must be established on a timely basis. A proper response should also be in place before any breach or breakdown occurs.

Conclusion

With the vastly growing number of computer networks connected to the Internet, network security has become a major concern for organizations throughout the world. Proprietary business information loss is estimated between $550 million to $5 billion annually in the U.S. alone (Sun Microsystems, 1998). Most people do not know they are at risk until an attack occurs. The general rule is that as network security increases, cost increases, and the overall system/ network performance decreases. Network security consists of authentication, access control, integrity, and confidentiality. It must be addressed at three levels: (1) user-internal security policies, (2) Application – firewalls, proxies, and software, and (3) hardware – intelligent hubs, switches, and routers. A network security policy, an auditing procedure, and a violation response plan must all be in place to deal with any breach or breakdown of network security before it occurs.

References

Cisco Systems. (1999, June 17). *Security technologies* [WWW document]. URL http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ security.htm.

Cisco Systems. (1999, March 5). *Network security for securities and investment institutions* [WWW document]. URL http://www.cisco.com/warp/ public/cc/sol/mkt/ent/ inds/fin/netsc_sd.htm.

Cisco Systems. (1997). *Security Overview* [WWW document]. URL http://www.cisco .com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scoverv.htm.

eMarketer. (1998). *Worldwide Internet Users*, 1998-2003. [WWW document]. URL http://www.emarketer.com/estats/sell-eglob.html.

Netscape Communications. (1999). *How SSL works* [WWW document]. URL http://developer.netscape.com/tech/security/ssl/howitworks.html.

RSA Data Security. (1998). *Glossary* [WWW document]. URL http://www.rsa.com /rsalabs/faq/html/glossary.html.

Shelly, G. S., Cashman, T. J., Vermaat, M. E., & Walker, T. J. (1999). *Discovering Computers 2000: Concepts for a Connected World*. Cambridge, MA: Course Technology.

SSH Communications Security. (1999). *Introduction to Cryptography* [WWW document]. URL http://www.ssh.fi/tech/crypto/intro.html.

Stallings, W. & Van Slyke, R. (1998). *Business Data Communications* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

Sun Microsystems. (1998). *How to Develop a Network Security Policy* [WWW document]. URL http://www.sun.com/security/sec.policy.wp.html.

Sun Microsystems. (1999). *Mastering Security on the Internet for Competitive Advantage: Network Security Technologies* [WWW document]. URL http://www.sun.com/security/wp-mastering.sec/intro.html.

United States Department of Defense. (1996). *Orange Book Parts I and II: The Criteria and Rationale and guidelines: A guideline on configuring mandatory access* [WWW document]. URL http://www.ru.kernel.org/pub/linux/ libs/security/orange-linux/refs/orange/orange-II-9.html.

United States General Accounting Office. (1996, May). *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*. Report GAO/AIMD-96-84. Washington, D.C.: Author.