UNIT-4

Security Technology: Intrusion detection, Access control and other security tools: Intrusion detection and prevention systems, Scanning and analysis tools, Access control devices.
Cryptography: Foundations of cryptology, cipher methods, crypryptographic Algorithms, Cryptographic tools, Protocols for secure communications, Attacks on cryptosystems

---

Introduction

- An intrusion is a type of attack on information assets in which the instigator attempts to gain entry into a system or disrupt the normal operations of a system with, almost always, the intent to do malicious harm.
- Incident response is the identification of, classification of, response to, and recovery from an incident, and is frequently discussed in terms of prevention, detection, reaction, and correction.
- Intrusion prevention consists of activities that seek to deter an intrusion from occurring.
- Intrusion detection consists of procedures and systems that are created and operated to detect system intrusions.
- Intrusion reaction encompasses the actions an organization undertakes when an intrusion event is detected.
- Intrusion correction activities finalize the restoration of operations to a normal state, and by seeking to identify the source and method of the intrusion in order to ensure that the same type of attack cannot occur again, they return to intrusion prevention—thus closing the incident response loop.

Intrusion Detection Systems (IDSs)

- An IDS detects a violation of its configuration and activates an alarm. System administrators can choose the configuration of the various alerts and the associated alarm levels for each type of alert.
- Many IDSs enable administrators to configure the systems to notify them directly of trouble via e-mail or pagers.
- The systems can also be configured to notify an external security service organization of a "break-in."

IDS Terminology

- **Alert or Alarm**: An indication that a system has just been attacked and/or continues to be under attack.
- **False Attack Stimulus**: An event that triggers alarms and causes a false positive when no actual attacks are in progress.
- **False Negative**: The failure of an IDS system to react to an actual attack event.
- **False Positive**: An alarm or alert that indicates that an attack is in progress or that an attack has successfully occurred when in fact there was no such attack.
- **Noise**: The ongoing activity from alarm events that are accurate and noteworthy but not necessarily significant as potentially successful attacks.
- **Site Policy**: The rules and configuration guidelines governing the implementation and operation of IDSs within the organization.
- **Site Policy Awareness**: An IDS's ability to dynamically modify its site policies in reaction or response to environmental activity.

- **True Attack Stimulus:** An event that triggers alarms and causes an IDS to react as if a real attack is in progress.
- **Confidence Value:** A value associated with an IDS's ability to detect and identify an attack correctly.
- **Alarm Filtering:** The process of classifying the attack alerts that an IDS produces in order to distinguish/sort false positives from actual attacks more efficiently.

Why Use an IDS?

- To prevent problem behaviors by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system
- To detect attacks and other security violations that are not prevented by other security measures
- To detect and deal with the preambles to attacks
- To document the existing threat to an organization
- To act as quality control for security design and administration, especially of large and complex enterprises
- To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors

Types of IDSs and Detection Methods

IDSs operate as network-based, host-based, or application-based systems.

- A network-based IDS is focused on protecting network information assets.
- A host-based version is focused on protecting the server or host's information assets.

- The application-based model works on one or more host systems that support a single application and is oriented to defend that specific application from special forms of attack.

All IDSs use one of two detection methods:

- Signature-based
- Statistical anomaly-based

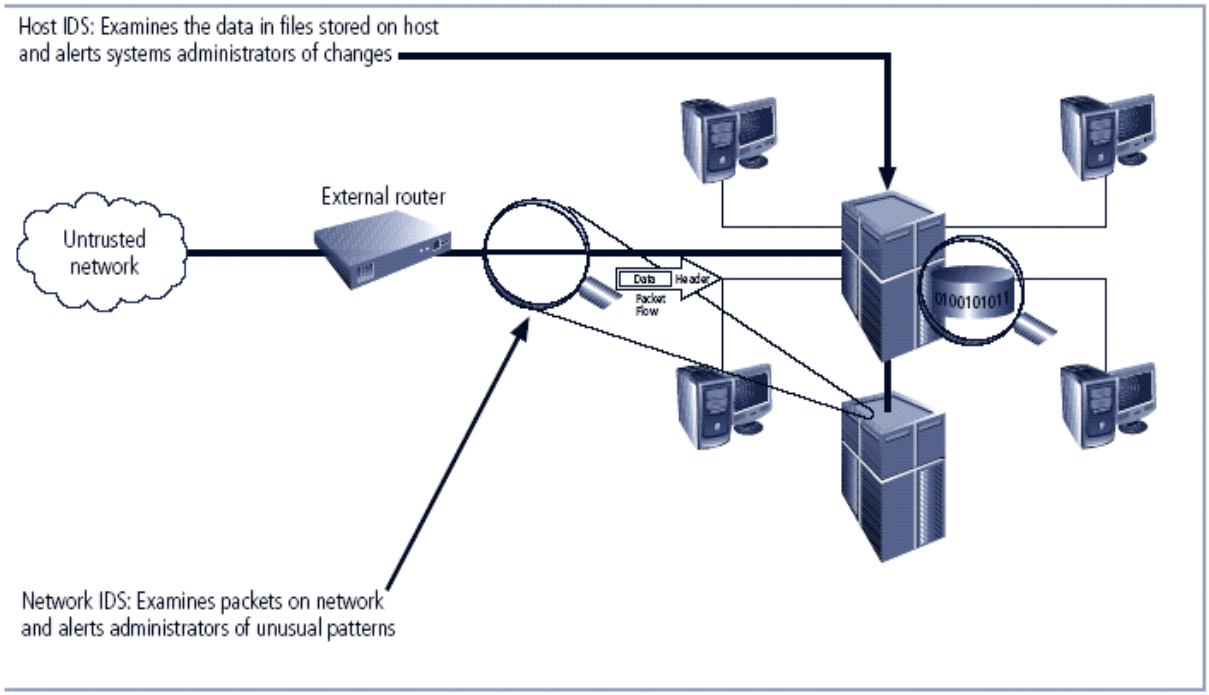


FIGURE 7-1 Intrusion Detection Systems

Network-Based IDS

A network-based IDS resides on a computer or appliance connected to a segment of an organization's network and monitors network traffic on that network segment, looking for indications of ongoing or successful attacks.

When a situation occurs that the network-based IDS is programmed to recognize as an attack, it responds by sending notifications to administrators.

When examining the packets transmitted through an organization's networks, a NIDS looks for attack patterns within network traffic such as large collections of related items that are of a certain type, which could indicate that a denial-of-service attack is underway, or the exchange of a series of related packets in a certain pattern, which could indicate that a port scan is in progress.

NIDSs are installed at a specific place in the network (such as on the inside of an edge router) from where it is possible to watch the traffic going into and out of a particular network segment.

The NIDS can be deployed to watch a specific grouping of host computers on a specific network segment, or it may be installed to monitor all traffic between the systems that make up an entire network.

NIDS Signature Matching

To determine whether or not an attack has occurred or may be underway, NIDSs look for attack patterns by comparing measured activity to known signatures in their knowledge base.

They do this by comparing captured network traffic using a special implementation of the TCP/IP stack that reassembles the packets and applies protocol stack or application protocol verification:

- In the process of protocol stack verification, the NIDSs look for invalid data packets.
- In application protocol verification, the higher-order protocols are examined for unexpected packet behavior or improper use.

Advantages of NIDSs

- Good network design and placement of NIDS devices can enable an organization to use a few devices to monitor a large network.
- NIDSs are usually passive devices and can be deployed into existing networks with little or no disruption to normal network operations.
- NIDSs are not usually susceptible to direct attack and, in fact, may not be detectable by attackers.
- A NIDS can become overwhelmed by network volume and fail to recognize attacks it might otherwise have detected.
- NIDSs require access to all traffic to be monitored.
- NIDSs cannot analyze encrypted packets, making some of the network traffic invisible to the process.
- NIDSs cannot reliably ascertain if an attack was successful or not.
- Some forms of attack are not easily discerned by NIDSs, specifically those involving fragmented packets.

Disadvantages of NIDSs

- A NIDS can become overwhelmed by network volume and fail to recognize attacks it might otherwise have detected.
- NIDSs require access to all traffic to be monitored.
- NIDSs cannot analyze encrypted packets, making some of the network traffic invisible to the process.
- NIDSs cannot reliably ascertain if an attack was successful or not.
- Some forms of attack are not easily discerned by NIDSs, specifically those involving fragmented packets.

Host-Based IDS

A host-based IDS resides on a particular computer or server, known as the host, and monitors activity only on that system.

HIDSs are also known as system integrity verifiers, as they benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files.

Most HIDSs work on the principle of configuration or change management, which means they record the sizes, locations, and other attributes of system files.

The HIDS then triggers an alert when one of the following changes occurs: file attributes change, new files are created, or existing files are deleted.

A HIDS has an advantage over NIDS in that it can usually be installed in such a way that it can access information that is encrypted when traveling over the network.

A HIDS relies on the classification of files into various categories and then applies various notification actions, depending on the rules in the HIDS configuration.

Managed HIDSs can monitor multiple computers simultaneously by creating a configuration file on each monitored host and by making each HIDS report back to a master console system, which is usually located on the system administrator's computer.

Advantages of HIDSs

- A HIDS can detect local events on host systems and also detect attacks that may elude a network-based IDS.
- A HIDS functions on the host system, where encrypted traffic will have been decrypted and is available for processing.
- The use of switched network protocols does not affect a HIDS.
- A HIDS can detect inconsistencies in how applications and systems programs were used by examining the records stored in audit logs.

Disadvantages of HIDS

- HIDSs pose more management issues since they are configured and managed on each monitored host.
- A HIDS is vulnerable both to direct attacks and to attacks against the host operating system.
- A HIDS is not optimized to detect multi-host scanning, nor is it able to detect the scanning of non-host network devices, such as routers or switches.
- A HIDS is susceptible to some denial-of-service attacks.
- A HIDS can use large amounts of disk space to retain the host OS audit logs; to function properly, it may require disk capacity to be added to the system.
- A HIDS can inflict a performance overhead on its host systems, and in some cases may reduce system performance below acceptable levels.

Signature-Based IDS

A signature-based IDS (or knowledge-based IDS) examines data traffic in search of patterns that match known signatures—preconfigured, predetermined attack patterns.

Signature-based IDS technology is widely used because many attacks have clear and distinct signatures.

The problem with the signature-based approach is that as new attack strategies are identified, the IDS's database of signatures must be continually updated.

Statistical Anomaly-Based IDS

The statistical anomaly-based IDS (stat IDS) or behavior-based IDS periodically sample network activity, and, using statistical methods, compare the sampled network activity to traffic that is known to be normal (performance baseline).

When the measured activity is outside the baseline parameters or clipping level, the IDS will trigger an alert to notify the administrator.

The data that is measured from the normal traffic and is used to prepare the baseline can include variables such as host memory or CPU usage, network packet types, and packet quantities.

The advantage of the statistical anomaly-based approach is that the IDS can detect new types of attacks, for it is looking for abnormal activity of any type.

Unfortunately, however, these systems require much more overhead and processing capacity than signature-based ones, as they must constantly compare patterns of activity against the baseline.

Another drawback is that these systems may not detect minor changes to system variables and may generate many false positives.

State ful Protocol Analysis IDPS

- SP 800-94: state ful protocol analysis (SPA) process of comparing predetermined profiles of definitions of benign activity for each protocol state against observed events to identify deviations
- Stores and uses relevant data detected in a session to identify intrusions involving multiple requests/responses; allows IDPS to better detect specialized, multisession attacks (deep packet inspection)
- Drawbacks: analytical complexity; processing overhead; may fail to detect unless protocol violates fundamental behavior; may cause problems with protocol it’s examining

Log File Monitors

A log file monitor (LFM) is similar to a NIDS and reviews the log files generated by servers, network devices, and even other IDSs for patterns and signatures in the log files that may indicate that an attack or intrusion is in process or has already succeeded.

The patterns that signify an attack can be subtle and hard to distinguish when one system is examined in isolation, but they may be much easier to identify when the entire network and its systems are viewed holistically.

Of course, this approach will require the allocation of considerable resources since it will involve the collection, movement, storage, and analysis of very large quantities of log data.

IDS Response Behavior

Once an IDS detects an anomalous network situation, it has a number of options, depending on the policy and objectives of the organization that has configured it as well as the capabilities of the organization's system.

IDS responses can be classified as active or passive. An active response is one in which a definitive action is initiated when certain types of alerts are triggered. IDSs with passive response options simply report the information they have already collected and wait for the administrator to take actions.

- Audible / visual alarm
- SNMP traps and plug-ins
- E-mail message
- Page or phone message
- Log entry
- Evidentiary packet dump
- Take action against the intruder
- Launch program
- Reconfigure firewall
- Terminate session
- Terminate connection

Selecting IDS Approaches and Products

The wide array of intrusion detection products available today addresses a broad range of organizational security goals and considerations.

Given that range of products and features, the process of selecting products that represent the best fit for any specific organization's needs is challenging. The following questions may be useful when preparing a specification for acquiring and deploying an intrusion detection product

Organizational Requirements & Constraints

- What are requirements that are levied from outside the org?

Is your org subject to oversight or review by another org?

Are there requirements for public access to information on your org's systems?

Are there other security-specific requirements levied by law?

Are there internal audit requirements for security best practices or due diligence?

Is the system subject to accreditation?

Are there requirements for law enforcement investigation and resolution of security incidents?

- What are your organization's resource constraints?

What is the budget for acquisition and life cycle support of intrusion detection hardware, software, and infrastructure?

Is there sufficient existing staff to monitor an IDS full time?

Does your org have authority to instigate changes based on the findings of an IDS?

IDSs Product Features & Quality

- Is the product sufficiently scalable for your environment?
- How has the product been tested?

Has the product been tested against functional requirements?

Has the product been tested against attack? Ask vendors for details of the security testing to which its products have been subjected.

- What is the user level of expertise targeted by the product?
- Is the product designed to evolve as the organization grows?

Can the product adapt to growth in user expertise?

Can the product adapt to growth and change of the organization's systems infrastructure?

Can the product adapt to growth and change of the security threat environment?

- What are the support provisions for the product?

What are commitments for product installation and configuration support?

What are commitments for ongoing product support?

Are subscriptions to signature updates included?

How often are subscriptions updated?

How quickly after a new attack is made public will the vendor ship a new signature?

Are software updates included?

How quickly will software updates and patches be issued after a problem is reported to the vendor?

Are technical support services included?

What are the contact provisions for contacting technical support?

Are there any guarantees associated with the IDS?

What training resources does the vendor provide as part of the product?

IDPSs perform the following functions well:

- Monitoring and analysis of system events and user behaviors
- Testing security states of system configurations
- Baselining security state of system and tracking changes
- Recognizing system event patterns matching known attacks
- Recognizing activity patterns that vary from normal activity
- Managing OS audit and logging mechanisms and data they generate
- Alerting appropriate staff when attacks are detected

IDPSs cannot perform the following functions:

- Detecting new attacks or variants of existing attacks
- Effectively responding to attacks by sophisticated attackers
- Investigating attacks without human intervention
- Resisting attacks intended to defeat or circumvent them
- Compensating for problems with fidelity of data sources
- Dealing effectively with switched networks

IDS Control Strategies

An IDS can be implemented via one of three basic control strategies.

A control strategy determines how an organization exerts influence and maintains the configuration of an IDS.

The three commonly utilized control strategies are:

- Centralized IDS control strategy—All IDS control functions are implemented and managed in a central location.

- Fully distributed IDS control strategy—Control functions are applied at the physical location of each IDS component.
- Partially distributed IDS control strategy—Combines the two: While the individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable the organization to detect widespread attacks.

IDS Deployment Overview

Like the decision regarding control strategies, the decision about where to locate the elements of the intrusion detection systems can be an art in itself.

As an organization selects an IDS and prepares for implementation, planners must select a deployment strategy that is based on a careful analysis of the organization's information security requirements and integrates with the organization's existing IT infrastructure but, at the same time, causes minimal impact.

NIDS and HIDS can be used in tandem to cover both the individual systems that connect to an organization's networks and the networks themselves.

Deploying Network-Based IDSs

NIST recommends four locations for NIDS sensors:

Location 1: Behind each external firewall, in the network DMZ

- IDS sees attacks that originate from the outside world and may penetrate the network's perimeter defenses.
- IDS can identify problems with the network firewall policy or performance.
- IDS sees attacks that might target the Web server or ftp server, both of which commonly reside in this DMZ.
- Even if the incoming attack is not detected, the IDS can sometimes recognize, in the outgoing traffic, patterns that suggest that the server has been compromised.

Location 2: Outside an external firewall

- IDS documents the number of attacks originating on the Internet that target the network.
- IDS documents the types of attacks originating on the Internet that target the network.

Location 3: On major network backbones

- IDS monitors a large amount of a network's traffic, thus increasing its chances of spotting attacks.
- IDS detects unauthorized activity by authorized users within the organization's security perimeter.

Location 4: On critical subnets

- IDS detects attacks targeting critical systems and resources.

Location allows organizations with limited resources to focus these resources on the network assets considered of greatest value

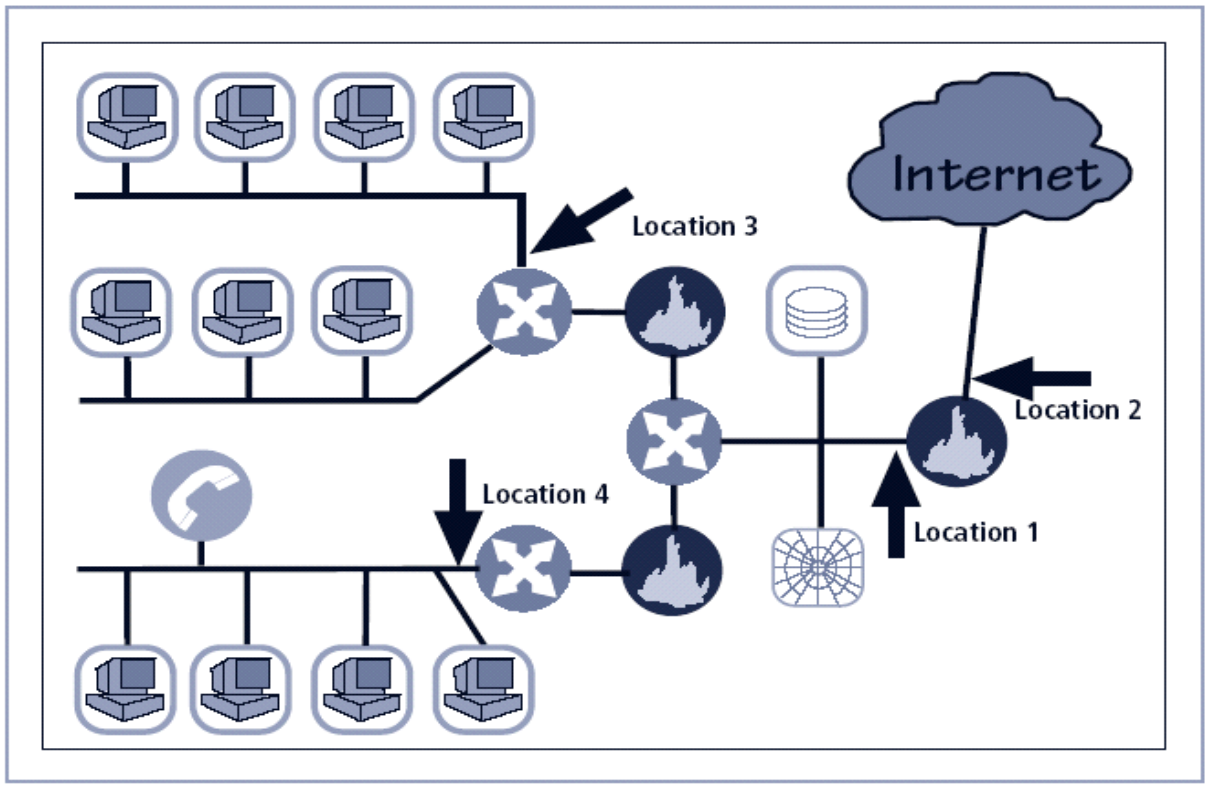


FIGURE 7-7 Network IDS Sensor Locations[17]

Deploying Host-Based IDSs

The proper implementation of HIDSs can be a painstaking and time-consuming task, as each HIDS must be custom configured to its host systems.

Deployment begins with implementing the most critical systems first.

Installation continues until either all systems are installed or the organization reaches the planned degree of coverage it is willing to live with, with regard to the number of systems or percentage of network traffic.

Just as technicians can install the HIDS in off-line systems to develop expertise and identify potential problems, users and managers can gain expertise and understanding of the operation of the HIDS by using a test facility.

Measuring IDSs' Effectiveness

IDSs are evaluated using two dominant metrics:

1. Administrators evaluate the number of attacks detected in a known collection of probes.
2. Administrators examine the level of use, commonly measured in megabits per second of network traffic, at which the IDSs fail

Honey Pots & Honey Nets

Honey pots are decoy systems designed to lure potential attackers away from critical systems and encourage attacks against themselves.

Honey nets are a collection of honey pots connecting several honey pot systems on a subnet.

Honey pots are designed to:

- Divert an attacker from accessing critical systems
- Collect information about the attacker's activity
- Encourage the attacker to stay on the system long enough for administrators to document the event and, perhaps, respond

Padded Cell Systems

- A padded cell is a honey pot that has been protected so that that it cannot be easily compromised.
- In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDS.
- When the IDS detects attackers, it seamlessly transfers them to a special simulated environment where they can cause no harm—the nature of this host environment is what gives the approach its name, padded cell.

Advantages:

- Attackers can be diverted to targets that they cannot damage.
- Administrators have time to decide how to respond to an attacker.
- Attackers' actions can be easily and more extensively monitored, and the records can be used to refine threat models and improve system protections.
- Honey pots may be effective at catching insiders who are snooping around a network.

Disadvantages:

- The legal implications of using such devices are not well defined.
- Honey pots and padded cells have not yet been shown to be generally useful security technologies.
- An expert attacker, once diverted into a decoy system, may become angry and launch a more hostile attack against an organization's systems.
- Administrators and security managers will need a high level of expertise to use these systems.

Trap and Trace Systems

Trap and trace systems use a combination of techniques to detect an intrusion and then to trace incidents back to their sources.

The trap usually consists of a honey pot or padded cell and an alarm. While the intruders are distracted, or trapped, by what they perceive to be successful intrusions, the system notifies the administrator of their presence.

The trace feature is a process by which the organization attempts to determine the identity of someone discovered in unauthorized areas of the network or systems.

If the individual is outside the security perimeter of the organization, then numerous legal issues arise.

There are more legal drawbacks to trap and trace.

The trap portion frequently involves the use of honey pots or honey nets.

When using honey pots and honey nets, administrators should be careful not to cross the line between enticement and entrapment.

- Enticement is the process of attracting attention to a system by placing tantalizing bits of information in key locations.
- Entrapment is the action of luring an individual into committing a crime to get a conviction.

Enticement is legal and ethical, whereas entrapment is not.

Active Intrusion Prevention

Some organizations implement active countermeasures to stop attacks. One tool that provides active intrusion prevention works by taking up the unused IP address space within a network.

If an address is not currently being used by a real computer or network device, LaBrea will pretend to be a computer at that IP address and allow the attacker to complete the connection request but then hold the connection open but inactive, allowing the system time to notify administrators about the anomalous behavior on the network.

Scanning and Analysis Tools

Scanning tools are typically used as part of an attack protocol to collect information that an attacker would need to launch a successful attack.

The attack protocol is a series of steps or processes used by an attacker, in a logical sequence, to launch an attack against a target system or network.

- **Fingerprinting:** systematic survey of all of target organization's Internet addresses collected during the footprinting phase
- Fingerprinting reveals useful information about internal structure and operational nature of target system or network for anticipated attack
- These tools are valuable to network defender since they can quickly pinpoint the parts of the systems or network that need a prompt repair to close the vulnerability

Port Scanners

Port scanning utilities (or port scanners) are tools used by both attackers and defenders to identify (or fingerprint) the computers that are active on a network, as well as the ports and services active on those computers, the functions and roles the machines are fulfilling, and other useful information.

These tools can scan for specific types of computers, protocols, or resources, or their scans can be generic.

The more specific the scanner is, the better it can give attackers and defenders information that is detailed and will be useful later. However, it is also recommended that you keep a generic, broad-based scanner in your toolbox as well.

Firewall Analysis Tools

There are several tools that automate the remote discovery of firewall rules and assist the administrator in analyzing the rules to determine exactly what they allow and what they reject.

Incidentally, administrators who feel wary of using the same tools that attackers use should remember:

1. Regardless of the nature of the tool that is used to validate or analyze a firewall's configuration, it is the intent of the user that will dictate how the information gathered will be used.
2. In order to defend a computer or network well, it is necessary to understand the ways it can be attacked.

Thus, a tool that can help close up an open or poorly configured firewall will help the network defender minimize the risk from attack.

Operating System Detection Tools

Detecting a target computer's OS is very valuable to an attacker, because once the OS is known, all of the vulnerabilities to which it is susceptible can easily be determined. There are many tools that use networking protocols to determine a remote computer's OS.

As most OSs have a unique way of responding to ICMP requests, these tools are very reliable in finding matches and thus detecting the OSs of remote computers.

System and network administrators should take note of this and plan to restrict the use of ICMP through their organization's firewalls and, when possible, within its internal networks.

Vulnerability Scanners

An "active" vulnerability scanner is one that initiates traffic on the network in order to determine security holes.

As a class, this type of scanner identifies exposed usernames and groups, shows open network shares, and exposes configuration problems and other vulnerabilities in servers.

A passive vulnerability scanner is one that listens in on the network and determines vulnerable versions of both server and client software.

Passive scanners are advantageous in that they do not require vulnerability analysts to get approval prior for testing.

These tools simply monitor the network connections to and from a server to gain a list of vulnerable applications.

Furthermore, passive vulnerability scanners have the ability to find client-side vulnerabilities that are typically not found in active scanners.

Packet Sniffers

A packet sniffer or network protocol analyzer is a network tool that collects copies of packets from the network and analyzes them.

It can provide a network administrator with valuable information for diagnosing and resolving networking issues.

In the wrong hands, a sniffer can be used to eavesdrop on network traffic.

Typically, to use these types of programs most effectively, the user must be connected to a network from a central location.

To use a packet sniffer legally, the administrator must:

1) Be on a network that the organization owns

2) Be under direct authorization of the owners of the network

3) Have knowledge and consent of the content creators

Wireless Security Tools

An organization that spends all of its time securing the wired network and leaves wireless networks to operate in any manner is opening itself up for a security breach.

As a security professional, you must assess the risk of wireless networks.

A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess the level of privacy or confidentiality afforded on the wireless network.

Access Control Devices

A successful access control system includes a number of components, depending on the system's needs for authentication and authorization.

Strong authentication requires at least two of the forms of authentication listed below to authenticate the supplicant's identity. When a second factor is required to verify the supplicant's identity, this is frequently a physical device.

The technology to manage authentication based on what a supplicant knows is widely integrated into the networking and security software systems in use across the IT industry.

Authentication

Authentication is the validation of a supplicant's identity.

There are four general ways in which authentication is carried out:

- What a supplicant knows
- What a supplicant has
- What a supplicant is
- What a supplicant produces

Effectiveness of Biometrics

Biometric technologies are evaluated on three basic criteria:

- The false reject rate: The rate at which supplicants who are authentic users are denied or prevented access to authorized areas as a result of a failure in the biometric device (Type I error).
- The false accept rate: The rate at which supplicants who are not legitimate users are allowed access to systems or areas as a result of a failure in the biometric device (Type II error).
- The crossover error rate (CER): The level at which the number of false rejections equals the false acceptances (Equal error rate).

This is the most common and important overall measure of the accuracy of a biometric system.

Acceptability of Biometrics

A balance must be struck between how acceptable a security system is to its users and how effective it is in maintaining security.

Many of the biometric systems that are highly reliable and effective are considered somewhat intrusive to users.

As a result, many information security professionals, in an effort to avoid confrontation and possible user boycott of the biometric controls, don't implement them.

TABLE 7-3 Ranking of Effectiveness and Acceptance[21]

Effectiveness of Biometric Authentication Systems—Ranked from Most Secure to Least Secure	Acceptance of Biometric Authentication Systems—Ranked from Most Accepted to Least Accepted
Retina pattern recognition	Keystroke pattern recognition
Fingerprint recognition	Signature recognition
Handprint recognition	Voice pattern recognition
Voice pattern recognition	Handprint recognition
Keystroke pattern recognition	Fingerprint recognition
Signature recognition	Retina pattern recognition

CRYPTOGRAPHY

INTRODUCTION

Although not a specific application or security tool, encryption represents a sophisticated approach to security that is implemented in many security systems.

In fact, many security-related tools use embedded encryption technologies to protect sensitive information handled by the application.

Encryption is the process of converting an original message into a form that is unreadable by unauthorized individuals, that is, anyone without the tools to convert the encrypted message back to its original format.

The science of encryption, known as cryptology, encompasses cryptography, from the Greek words kryptos, meaning hidden; graphein, meaning to write; and cryptanalysis, the process of obtaining the original message (or plaintext) from an encrypted message (or ciphertext), without the knowledge of the algorithms and keys used to perform the encryption.

Foundations of Cryptology

- With emergence of technology, need for encryption in information technology environment greatly increased
- All popular Web browsers use built-in encryption features for secure e-commerce applications

Encryption Definitions

Algorithm: The mathematical formula used to convert an unencrypted message into an encrypted message.

Cipher: The transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components.

Ciphertext or cryptogram: The unintelligible encrypted or encoded message resulting from an encryption.

Code: The transformation of the larger components (words or phrases) of an unencrypted message into encrypted components.

Cryptosystem: The set of transformations necessary to convert an unencrypted message into an encrypted message.

Decipher: To decrypt or convert ciphertext to plaintext.

Encipher: To encrypt or convert plaintext to ciphertext.

Key or cryptovariable: The information used in conjunction with the algorithm to create ciphertext from plaintext.

Keyspace: The entire range of values that can possibly be used to construct an individual key.

Link encryption: A series of encryptions and decryptions between a number of systems, whereby each node decrypts the message sent to it and then reencrypts it using different keys and sends it to the next neighbor, until it reaches the final destination.

Plaintext: The original unencrypted message that is encrypted and results from successful decryption.

Steganography: The process of hiding messages in a picture or graphic.

Work factor: The amount of effort (usually in hours) required to perform cryptanalysis on an encoded message.

CIPHER METHODS

The notation used to describe the encryption process differs depending on the source.

The first uses the letters M to represent the original message, C to represent the ending ciphertext, and E to represent the encryption process: E(M) = C.

This formula represents the application of encryption to a message to create ciphertext. D represents the decryption or deciphering process, thus D[E(M)]=M.

K is used to represent the key, thus E(M, K) = C, or encrypting the message with the key results in the ciphertext.

Now look at a simple form of encryption based on two concepts: the block cipher and the exclusive OR operation.

With the block cipher method, the message is divided into blocks, i.e., 8- or 16-bit blocks, and then each block is transformed using the algorithm and key.

The exclusive OR operation (XOR) is a function of Boolean algebra whereby two bits are compared, and if the two bits are identical, the result is a binary 0. If the two bits are NOT the same, the result is a binary 1.

Encryption Operations

In encryption, the most commonly used algorithms include two functions: substitution and transposition.

In a substitution cipher, you substitute one value for another.

This is a simple enough method by itself but very powerful if combined with other operations. This type of substitution is based on a monoalphabetic substitution, since it only uses one alphabet.

More advanced substitution ciphers use two or more alphabets and are referred to as polyalphabetic substitutions.

Caesar reportedly used a three-value shift to the right, giving that particular substitution cipher his name–the "Caesar Cipher."

Just like the substitution operation, the transposition cipher is simple to understand but can be complex to decipher if properly used.

Unlike the substitution cipher, the transposition cipher (or permutation cipher) simply rearranges the values within a block to create the ciphertext.

This can be done at the bit level or at the byte (character) level.

Transposition ciphers move these bits or bytes to another location in the block, so that bit 1 becomes bit 4, bit 2 becomes bit 7, etc.

Transposition Cipher Method

The transposition cipher (or permutation cipher) simply rearranges the values within a block to create the ciphertext

This can be done at the bit level or at the byte (character) level. Transposition ciphers move these bits or bytes to another location in the block, so that bit 1 becomes bit 4, bit 2 becomes bit, 7 etc.

TABLE 8-3 Exclusive OR Operations

Bit 1	Bit 2	Exclusive OR result
0	0	0
0	1	1
1	0	1
1	1	0

Vernam Cipher

Also known as the one-time pad, the Vernam cipher was developed at AT&T and uses a one-use set of characters, the value of which is added to the block of text.

The resulting sum is then converted to text.

When the two are added, if the values exceed 26, 26 is subtracted from the total (Modulo 26). The corresponding results are then converted back to text.

Hash Functions

Hash algorithms are publicly known functions that create a hash value, also known as a message digest, by converting variable-length messages into a single fixed-length value.

The message digest is a *fingerprint* of the author's message that is to be compared with the receiver's locally calculated hash of the same message.

Hashing functions do not require the use of keys, but a message authentication code (MAC), which is essentially a one-way hash value that is encrypted with a symmetric key. The recipients must possess the key to access the message digest and to confirm message integrity.

Cryptographic Algorithms

In general, cryptographic algorithms are often grouped into two broad categories—symmetric and asymmetric—but in practice, today's popular cryptosystems use a hybrid combination of symmetric and asymmetric algorithms.

Symmetric and asymmetric algorithms can be distinguished by the types of keys they use for encryption and decryption operations.

Symmetric Encryption

Symmetric encryption indicates that the same key, also known as a secret key, is used to conduct both the encryption and decryption of the message.

Symmetric encryption methods can be extremely efficient, requiring minimal processing to either encrypt or decrypt the message.

The problem is that both the sender and the receiver must own the encryption key.

If either copy of the key is compromised, an intermediate can decrypt and read the messages.

One of the challenges of symmetric key encryption is getting a copy of the key to the receiver, a process that must be conducted out-of-band to avoid interception.

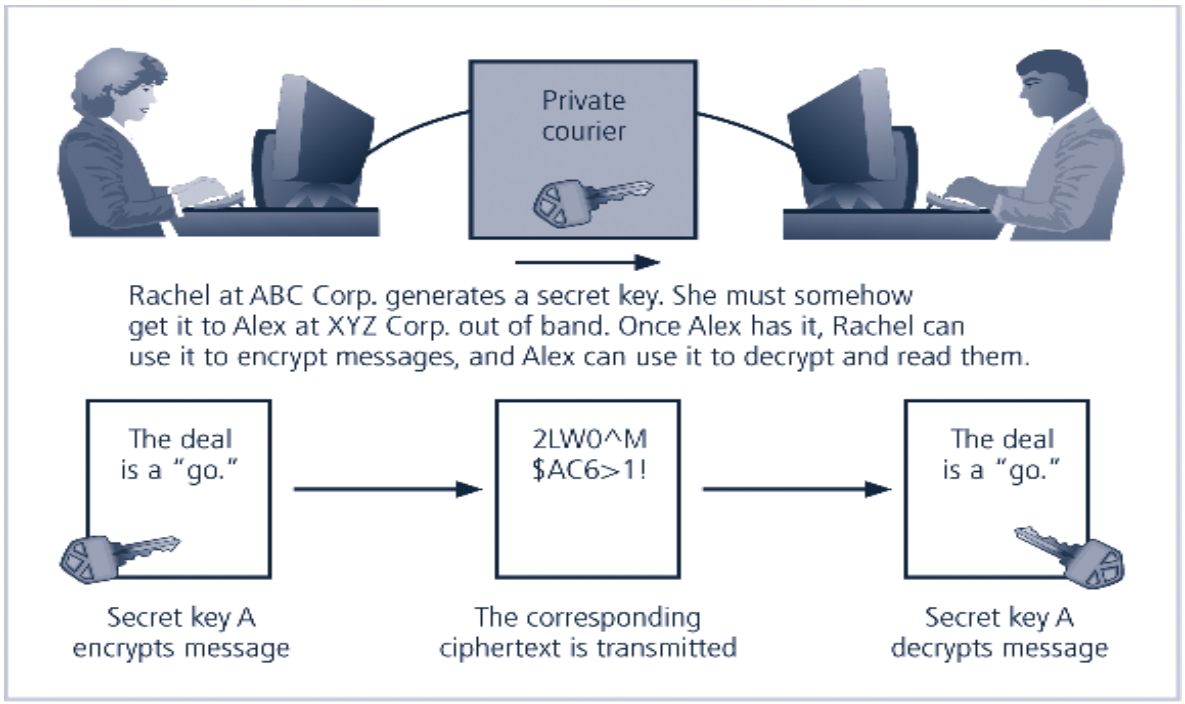


FIGURE 8-3 Example of Symmetric Encryption

There are a number of popular symmetric encryption cryptosystems.

One of the most familiar is **Data Encryption Standard (DES),** developed in 1977 by IBM and based on the Data Encryption Algorithm (DEA).

DEA uses a 64-bit block size and a 56-bit key. The algorithm begins by adding parity bits to the key (resulting in 64 bits) and then apples the key in 16 rounds of XOR, substitution, and transposition operations.

With a 56-bit key, the algorithm has 256 possible keys to choose from (over 72 quadrillion).

DES is a federally approved standard for non-classified data. DES was cracked in 1997 when **Rivest-Shamir-Aldeman (RSA)** put a bounty on the algorithm.

RSA offered a $10,000 reward for the first person or team to crack the algorithm. Fourteen thousand users collaborated over the Internet to finally break the encryption.

Asymmetric Encryption

Another category of encryption techniques is asymmetric encryption, also known as public-key encryption.

Whereas the symmetric encryption systems are based on a single key to both encrypt and decrypt a message, asymmetric encryption uses two different keys.

Either key can be used to encrypt or decrypt the message. However, if Key A is used to encrypt the message, only Key B can decrypt, and if Key B is used to encrypt a message, only Key A can decrypt it.

The public key is stored in a public location, where anyone can use it.

The private key, as its name suggests, is a secret known only to the owner of the key pair.

The problem with asymmetric encryption is that it requires four keys to hold a single conversation between two parties.

Asymmetric encryption is not as efficient as symmetric encryptions in terms of CPU computations.

As a result, the hybrid system described in the section on Public Key Infrastructure is more commonly used, instead of a pure asymmetric system.

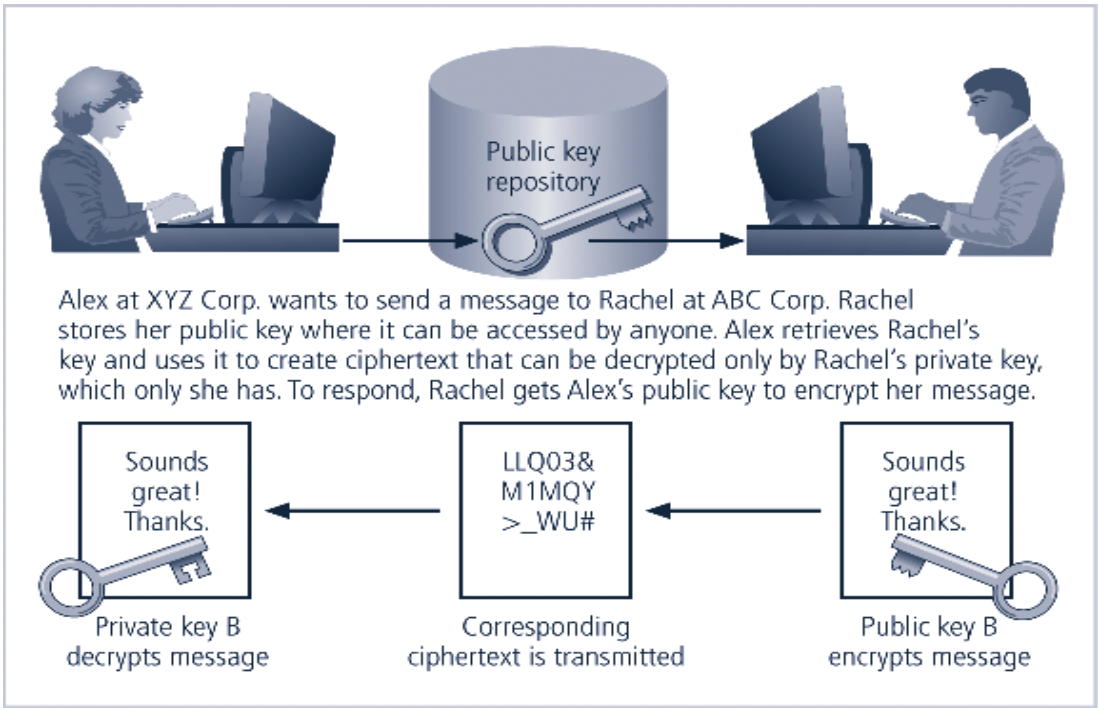


FIGURE 8-4 Example of Asymmetric Encryption

Encryption Key Size

When using ciphers, one of the decisions that has to be made is the size of the cryptovariable or key. The strength of many encryption applications and cryptosystems is measured by key size.

When it comes to cryptosystems, the security of encrypted data is not dependent on keeping the encrypting algorithm secret; in fact, algorithms are often published, so that research to uncover their weaknesses can be done.

The security of any cryptosystem depends on keeping some or all of the elements of the cryptovariable(s) or key(s) secret.

TABLE 8-7 Encryption Key Power

Number of Bits in Key	Odds of Cracking: 1 in	Estimated Time to Crack*
8	256	.000032 seconds
16	65,536	.008192 seconds
24	16,777,216	2.097 seconds
32	4,294,967,296	8 minutes 56.87 seconds
56	72,057,594,037,927,900	285 years 32 weeks 1 day
64	18,446,744,073,709,600,000	8,090,677,225 years
128	3.40282E+38	5,257,322,061,209,440,000,000 years
256	1.15792E+77	2,753,114,795,116,330,000,000,000,000, 000,000,000,000,000,000,000 years
512	1.3408E+154	608,756,305,260,875,000,000,000,000,000, 000,000,000,000,000,000,000,000,000,000, 000,000,000,000,000,000,000,000,000,000, 000,000,000 years

[NOTE]*Estimated Time to Crack is based on a general-purpose personal computer performing eight million guesses per second.

Cryptography Tools

Public Key Infrastructure (PKI) is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely.

PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs).

PKI Protects Information Assets in Several Ways:

Authentication. Digital certificates in a PKI system permit parties to validate the identity of other parties in an Internet transaction.

Integrity. A digital certificate demonstrates that the content signed by the certificate has not been altered while being moved from server to client.

Privacy. Digital certificates keep information from being intercepted during transmission over the Internet.

Authorization. Digital certificates issued in a PKI environment can replace user IDs and passwords, enhance security, and reduce some of the overhead required for authorization processes and controlling access privileges.

Nonrepudiation. Digital certificates can validate actions, making it less likely that customers or partners can later repudiate a digitally signed transaction.

Digital Signatures

An interesting thing happens when the asymmetric process is reversed, that is, the private key is used to encrypt a short message.

The public key can be used to decrypt it, and the fact that the message was sent by the organization that owns the private key cannot be refuted.

This is known as nonrepudiation, which is the foundation of digital signatures.

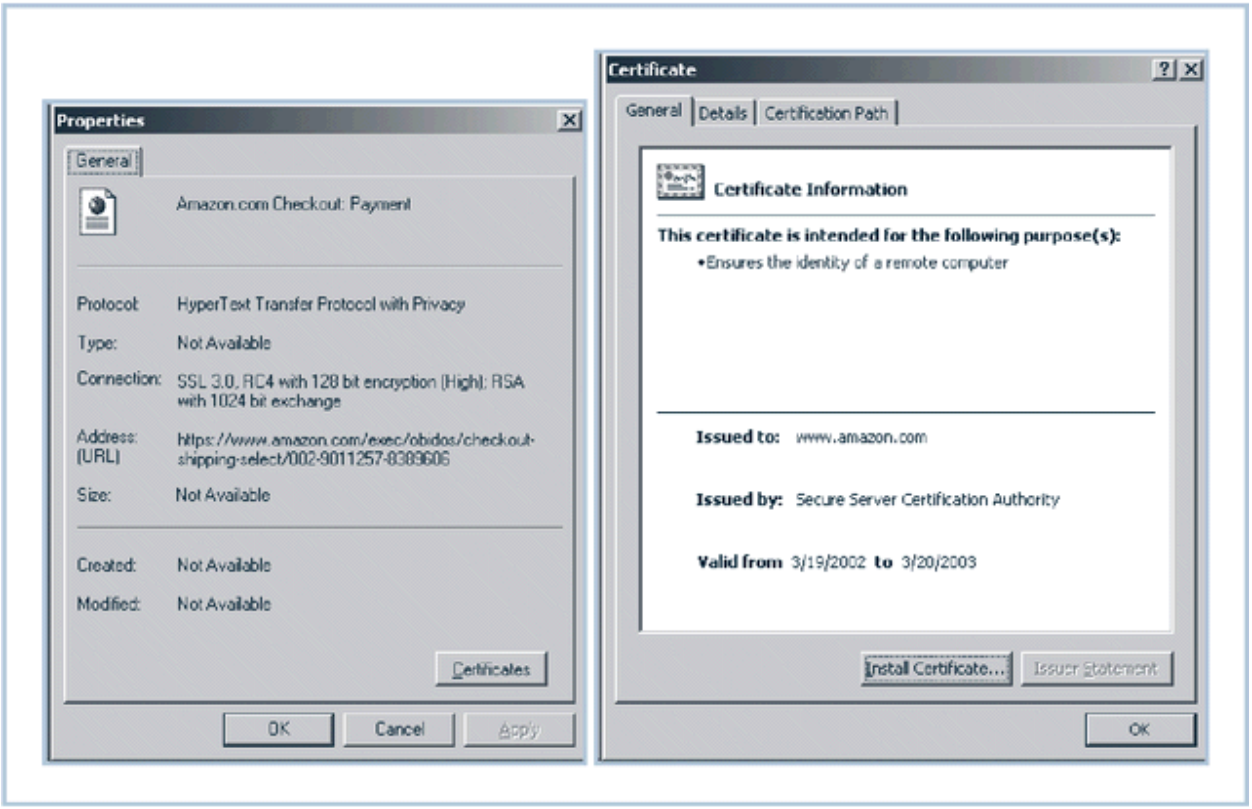
Digital signatures are encrypted messages that are independently verified by a central facility (registry) as authentic.

Digital Certificates and Certificate Authorities

As alluded to earlier, a digital certificate is an electronic document, similar to a digital signature, attached to a file certifying that this file is from the organization it claims to be from and has not been modified from the originating format.

A certificate authority is an agency that manages the issuance of certificates and serves as the electronic notary public to verify their worth and integrity.

Below diagram shows digital certificates



Hybrid Systems

In practice, asymmetric key encryption is not widely used except in the area of certificates. Instead, it is more often used in conjunction with symmetric key encryption creating a hybrid system.

The current process is based on the Diffie-Hellman Key Exchange method, which is a way to exchange private keys without exposure to any third parties using public key encryption.

With this method, asymmetric encryption is used as a method to exchange symmetric keys so that two organizations can conduct quick, efficient, secure communications based on symmetric encryption.

Diffie-Hellman provided the foundation for subsequent developments in public key encryption.

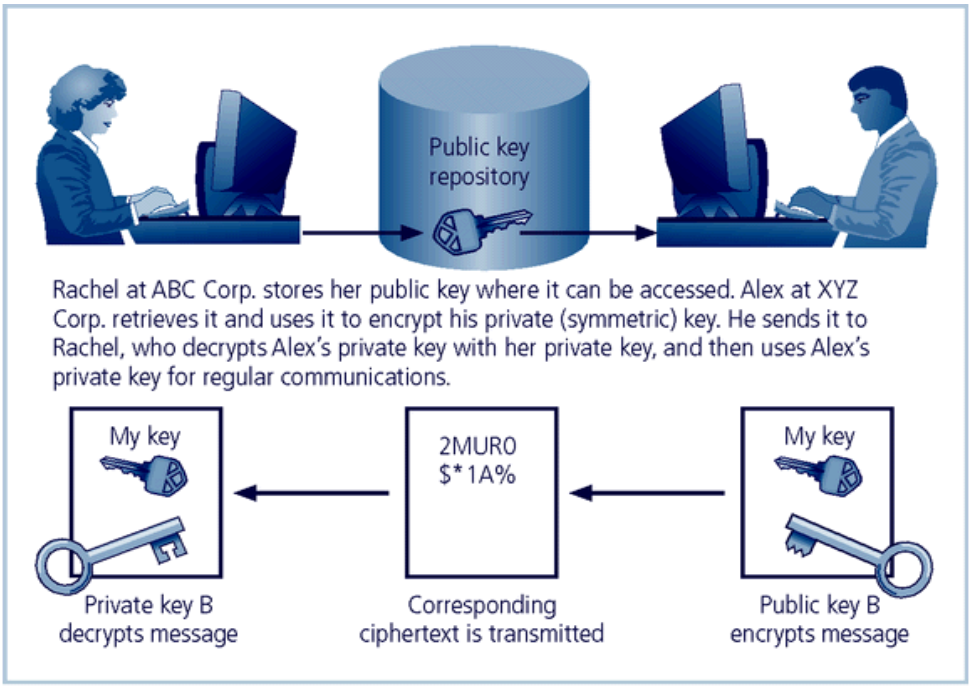


FIGURE 8-17 Hybrid Encryption Example

Steganography

Steganography is a process of hiding information and has been in use for a long time.

The word "steganography" is derived from the Greek words steganos meaning "covered" and graphein meaning "to write."

The most popular modern version of steganography involves hiding information within files that appear to contain digital pictures or other images.

Most computer graphics standards use a combination of three color values (red, blue, and green (RGB)) to represent a picture element, or pixel.

Each of the three color values usually requires an 8-bit code for that color's intensity (e.g., 00000000 for no red and 11111111 for maximum red).

This inability to perceive difference on the part of humans provides the steganographer with one bit per color (or three bits per pixel) to use for encoding data into an image file.

Some applications are capable of hiding messages in .bmp, .wav, .mp3, and .au files, as well as in unused storage space on CDs and DVDs.

Securing the Web

Secure Electronic Transactions (SET) was developed by MasterCard and Visa in 1997 to provide protection from electronic payment fraud.

SET works by encrypting the credit card transfers with DES for encryption and RSA for key exchange, much as other algorithms do.

SET provides the security for both Internet-based credit card transactions and the encryption of swipe systems of those credit cards in retail stores.

Secure Socket Layer was developed by Netscape in 1994 to provide security in online electronic commerce transactions.

It uses a number of algorithms but mainly relies on RSA for key transfer and IDEA, DES, or 3DES for encrypted symmetric key-based data transfer.

Secure Hypertext Transfer Protocol (SHTTP) is an encrypted solution to the unsecured version of HTTP.

It provides an alternative to the aforementioned protocols and can provide secure e-commerce transactions as well as encrypted Web pages for secure data transfer over the Web, using a number of different algorithms.

Secure Shell (SSH) provides security over remote access connections using tunneling. It provides authentication services between a client and server.

IP Security (IPSec) is the cryptographic authentication and encryption product of the IETF's IP Protocol Security Working Group, defined in RFC 1825, 1826 and 1827.

IP Security (IPSec) is used to create virtual private networks (VPNs) and is an open framework for security development within the TCP/IP family of protocol standards.

Securing E-mail

A number of encryption cryptosystems have been adapted in an attempt to inject some degree of security into e-mail, a notoriously unsecured medium.

S/MIME builds on the Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication through digital signatures based on public key cryptosystems.

Privacy Enhanced Mail (PEM) was proposed by the Internet Engineering Task Force (IETF) as a standard to function with the public-key cryptosystems.

PEM uses 3DES symmetric key encryption and RSA for key exchanges and digital signatures.

Pretty Good Privacy (PGP) was developed by Phil Zimmerman and uses the IDEA Cipher, a 128-bit symmetric key block encryption algorithm with 64-bit blocks for message encoding.

IDEA performs eight rounds on 16-bit sub-blocks using algebraic calculations.

PGP also uses RSA for symmetric key exchange and for digital signatures.

Securing Web Transactions with SET, SSL, and S-HTTP

Just as PGP, PEM, and S/MIME work to secure e-mail operations, a number of related protocols work to secure Web browsers, especially at electronic commerce sites.

Among these are Secure Electronic Transactions (SET), Secure Socket Layer (SSL), Secure Hypertext Transfer Protocol (S-HTTP), Secure Shell (SSH-2), and IP Security (IPSec).

Secure Electronic Transactions (SET) was developed by MasterCard and VISA in 1997 to provide protection from electronic payment fraud.

SET uses DES to encrypt credit card information transfers and RSA for key exchange. SET provides the security for both Internet-based credit card transactions and credit card swipe systems in retail stores.

IPSec

IPSec combines several different cryptosystems including:

- Diffie-Hellman key exchange for deriving key material between peers on a public network
- Public-key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties
- Bulk encryption algorithms, such as DES, for encrypting the data
- Digital certificates signed by a certificate authority to act as digital ID cards.

IPSec includes:

1) The IP Security Protocol itself, which defines the information to add to an IP packet, as well as how to encrypt packet data

2) The Internet Key Exchange, which uses asymmetric-based key exchange and negotiates the security associations.

PGP

Pretty Good Privacy (PGP) is a hybrid cryptosystem originally designed in 1991 by Phil Zimmermann.

PGP combined some of the best available cryptographic algorithms to become the open source *de facto* standard for encryption and authentication of e-mail and file storage applications.

Both freeware and low-cost commercial versions of PGP are available for a wide variety of platforms.

The PGP security solution provides six services: authentication by digital signatures, message encryption, compression, e-mail compatibility, segmentation, and key management.

Attacks on Cryptosystems

Historically, attempts to gain unauthorized access to secure communications have used brute force attacks.

Ciphertext attacks involve a hacker searching for a common text structure, wording, or syntax in the encrypted message that can enable him or her to calculate the number of each type of letter used in the message.

Frequency analysis can be used along with published frequency of occurrence patterns of various languages and can allow an experienced attacker to crack almost any code quickly if the individual has a large enough sample of the encoded text.

To protect against this, modern algorithms attempt to remove the repetitive and predictable sequences of characters from the ciphertext.

Occasionally, an attacker may obtain duplicate texts, one in ciphertext and one in plaintext, which enable the individual to reverse-engineer the encryption algorithm in a known-plaintext attack scheme.

Alternatively, an attacker may conduct a selected-plaintext attack by sending the potential victim a specific text that they are sure the victim will forward on to others.

Man-in-the-Middle Attack

A man-in-the-middle attack is designed to intercept the transmission of a public key or even to insert a known key structure in place of the requested public key.

From the perspective of the victims of such attacks, their encrypted communication appears to be occurring normally, but in fact the attacker is receiving each encrypted message and decoding it and then encrypting and sending it to the originally intended recipient.

Establishment of public keys with digital signatures can prevent the traditional man-in-the-middle attack, as the attacker cannot duplicate the signatures.

Correlation Attacks

Correlation attacks are a collection of brute-force methods that attempt to deduce statistical relationships between the structure of the unknown key and the ciphertext that is the output of the cryptosystem.

Differential and linear cryptanalysis, both of which are advanced methods of breaking codes, have been used to mount successful attacks on block cipher encryptions such as DES.

The only defense against this kind of attack is the selection of strong cryptosystems that have stood the test of time, thorough key management, and strict adherence to the best practices of cryptography in the frequency of changing keys.

Dictionary Attacks

In a **dictionary attack**, the attacker encrypts every word in a dictionary using the same cryptosystem as used by the target.

Dictionary attacks can be successful when the ciphertext consists of relatively few characters, as for example files that contain encrypted usernames and passwords.

After a match is located, the attacker has essentially identified a potential valid password for the system under attack.

Timing Attacks

In a timing attack, the attacker eavesdrops during the victim's session and uses statistical analysis of the user's typing patterns and inter-keystroke timings to discern sensitive session information.

While timing analysis may not directly result in the decryption of sensitive data, it can be used to gain information about the encryption key and perhaps the cryptosystem in use.

Once the attacker has successfully broken an encryption, he or she may launch a replay attack, which is an attempt to resubmit a recording of the deciphered authentication to gain entry into a secure source.

Defending From Attacks

No matter how sophisticated encryption and cryptosystems have become, however, they have retained the same flaw that the first systems contained thousands of years ago: if you discover the key, you can determine the message.

Thus, key management is not so much the management of technology but rather the management of people.