



Internet Security

Definition

Internet security is the practice of protecting and preserving private resources and information on the Internet.

Overview

Computer and network security are challenging topics among executives and managers of computer corporations. Even discussing security policies may seem to create a potential liability. As a result, enterprise management teams are often not aware of the many advances and innovations in Internet and intranet security technology. Without this knowledge, corporations are not able to take full advantage of the benefits and capabilities of the network. Together, network security and a well-implemented security policy can provide a highly secure solution. Employees can then confidently use secure data transmission channels and reduce or eliminate less secure methods, such as photocopying proprietary information, sending purchase orders and other sensitive financial information by fax, and placing orders by phone.

Topics

1. Elements of Networking Security: Orange Book Security Levels and Firewalls
2. Elements of Networking Security: Passwords
3. Elements of Networking Security: Encryption, Authentication, and Integrity
4. Developing a Site Security Policy
5. Violation Response
6. Other Security Resources
 - Self-Test
 - Correct Answers
 - Glossary

1. Elements of Networking Security: Orange Book Security Levels and Firewalls

While this tutorial will provide a basic understanding of the need for a site security policy and factors to consider in creating a security policy, it will not outline one policy that will fit every company. The reason for this is simple—security is very subjective. Every business has a different threshold of well-being, different assets, a different culture, and a different technology infrastructure. Every business has different requirements for storing, sending, and communicating information in electronic form. Just as a business evolves in changing market conditions, a site security policy must adapt to meet changing technology conditions. This tutorial is based on a publicly available document, request for comment (RFC) 1244.

There are many strong tools available for securing a computer network. By themselves, the software applications and hardware products that secure a business' computer network do not comprise a security policy, yet they are essential elements in the creation of site security. While these technologies are not the focus of this paper, a basic understanding of them will facilitate the creation of a site security policy.

Tools to protect your enterprise network have been evolving for the last two decades, roughly the same amount of time that people have been trying to break into computer networks. These tools can protect a computer network at many levels, and a well-guarded enterprise deploys many different types of security technologies. The most obvious element of security is often times the most easily overlooked: physical security—namely, controlling access to the most sensitive components in your computer network, such as a network administration station or the server room. No amount of planning or expensive equipment will keep your network secure if unauthorized personnel can have access to central administration consoles. Even if a user does not have evil intent, an untrained user may unknowingly provide unauthorized outside access or override certain protective configurations.

The next level of computer security is operating system security (OSS). The U. S. Department of Defense (DOD) established general guidelines for operating system security, and other countries around the world (as well as other federal organizations) have set their standards as well. In the past few years, certified (tested and approved) secure OSS has been introduced in commercial operating systems like UNIX® and Microsoft Windows NT. These are at the C2 level, which provides discretionary access control-file, directory read and write permission, and auditing and authentication controls.

Orange Book Security Levels

The DOD has defined seven levels of computer OSS in the Trusted Computer Standards Evaluation Criteria, otherwise known as the Orange Book. The levels are used to evaluate protection for hardware, software, and stored information. The system is additive—higher ratings include the functionality of the levels below. The definition centers around access control, authentication, auditing, and levels of trust. D1 is the lowest form of security available and states that the system is insecure. A D1 rating is never awarded because this is essentially no security at all. C1 is the lowest level of security. The system has file and directory read and write controls and authentication through user login. However, root is considered an insecure function and auditing (system logging) is not available. C2 features an auditing function to record all security-related events and provides stronger protection on key system files, such as the password file.

A B-rated system supports multilevel security, such as secret, top secret, and mandatory access control, which states that a user cannot change permissions on files or directories. B2 requires that every object and file be labeled according to its security level and that these labels change dynamically depending on what is being used. B3 extends security levels down into the system hardware; for example, terminals can only connect through trusted cable paths and specialized system hardware to ensure that there is no unauthorized access. A1 is the highest level of security validated through the Orange Book. The design must be mathematically verified; all hardware and software must have been protected during shipment to prevent tampering. A word of caution on secure operating systems must be mentioned: the features and capabilities require significant amounts of central processing unit (CPU) processing power and disk space. In low-end servers, enabling the security features may seriously affect the number of users a server can support.

Firewalls

While in theory firewalls allow only authorized communications between the internal and external networks, new ways are always being developed to compromise these systems. However, properly implemented, they are very effective at keeping out unauthorized users and stopping unwanted activities on an internal network. Firewall systems protect and facilitate your network at a number of levels. They allow e-mail and other applications, such as file transfer protocol (FTP) and remote login as desired, to take place while otherwise limiting access to the internal network. Firewall systems provide an authorization mechanism that assures that only specified users or applications can gain access through the firewall. They typically provide a logging and alerting feature, which tracks designated usage and signals at specified events. These systems offer address translation, which masks the actual name and address of any machine communicating through the firewall. For example, all messages for anyone in the

technical support department would have his/her address translated to techsupp@company.com, effectively hiding the name of an actual user and network address. Firewall system providers are adding new functionality, such as encryption and virtual private network (VPN) capabilities.

Firewall systems can also be deployed within an enterprise network to compartmentalize different servers and networks, in effect controlling access within the network. For example, an enterprise may want to separate the accounting and payroll server from the rest of the network and only allow certain individuals to access the information. Unfortunately, all firewall systems have some performance degradation. As a system is busy checking or rerouting data communications packets, they do not flow through the system as efficiently as they would if the firewall system were not in place.

2. Elements of Networking Security: Passwords

Password Mechanisms

Passwords are a way to identify and authenticate users as they access the computer system. Unfortunately, there are a number of ways in which a password can be compromised. For example, someone wanting to gain access can listen for a username password as an authorized user gains access over a public network. In addition, a potential intruder can mount an attack on the access gateway, entering an entire dictionary of words (or license plates or any other list) against a password field. Users may loan their password to a co-worker or inadvertently leave out a list of system passwords. Fortunately, there are password technologies and tools to help make your network more secure. Useful in ad hoc remote access situations, one-time password generation assumes that a password will be compromised. Before leaving the internal network, a list of passwords that will work only one time against a given username is generated. When logging into the system remotely, a password is used once and then will no longer be valid.

Password Aging and Policy Enforcement

Password aging is a feature that requires users to create new passwords every so often. Good password policy dictates that passwords must be a minimum number of characters and a mix of letters and numbers. Smart cards provide extremely secure password protection. Unique passwords, based on a challenge-response scheme, are created on a small credit-card device. The password is then entered as part of the log-on process and validated against a password server, which logs all access to the system. As might be expected, these systems can be expensive to implement.

Single sign-on overcomes what can only be the ultimate irony in system security: as a user gains more passwords, these passwords become less secure, not more, and the system opens itself up for unauthorized access. Many enterprise computer networks are designed to require users to have different passwords to access different parts of the system. As users acquire more passwords—some people have more than 50—they cannot help but write them down or create easy-to-remember passwords. A single sign-on system is essentially a centralized access control list which determines who is authorized to access different areas of the computer network and a mechanism for providing the expected password. A user need only remember a single password to sign onto the system.

Good password procedures:

- **Do not** use your login name in any form (as is, reversed, capitalized, doubled, etc.).
- **Do not** use your first, middle, or last name in any form or use your spouse's or children's names.
- **Do not** use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the make of your automobile, the name of the street you live on, etc.
- **Do not** use a password of all digits or all the same letter.
- **Do not** use a word contained in English or foreign language dictionaries, spelling lists, or other lists of words.
- **Do not** use a password shorter than six characters.
- **Do** use a password with mixed-case alphabets.
- **Do** use a password with non-alphabetic characters (digits or punctuation).
- **Do** use a password that is easy to remember, so you don't have to write it down.

3. Elements of Networking Security: Encryption, Authentication, and Integrity

A firewall system is a hardware/software configuration that sits at perimeter between a company's network and the Internet, controlling access into and out of the network. Encryption can be understood as follows:

- the coding of data through an algorithm or transform table into apparently unintelligible garbage
- used on both data stored on a server or as data is communicated through a network
- a method of ensuring privacy of data and that only intended users may view the information

There are many forms of encryption, but only the most popular forms will be discussed in this tutorial. The digital encryption standard (DES) has been endorsed by the National Institute of Standards and Technology (NIST) since 1975 and is the most readily available encryption standard. One major drawback with DES is that it is subject to U. S. export control; programs that deploy DES technology are generally not available for export from the United States. Rivest, Shamir, and Adleman (RSA) encryption is a public-key encryption system, is patented technology in the United States, and thus is not available without a license. However, the fundamental DES algorithm was published before the patent filing, and RSA encryption may be used in Europe and Asia without a royalty. RSA encryption is growing in popularity and is considered quite secure from brute force attacks. An emerging encryption mechanism is pretty good privacy (PGP), which allows users to encrypt information stored on their system as well as to send and receive encrypted e-mail. PGP also provides tools and utilities for creating, certifying, and managing keys. PGP should not be confused with privacy enhanced mail (PEM), a protocol standard.

Encryption mechanisms rely on keys or passwords. The longer the password, the more difficult the encryption is to break. DES relies on a 56-bit key length, and some mechanisms have keys that are hundreds of bits long. There are two kinds of encryption mechanisms used—private key and public key. Private-key encryption uses the same key to encode and decode the data. Public-key encryption uses one key to encode the data and another to decode the data. The name public key comes from a unique property of this type of encryption mechanism—namely, one of the keys can be public without compromising the privacy of the message or the other key. In fact, usually a trusted recipient, perhaps a remote office network gateway, keeps a private key to decode data as it comes from the main office. VPNs employ encryption to provide secure transmissions over public networks such as the Internet.

Authentication and Integrity

Authentication is simply making sure users are who they say they are. When using resources or sending messages in a large private network, not to mention the Internet, authentication is of the utmost importance. Integrity is knowing that the data sent has not been altered along the way. Of course, a message

modified in any way would be highly suspect and should be completely discounted. Message integrity is maintained with digital signatures. A digital signature is a block of data at the end of a message that attests to the authenticity of the file. If any change is made to the file, the signature will not verify. Digital signatures perform both an authentication and message integrity function. Digital signature functionality is available in PGP and when using RSA encryption. Kerberos is an add-on system that can be used with any existing network. Kerberos validates a user through its authentication system and uses DES when communicating sensitive information—such as passwords—in an open network. In addition, Kerberos sessions have a limited lifespan, requiring users to login after a predetermined length of time and disallowing would-be intruders to replay a captured session and thus gain unauthorized entry.

4. Developing a Site Security Policy

The first rule of network site security is easily stated: that which is not expressly permitted is prohibited. A security policy should deny access to all network resources and then add back access on a specific basis. Implemented in this way, a site security policy will not allow any inadvertent actions or procedures. The goal in developing an official site policy on computer security is to define the organization's expectations for proper computer and network use and to define procedures to prevent and respond to security incidents. In order to do this, specific aspects of the organization must be considered and agreed upon by the policy-making group. For example, a military base may have very different security concerns from those of a university. Even departments within the same organization will have different requirements.

It is important to consider who will make the network site security policy. Policy creation must be a joint effort by a representative group of decision-makers, technical personnel, and day-to-day users from different levels within the organization. Decision-makers must have the power to enforce the policy; technical personnel will advise on the ramifications of the policy; and day-to-day users will have a say in how usable the policy is. A site security policy that is unusable, unimplementable, or unenforceable is worthless.

Developing a security policy comprises identifying the organizational assets, identifying the threats, assessing the risk, implementing the tools and technologies available to meet the risks, and developing a usage policy. In addition, an auditing procedure must be created that reviews network and server usage on a timely basis. A response should be in place before any violation or breakdown occurs as well. Finally, the policy should be communicated to everyone who uses the computer network, whether employee or contractor, and should be reviewed on a regular basis.

Identifying the Organizational Assets

The first step in creating a site security policy is creating a list of all the things that must be protected. The list must be easily and regularly updated, as most organizations add and subtract equipment all the time. Items to be considered include the following:

- **hardware**—CPUs, boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers, routers
- **software**—source programs, object programs, utilities, diagnostic programs, operating systems, communication programs
- **data**—during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media
- **documentation**—on programs, hardware, systems, and local administrative procedures

Assessing the Risk

While there is a great deal of publicity about intruders on computer networks, most surveys show that the loss from people within the organization is significantly greater. Risk analysis involves determining what must be protected, from what it must be protected, and how to protect it.

Possible risks to your network include the following:

- unauthorized access
- unavailable service, corruption of data, or a slowdown due to a virus
- disclosure of sensitive information, especially that which gives someone else a particular advantage, or theft of information such as credit card information

Once the list has been assembled, a scheme for weighing the risk against the importance of the resource should be developed. This will allow the site policy makers to determine how much effort should be spent protecting the resource. Some security experts advocate the proactive use of the very tools that hackers use in order to find system weaknesses. By discovering weaknesses before the fact, protective action can be implemented to fend off certain attacks. Perhaps the most famous of these tools is security analysis tool for auditing networks (SATAN), which is publicly available on many WWW sites.

Auditing and Review

To help determine if there is a violation of a security policy, take advantage of the tools that are included in computers and networks. Most operating systems store numerous bits of information in log files. Examination of these log files on a regular basis is often the first line of defense in detecting unauthorized use of the system. Compare lists of currently logged in users and past login histories. Most users typically log in and out at roughly the same time each day. An account logged in outside the normal time for the account may be being used by an intruder.

In addition, accounting records can be used to determine usage patterns for the system; unusual accounting records may indicate unauthorized use of the system. System logging facilities, such as the UNIX "syslog" utility, should be checked for unusual error messages from system software. For example, a large number of failed login attempts in a short period of time may indicate someone trying to guess passwords. Operating system commands that list currently executing processes can be used to detect users running programs they are not authorized to use, as well as to detect unauthorized programs that have been started by an intruder. By running various monitoring commands at different times throughout the day, a company makes it harder for intruders to predict when they can be detected. While it may be exceptionally fortuitous that an administrator would catch a violator in their first act, by reviewing log files there is a very good chance for setting up procedures to identify them at a later date.

5. Violation Response

Planning responses for different violation scenarios well in advance—without the burden of an actual event—is good practice. Not only must companies define actions based on the type of violation, but it is also important to have solutions ready based on the anticipated kind of user violating the computer security policy.

Answers to the following questions should be a part of a company's site security plan:

- 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? Whenever a site suffers an incident that may compromise computer security, the strategies for reacting may be influenced by two opposing pressures.

If management fears that the site is sufficiently vulnerable, it may choose a protect and proceed strategy. The primary goals of this approach are to protect and preserve the site facilities and to provide normalcy for its users as quickly as possible. Attempts will be made to interfere with the intruder's processes, prevent further access, and begin immediate damage assessment and recovery. This process may involve shutting down the facilities, closing off access to the network, or other drastic measures. The drawback is that unless the intruders are identified, they may come back into the site via a different path or may attack another site.

The alternate approach, pursue and prosecute, adopts the opposite philosophy and goals. The primary goal is to allow intruders to continue their activities at the site until the site can identify the responsible persons. Law enforcement agencies and prosecutors endorse this approach. The drawback is that the agencies cannot exempt a site from possible user lawsuits if damage is done to their systems and data. Prosecution is not the only outcome possible if the intruder is identified. If the culprit is an employee or a student, the organization may choose to take disciplinary actions. Site management must carefully consider potential approaches to this issue before the problem occurs. The strategy adopted might depend upon each circumstance, or there may be a global policy that mandates one approach in all circumstances. The following are checklists to help a site determine which of the two strategies to adopt.

Protect and Proceed

- if assets are not well protected
- if continued penetration could result in great financial risk
- if there is no possibility or willingness to prosecute
- if user base is unknown
- if users are unsophisticated and their work is vulnerable
- if the site is vulnerable to lawsuits from users, e.g., if their resources are undermined

Pursue and Prosecute

- if assets and systems are well protected
- if good backups are available
- if the risk to the assets is outweighed by the disruption caused by the present and potential future penetrations
- if this is a concentrated attack occurring with great frequency and intensity
- if the site has a natural attraction to intruders and consequently regularly attracts intruders
- if the site is willing to incur the financial (or other) risk to assets by allowing the perpetrator to continue
- if intruder access can be controlled
- if the monitoring tools are sufficiently well developed to make the pursuit worthwhile
- if the support staff is sufficiently clever and knowledgeable about the operating system, related utilities, and systems to make the pursuit worthwhile
- if management is willing to prosecute
- if the system administrators know what kind of evidence would lead to prosecution
- if there is established contact with knowledgeable law enforcement
- if there is a site representative versed in the relevant legal issues
- if the site is prepared for possible legal action from its own users if their data or systems become compromised during the pursuit

Capturing Lessons Learned

Once you believe that a system has been restored to a safe state, it is still possible that holes and even traps could be lurking. In the follow-up stage, the system should be monitored for items that may have been missed during the clean-up stage. It would be prudent to utilize some of the tools mentioned as a start.

Remember that these tools do not replace continual system monitoring and good systems administration procedures. A security log can be most valuable during this phase of removing vulnerabilities. There are two considerations here. The first is to keep logs of the procedures that have been used to make the system secure again. This should include command procedures (e.g., shell scripts) that can be run on a periodic basis to recheck the security. Second, keep logs of important system events. These can be referenced when trying to determine the extent of the damage of a given incident.

After an incident, it is prudent to write a report describing the incident, method of discovery, correction procedure, monitoring procedure, and a summary of lessons learned. This will help develop a clear understanding of the problem. Remember that it is difficult to learn from an incident if you do not understand the source.

6. Other Security Resources

There is a growing list of resources that can provide details on virtually every subject mentioned in this tutorial. Among these are several good books and a number of newsgroups and mailing lists.

Books

Chapman, D. Brent and Elizabeth D. Zwicky. *Building Internet Firewalls*. O'Reilly and Associates, Inc., 1995.

Garfinkel, Simson. *PGP—Pretty Good Privacy*. O'Reilly and Associates, Inc., 1995.

Garfinkel, Simson and Gene Spafford. *Practical UNIX Security*. O'Reilly and Associates, Inc., 1991.

Siyam, Karanjit and Chris Hare. *Internet Firewalls and Network Security*. New Riders Publishing, 1995.

Vacca, John. *Internet Security Secrets*. IDG Books, 1996.

Security Newsgroups and Mailing Lists

The following newsgroups are available on the USENET news system:

- comp.security.announce
- comp.security.misc

- comp.security.unix
- alt.security
- misc.security

The UNIX security mailing list is only open to people who are the principal administrators of a site. The address for a subscription request is security-request@cpd.com.

The Bugtraq list discusses security holes and software bugs and how to fix them. To subscribe, send e-mail to bugtraq-request@crimelab.com. In the body of the message include the following line: subscribe bugtraq-list firstname lastname.

Computer Emergency Response Team (CERT) is an organization that helps Internet users identify and rectify damage done to their system by hackers and crackers. To subscribe to the CERT advisory mailing list, send e-mail to cert-request@cert.sei.cmu.edu and put the following in the body of the message: subscribe cert firstname lastname. CERT also maintains a CERT-TOOLS list for the purpose of exchanging information on tools and techniques that increase the secure operation of Internet systems. To subscribe, send e-mail to cert-tools-request@cert.sei.cmu.edu and put the following in the body of the message: subscribe cert-tools firstname lastname.

Other Documents

The basis for this tutorial is "The Site Security Handbook" by J.P. Holbrook and J.K. Reynolds, RFC 1244 Jul-01-1991. The full text is available at <ftp://archie.au/rfc/rfc1244.au.gz> or at <http://ds.internic.net/ds/dspg2intdoc.html>. NIST has published a document entitled *Establishing a Computer Security Incident Response Capability*. It is NIST Special Publication 800-3.

Self-Test

1. Which of the following is not part of the DOD's Orange Book?
 - a. access control
 - b. auditing
 - c. authentication
 - d. encryption

- e. levels of trust
2. _____ is a protocol standard.
- a. DES
 - b. PEM
 - c. PGP
 - d. RSA
3. The first step in creating a site security policy is _____.
- a. making a list of assets
 - b. making a list of threats
 - c. finding tools to monitor your systems
 - d. identifying the biggest risk
4. Network security requirements are _____.
- a. the responsibility of the system administrator
 - b. only needed if a computer is a connection to the Internet
 - c. unique for each organization
 - d. defined by your operating system
5. The DOD Orange Book defines the lowest level of security as _____.
- a. A1
 - b. A2
 - c. C1
 - d. C2
 - e. D1

6. An encryption method that requires the use of two keys is called _____.
- a. public-key encryption
 - b. private-key encryption
 - c. certificate of authority
7. Single network sign-ons are not as good as individual logins for each system that a user needs to access.
- a. true
 - b. false
8. A good password should be pure gibberish, so that it will be hard to remember.
- a. true
 - b. false
9. Most users log in and out at roughly the same time each day; access outside the normal pattern may indicate an intruder.
- a. true
 - b. false
10. Firewall systems can be used both for separating an organization from the outside world and dividing departments within an organization.
- a. true
 - b. false

Correct Answers

1. Which of the following is not part of the DOD's Orange Book?
- a. access control
 - b. auditing
 - c. authentication

d. encryption

e. levels of trust

(See Topic 1).

2. _____ is a protocol standard.

a. DES

b. PEM

c. PGP

d. RSA

(See Topic 3).

3. The first step in creating a site security policy is _____.

a. making a list of assets

b. making a list of threats

c. finding tools to monitor your systems

d. identifying the biggest risk

(See Topic 4).

4. Network security requirements are _____.

a. the responsibility of the system administrator

b. only needed if a computer is a connection to the Internet

c. unique for each organization

d. defined by your operating system

(See Topic 1).

5. The DOD Orange Book defines the lowest level of security as _____.

a. A1

b. A2

- c. C1
- d. C2
- e. D1**

(See Topic 1).

6. An encryption method that requires the use of two keys is called _____.

- a. public-key encryption**
- b. private-key encryption
- c. certificate of authority

(See Topic 3).

7. Single network sign-ons are not as good as individual logins for each system that a user needs to access.

a. true

b. false

(See Topic 2).

8. A good password should be pure gibberish, so that it will be hard to remember.

a. true

b. false

(See Topic 2).

9. Most users log in and out at roughly the same time each day; access outside the normal pattern may indicate an intruder.

a. true

b. false

(See Topic 4).

10. Firewall systems can be used both for separating an organization from the outside world and dividing departments within an organization.

a. true

b. false

(See Topic 1).

Glossary

CERT

computer emergency response team

CPU

central processing unit

DES

digital encryption standard

DOD

U.S. Department of Defense

FTP

file transfer protocol

NIST

National Institute of Standards and Technology

OSS

operating system security

PEM

privacy enhanced mail

PGP

pretty good privacy

RFC

request for comment

RSA

RSA is a public-key cryptosystem for both encryption and authentication; it was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

SATAN

security analysis tool for auditing networks

VPN
virtual private network