UNIT IV

INTRUSION DETECTION AND PREVENTION SYSTEMS

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."

Why Use an IDS?

The reasons to 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 IDP

IDSs operate as network-based, host-based, or application-based systems. A network-based IDS is focused on protecting network information assets. 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

1. Network-based IDPSs

- A network-based IDPS (NIDPS) 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 NIDPS 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 it looks for the exchange of a series of related packets in a certain pattern, which could indicate that a port scan is in progress.
- NIDPSs 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 NIDPS can be deployed to watch a specific grouping of host computers on a specific network segment, or it can be installed to monitor all traffic between the systems that make up an entire network.
- To determine whether or not an attack has occurred or may be underway, NIDPSs look for attack patterns by comparing measured activity to known signatures in their knowledge base.
- This is accomplished by the comparison of 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 NIDPSs

- Good network design and placement of NIDPS devices can enable an organization to use a few devices to monitor a large network.
- NIDPSs are usually passive devices and can be deployed into existing networks with little or no disruption to normal network operations.
- NIDPSs are not usually susceptible to direct attack and, in fact, may not be detectable by attackers.

Disadvantages of NIDPS

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

2. Host-Based IDPS

- A host-based IDPS (HIDPS) resides on a particular computer or server, known as the host, and monitors activity only on that system.
- HIDPSs 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 HIDPSs work on the principle of configuration or change management, which means they record the sizes, locations, and other attributes of system files. The HIDPS then triggers an alert when one of the following changes occurs: file attributes change; new files are created; or existing files are deleted.
- A HIDPS has an advantage over NIDPS 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 HIDPS relies on the classification of files into various categories and then applies various notification actions, depending on the rules in the HIDPS configuration.
- Managed HIDPSs can monitor multiple computers simultaneously by creating a configuration file on each monitored host and by making each HIDPS report back to a master console system, which is usually located on the system administrator's computer.

Advantages of HIDPSs

- A HIDPS can detect local events on host systems and also detect attacks that may elude a network-based IDPS.
- A HIDPS 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 HIDPS.
- A HIDPS can detect inconsistencies in how applications and systems programs were used by examining the records stored in audit logs.

Disadvantages of HIDPSs

- HIDPSs pose more management issues since they are configured and managed on each monitored host. A HIDPS is vulnerable both to direct attacks and to attacks against the host operating system.
- A HIDPS 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 HIDPS is susceptible to some denial-of-service attacks.
- A HIDPS can use large amounts of disk space to retain the host OS audit logs, and to function properly, it may require disk capacity to be added to the system.
- A HIDPS can inflict a performance overhead on its host systems, and in some cases, may reduce system performance below acceptable levels.

IDPS Detection Methods

IDPSs use a variety of detection methods to monitor and evaluate network traffic. Three methods dominate: the signature-based approach, the statistical-anomaly approach, and the stateful packet inspection approach.

1. **Signature-based IDSs**

- A signature-based IDS (also known as a knowledge-based IDS) examines data traffic in search of patterns that match known signatures—that is, 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.

2. **Statistical anomaly-based IDSs**

- The statistical anomaly-based IDS (stat IDS) or behavior-based IDS collects statistical summaries by observing traffic that is known to be normal. This normal period of evaluation establishes a performance baseline.
- Once the baseline is established, the stat IDS will periodically sample network activity, and, using statistical methods, compare the sampled network activity to this baseline. When the measured activity is outside the baseline parameters, it is said to exceed the clipping level, and 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, because 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.

3. Stateful protocol analysis IDPSs

- According to SP 800-94, “Stateful protocol analysis (SPA) is a process of comparing predetermined profiles of generally accepted definitions of benign activity for each protocol state against observed events to identify deviations. Stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used.”
- By storing relevant data detected in a session and then using that data to identify intrusions that involve multiple requests and responses, the IDPS can better detect specialized, multisession attacks. This process is sometimes called deep packet inspection because SPA closely examines packets at the application layer for information that indicates a possible intrusion.
- The analytical complexity of session-based assessments is the principal drawback to this type of IDPS method, which is further complicated by the amount of processing overhead in tracking multiple, simultaneous connections.
- Additionally, unless the protocol violates its fundamental behavior, this type of IDPS method may completely fail to detect the intrusion. One final issue is the possibility that the IDPS may in fact cause problems with the protocol it is examining, especially with client- and server-differentiated operations.

4. Log file monitors

- Similar to a NIDS, a log file monitor (LFM) 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.

IDPS 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: 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.

The following are some of the responses that an IDS can be configured to produce.

- Audible / visual alarms

  The IDPS can trigger a .wav file, beep, whistle, siren, or other audible or visual notification to alert the administrator of an attack. The most common type of such notifications is the computer pop-up.
- SNMP traps and plug-ins

  The Simple Network Management Protocol contains trap functions, which allow a device to send a message to the SNMP management console indicating that a certain threshold has been crossed, either positively or negatively. The IDPS can execute this trap, telling the SNMP console an event has occurred.
- E-mail messages

  The IDPS can send e-mail to notify network administrators of an event. Many administrators use smartphones and other e-mail enabled devices to check for alerts and other notifications frequently.
- Pager or phone messages

  The IDPS can be configured to dial a phone number and produce an alphanumeric page or a modem noise.
- Log entries

  The IDPS can enter information about the event (e.g., addresses, time, sys- tems involved, protocol information) into an IDPS system log file or operating system log file.
- Evidentiary packet dumps

  Organizations that require an audit trail of the IDPS data may choose to record all log data in a special way. This method allows the organiza- tion to perform further

analysis on the data and also to submit the data as evidence in a civil or criminal case.

- Take action against the intruder

  It has become possible, although not advisable, to take action against an intruder. Known as trap-and-trace, back-hacking, or traceback, this response option involves configuring intrusion detection systems to trace the data from the target system to the attacking system in order to initiate a counterattack.
- Launch program

  An IDPS can be configured to execute a specific program when it detects specific types of attacks
- Reconfigure firewall

  An IDPS can send a command to the firewall to filter out sus- pected packets by IP address, port, or protocol.
- Terminate session

  Terminating the session by using the TCP/IP protocol specified packet TCP close is a simple process.
- Terminate connection

  The last resort for an IDPS under attack is to terminate the organization's internal or external connections.

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.

1. Technical and policy considerations

   - What is your systems environment?
   - What are the technical specifications of your systems environment?
   - What are the technical specifications of your current security protections?

- What are the goals of your enterprise?
- How formal is the systems environment and management culture in your organization?
- What are your security goals and objectives?
- Is the primary concern of your organization to be protected from threats that originate outside of your organization?
- Is your organization concerned about insider attacks?
- Does your organization want to use the output of your IDS to determine new needs?
- Does your organization want to use an IDS to maintain managerial control over network usage?
- What is your existing security policy?
- How is it structured?
- What are the general job descriptions of your system users?
- Does the policy include reasonable use policies or other management provisions?
- Has your organization defined processes for dealing with specific policy violations?

2. Organizational requirements and constraints

- What are the requirements that are levied from outside the organization?
- Is your organization subject to oversight or review by another organization?
- Are there requirements for public access to information on your organization'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 organization have authority to instigate changes based on the findings of an IDS?

3. Product features and quality of IDPSs

- 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?
- What additional training resources are available from the vendor and at what cost?

Strengths and Limitations of IDPSs

Intrusion detection systems perform the following functions well:

- Monitoring and analysis of system events and user behaviors
- Testing the security states of system configurations
- Baselining the security state of a system, and then tracking any changes to that baseline
- Recognizing patterns of system events that correspond to known attacks
- Recognizing patterns of activity that statistically vary from normal activity
- Managing operating system audit and logging mechanisms and the data they generate
- Alerting appropriate staff by appropriate means when attacks are detected
- Measuring enforcement of security policies that are encoded in the analysis engine
- Providing default information security policies
- Allowing non-security experts to perform important security monitoring functions

Intrusion detection systems cannot perform the following functions:

- Compensating for weak or missing security mechanisms in the protection infrastructure
- Instantaneously detecting, reporting, and responding to an attack when there is a heavy network or processing load
- Detecting newly published attacks or variants of existing attacks
- Effectively responding to attacks launched by sophisticated attackers
- Automatically investigating attacks without human intervention
- Resisting attacks that are intended to defeat or circumvent them
- Compensating for problems with the fidelity of information sources
- Dealing effectively with switched networks

Deployment and Implementation of an IDPS

Deploying and implementing an IDPS, which is not always a straightforward task. The strategy for deploying an IDPS should consider a number of factors, the foremost being how the IDPS will be managed and where it should be placed.

IDPS control strategies

An IDS can be implemented using 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:

- A centralized IDS control strategy implements and manages all IDS control functions in a central location.
- A fully distributed IDS control strategy distributes all control functions that are applied at the physical location of each IDS component.
- A partially distributed IDS control strategy combines the best of the other two strategies. 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.

Deployment of IDPSs

- 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 that integrates with the organization's existing IT infrastructure but, at the same time, causes minimal impact.
- NIDSs and HIDSs can be used in tandem to cover both the individual systems that connect to an organization's networks and the networks themselves.

1. **Deploying network-based IDPSs.**

    - NIST recommends four locations for NIDS sensors as described below.
        - 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.
- This location allows organizations with limited resources to focus these resources on the network assets that have the greatest value.

2. Deploying host-based IDPSs

- The proper implementation of HIDPSs can be a painstaking and time-consuming task, as each HIDPS 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 HIDPS in off-line systems to develop expertise and identify potential problems, users and managers can gain expertise and understanding of the operation of the HIDPS by using a test facility.

Measuring the effectiveness of IDPSs

- IDPSs are evaluated using four dominant metrics:
    - Thresholds
    - Blacklists and whitelists
    - Alert settings
    - Code viewing and editing
- An evaluation of an IDS might read something like this: At 100 Mb/s, the IDS was able to detect 97% of directed attacks.
- Since developing this collection can be tedious, most IDS vendors provide testing mechanisms that verify that their systems are performing as expected. Some of these testing processes will enable the administrator to:
    - Record and retransmit packets from a real virus or worm scan.
    - Record and retransmit packets from a real virus or worm scan with incomplete TCP/IP session connections (missing SYN packets).
    - Conduct a real virus or worm scan against an invulnerable system.

HONEYPOTS, HONEYNETS, AND PADDED CELL SYSTEMS

Honeypots are decoy systems designed to lure potential attackers away from critical systems. By encouraging attacks against these bait systems, the defender may lure them away from actual targets and perhaps detect their presence and then block access. This approach has the risk of perhaps luring attackers into the defender's network.

Honey nets are a collection of honeypots that connect several honeypot systems on a subnet. Honeypots 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

A padded cell is a honeypot 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 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.

The advantages of honeypots, honeynets, and padded cell systems

- 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.
- Honeypots may be effective at catching insiders who are snooping around a network.

The disadvantages of honeypots, honeynets, and padded cell systems

- The legal implications of using such devices are not well defined.
- Honeypots 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

A trap and trace systems use a combination of techniques to detect an intrusion and 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 who is discovered in unauthorized areas of the network or system. If the individual is outside the security perimeter of the organization, then numerous legal issues arise.

The 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 is known as LaBrea. LaBrea 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, known as the three-way handshake. Once the handshake is complete, LaBrea will change the TCP sliding window size down to a low number to hold the TCP connection from the attacker open for many hours, days, or even months. Holding the connection open but inactive greatly slows down network-based worms and other attacks. It allows the LaBrea system time then to notify the system and network administrators about the anomalous behavior on the network.

SCANNING AND ANALYSIS TOOLS

In order to secure a network, it is imperative that someone in the organization knows exactly where the network needs securing. To truly assess the risk within a computing environment, one must deploy technical controls using a strategy of defense in depth. Scanner and analysis tools can find vulnerabilities in systems, holes in security components, and unsecured aspects of the network. Therefore, they can be invaluable to security

administrators because they enable administrators to see what the attacker sees. 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.

Footprinting is one of the preparatory parts of an attack.

- Footprinting is the organized research of the Internet addresses owned or controlled by a target organization.
- The attacker uses public Internet data sources to perform keyword searches to identify the network addresses of the organization.
- To assist in the footprint intelligence collection process, an enhanced Web scanner can be used.

Fingerprinting

- The next phase of the attack is a second intelligence or data-gathering process called fingerprinting.
- Fingerprinting is a systematic survey of all of the target organization's Internet addresses (which were collected during the footprinting phase) to ascertain the network services offered by the hosts in that range.

Fingerprinting reveals useful information about the internal structure and operational nature of the target system or network for the anticipated attack. Since these tools were created to find vulnerabilities in systems and networks, they are valuable for the 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), which 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 that are 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. It is also recommended that you keep a generic, broad-based scanner in your toolbox as well.

Firewall Analysis Tools

Several tools 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. Administrators who feel wary of using the same tools that attackers use should remember:

- 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.
- 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 has 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 ICMPs 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 to 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. A packet sniffer 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:

- Be on a network that the organization owns
- Be under direct authorization of the owners of the network
- 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, which should include the ability to sniff wireless traffic, scan wireless hosts, and assess the level of privacy or confidentiality afforded on the wireless network.

Biometric Access Controls

Biometric authentication technologies include the following:

- Fingerprint comparison of the supplicant's actual fingerprint to a stored fingerprint
- Palm print comparison of the supplicant's actual palm print to a stored palm print

- Hand geometry comparison of the supplicant's actual hand to a stored measurement
- Facial recognition using a photographic ID card, in which a human security guard compares the supplicant's face to a photo
- Facial recognition using a digital camera, in which a supplicant's face is compared to a stored image
- Retinal print comparison of the supplicant's actual retina to a stored image
- Iris pattern comparison of the supplicant's actual iris to a stored image

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 number of 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, do not implement them.

FOUNDATIONS OF CRYPTOLOGY

- Cryptology has a long and multicultural history
- 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

Terminology

- Cryptology: science of encryption; combines cryptography and cryptanalysis
- Cryptography: process of making and using codes to secure transmission of information
- Cryptanalysis: process of obtaining original message from encrypted message without knowing algorithms
- Encryption: converting original message into a form unreadable by unauthorized individuals
- Decryption: the process of converting the ciphertext message back into plaintext
- Algorithm: The programmatic steps used to convert an unencrypted message into an encrypted sequence of bits that represent the message; sometimes refers to the programs that enable the cryptographic processes
- Cipher or cryptosystem: An encryption method or process encompassing the algorithm, key(s) or cryptovariable(s), and procedures used to perform encryption and decryption
- Ciphertext or cryptogram: The encoded message resulting from an encryption
- Code: The process of converting components (words or phrases) of an unencrypted message into encrypted components
- Decipher: To decrypt, decode, or convert, ciphertext into the equivalent plaintext
- Encipher: To encrypt, encode, or convert, plaintext into the equivalent ciphertext
- Key or cryptovariable: The information used in conjunction with an algorithm to create the ciphertext from the plaintext or derive the plaintext from the ciphertext; the key can be a series of bits used by a computer program, or it can be a passphrase used by humans that is then converted into a series of bits used by a computer program
- Keyspace: The entire range of values that can be used to construct an individual key

- Link encryption: A series of encryptions and decryptions between a number of systems, wherein each system in a network decrypts the message sent to it and then reencrypts it using different keys and sends it to the next neighbor, and this process continues until the message reaches the final destination
- Plaintext or cleartext: The original unencrypted message, or a message that has been successfully decrypted
- Steganography: The hiding of messages—for example, within the digital encoding of a picture or graphic
- Work factor: The amount of effort (usually in hours) required to perform cryptanalysis to decode an encrypted message when the key or algorithm (or both) are unknown

CIPHER METHODS

A plaintext can be encrypted through one of two methods, the bit stream method or the block cipher method. With the bit stream method, each bit in the plaintext is transformed into a cipher bit one bit at a time. In the case of the block cipher method, the message is divided into blocks, for example, sets of 8-, 16-, 32-, or 64-bit blocks, and then each block of plaintext bits is transformed into an encrypted block of cipher bits using an algorithm and a key.

Substitution Cipher

In encryption, the most commonly used algorithms include three functions: substitution, transposition, and exclusive OR. In a substitution cipher, you substitute one value for another.

- Monoalphabetic substitution: uses only one alphabet
- Polyalphabetic substitution: more advanced; uses two or more alphabets
- Vigenère cipher: advanced cipher type that uses simple polyalphabetic code; made up of 26 distinct cipher alphabets

Transposition 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 the bit or byte in position 1 moves to position 4, and the bit or byte in position 2 moves to position 8, and so on.

Exclusive OR

Bit stream methods most commonly use algorithm functions like the exclusive OR operation (XOR), whereas block methods can use substitution, transposition, XOR, or some combination of these operations. 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.

First Bit	Second Bit	Result
0	0	0
0	1	1
1	0	1
1	1	0

Vernam Cipher

The Vernam cipher, also known as the one-time pad, was developed at AT&T and uses a set of characters only one time for each encryption process.

To perform the Vernam cipher encryption operation:

- The pad values are added to numeric values that represent the plaintext that needs to be encrypted.
- So, each character of the plaintext is turned into a number and a pad value for that position is added to it.
- The resulting sum for that character is then converted back to a ciphertext letter for transmission.
- When the two are added, if the values exceed 26, then 26 is subtracted from the total. (This is referred to as Modulo 26.)

- The corresponding results are then converted back to text.

Book or Running Key Cipher

Another method, made popular by spy movies, involves the use of text in a book as the key to decrypt a message. The cyphertext consists of a list of codes representing the Page number, line number, and word number of the plaintext word. The receiver must know which book to use. Dictionaries and thesauruses make the most popular sources as they guarantee every word needed, although almost any book will suffice.

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. A message authentication code (MAC), which is essentially a one-way hash value that is encrypted with a symmetric key, may be attached to a message to allow only specific recipients to access the message digest. The recipients must possess the key to access the message digest and to confirm message integrity.

The Secure Hash Standard (SHS) is a standard issued by the NIST. Standard document FIPS 180-1 specifies SHA-1 (Secure Hash Algorithm 1) as a secure algorithm for computing a condensed representation of a message or data file. SHA-1 produces a 160-bit message digest, which can then be used as an input to a digital signature algorithm. SHA-1 is based on principles modeled after MD4 (which is part of the MDx family of hash algorithms created by Ronald Rivest). New hash algorithms (SHA-256, SHA-384, and SHA-512) have been proposed by NIST as standards for 128, 192, and 256 bits, respectively.

CRYPTOGRAPHIC ALGORITHMS

In general, cryptographic algorithms are often grouped into two broad categories: symmetric and asymmetric. 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 uses the same key, also known as a secret key, to encrypt and decrypt a 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 possess 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.

Data Encryption Standard (DES)

- The Data Encryption Standard (DES) was developed in 1977 by IBM and is based on the Data Encryption Algorithm (DEA).
- As implemented, DES uses a 64-bit block size and a 56-bit key. 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 finally cracked in 1997 when the RSA offered $10,000 as a reward to the team that could crack the algorithm.
- Fourteen thousand users collaborated over the Internet to break the encryption.

Triple DES (3DES)

- Triple DES (3DES) was developed as an improvement to DES. 3DES encrypts the message three times with three different keys.
- In 1998, it took a dedicated computer designed by the Electronic Freedom Frontier (www.eff.org) over 56 hours to break a DES key.

Advanced Encryption Standard (AES)

- AES is based on the Rinjndael Block Cipher, a block cipher with a variable block length and a key length of either 128, 192, or 256 bits.

- It would take the same computer approximately 4,698,864 quintillion years to crack AES.

Asymmetric Encryption

Asymmetric encryption is another category of encryption techniques also known as public-key encryption. Symmetric encryption uses a single key to encrypt and decrypt, but asymmetric encryption uses two different but related keys, one public and one private. For example, if Key A is used to encrypt the message, only Key B can decrypt it. The public key is stored in a public location where anyone can use it, and the private key is known only to the owner of the key pair.

RSA

1. Choose two very large random prime integers:
   p and q
2. Compute n and φ(n):
   n = pq and φ(n) = (p-1)(q-1)
3. Choose an integer e, $1 < e < \varphi(n)$ such that:
   gcd(e, φ(n)) = 1(where gcd means greatest common denominator)
4. Compute d, $1 < d < \varphi(n)$ such that:
   $ed \equiv 1 \pmod{\varphi(n)}$

   - the public key is (n, e) and the private key is (n, d)
   - the values of p, q and φ(n) are private
   - e is the public or encryption exponent
   - d is the private or decryption exponent

   Encryption

   The cyphertext C is found by the equation '$C = M^e \bmod n$' where M is the original message.

   Decryption

   The message M can be found form the cyphertext C by the equation '$M = C^d \bmod n$'.

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.

CRYPTOGRAPHIC TOOLS

To be actually useful, these cryptographic capabilities must be embodied in tools that allow IT and information security practitioners to apply the elements of cryptography in the everyday world of computing.

Public-Key Infrastructure (PKI)

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 systems can be used to:

- Issue digital certificates
- Issue keys
- Provide tools to secure information
- Provide verification and return of certificates

PKI protects information assets using:

- Authentication
- Integrity
- Privacy
- Authorization
- Nonrepudiation

- Digital signatures

When an asymmetric cryptographic process uses the sender's private key to encrypt a message, the sender's public key must be used to decrypt the message—when the decryption happens successfully, it provides verification that the message was sent by the sender and 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 Signatures

Currently, asymmetric encryption processes are used to create digital signatures. When an asymmetric cryptographic process uses the sender's private key to encrypt a message, the sender's public key must be used to decrypt the message. When the decryption happens successfully, it provides verification that the message was sent by the sender and cannot be refuted. Process is known as nonrepudiation and is the principle of cryptography that underpins the authentication mechanism collectively known as a digital signature. Digital signatures are encrypted messages that can be mathematically proven authentic. Digital signatures should be created using processes and products that are based on the Digital Signature Standard (DSS).

Digital Certificates

Digital certificate, which is an electronic document, similar to a digital signature that is attached to a file and certifies that the file is from the organization it claims to be from and has not been modified from the original 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.

Hybrid Cryptography Systems

In practice, pure asymmetric key encryption is not widely used except in the area of certificates. Asymmetric key encryption is more often used in conjunction with symmetric key encryption—thus as part of a hybrid encryption system. The most common hybrid encryption system is based on the Diffie-Hellman Key Exchange method, which is a method

for exchanging private keys using public-key encryption. With Diffie-Hellman, asymmetric encryption is used to exchange session keys. These are limited-use symmetric keys for temporary communications; they allow two organizations to conduct quick, efficient, secure communications based on symmetric encryption. Diffie-Hellman provided the foundation for subsequent developments in public-key encryption.

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). It is this inability to perceive difference on part of humans that 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.

PROTOCOLS FOR SECURE COMMUNICATIONS

Many of the software currently used to protect the confidentiality of information are not true cryptosystems. Instead, they are applications to which cryptographic protocols have been added. This is perhaps particularly true of Internet protocols.

Securing Internet Communication with S-HTTP and SSL

Netscape developed the Secure Socket Layer (SSL) protocol to use public-key encryption to secure a channel over the public Internet, thus enabling secure communications. Secure Hypertext Transfer Protocol (S-HTTP) is an extended version of the Hypertext Transfer Protocol that provides for the encryption of individual messages between a client and server across the Internet. S-HTTP is the application of SSL over HTTP allows the encryption of all information passing between two computers through a protected and secure virtual connection.

Securing E-Mail with S/MIME, PEM, and PGP

Several encryption cryptosystems have been adapted to inject some degree of security into Web communications. S/MIME builds on the format of the Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication. 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 along with RSA for key exchange.

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.

Securing Wireless Networks with WEP and WPA

Wireless local area networks are thought by many in the IT industry to be inherently insecure. Without some form of protection, these signals can be intercepted by anyone with a wireless packet sniffer.

Wired Equivalent Privacy (WEP)

- WEP was an early attempt to provide security with the 8002.11 network protocol.
- It is now considered too cryptographically weak to provide any meaningful protection from eavesdropping.

- An intruder who collects enough data can threaten a WEP network in just a few minutes by decrypting or altering the data being transmitted, or by forging the WEP key to gain unauthorized access to the network.
- WEP also lacks a means of validating user credentials to ensure that only those who should be on the network are allowed to access it.

Wi-Fi Protected Access (WPA)

- WPA was created to resolve the issues with WEP.
- TKIP is a suite of algorithms that attempts to deliver the best security that can be obtained given the constraints of the wireless network environment.
- TKIP adds four new algorithms to WEP:

    - "A cryptographic message integrity code, or MIC, called Michael, to defeat forgeries;
    - A new IV sequencing discipline, to remove replay attacks from the attacker's arsenal;
    - A per-packet key mixing function, to de-correlate the public IVs from weak keys; and
    - A rekeying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse."

- While it offers dramatically improved security over WEP, WPA is not the most secure wireless protocol design. Some compromises were made in the security design to allow compatibility with existing wireless network components.
- Protocols to replace TKIP are currently under development.

Next generation wireless protocols

- Robust Secure Networks (RSN), a protocol planned for deployment as a replacement for TKIP in WPA, uses the Advanced Encryption Standard (AES), along with 802.1x and EAP. RSN extends AES with the Counter Mode CBC MAC Protocol (CCMP).

- AES supports key lengths up to 256 bits, but it is not compatible with older hardware.
- However, a specification called Transitional Security Network (TSN) allows RSN and WEP to coexist on the same wireless LAN.
- A number of protocols are being considered by the IEEE 802.11 group as a replacement for WPA.
- These include two based on the Advanced Encryption Standard (AES): The AES – Counter Mode Encapsulation and The AES – Offset Codebook Encapsulation.

Bluetooth technology

- Bluetooth is a de facto industry standard for short range wireless communications between devices.
- The Bluetooth wireless communications link can be exploited by anyone within the approximately 30 foot range, unless suitable security controls are implemented.
- It has been estimated that there will be almost a billion Bluetooth-enabled devices by the end of the decade.
- The only way to secure Bluetooth enabled devices is to incorporate a twofold approach: 1) turn off Bluetooth when you do not intend to use it and 2) do not accept an incoming communications pairing request unless you know who the requestor is.

Securing TCP/IP with IPSec and PGP

IP Security (IPSec) is the cryptographic authentication and encryption product of the IETF's IP Protocol Security Working Group. It is used to create virtual private networks (VPNs) and is an open framework for security development within the TCP/IP family of protocol standards.

The two modes of operation in which IPSec works:

- In transport mode, only the IP data is encrypted, not the IP headers.

- In tunnel mode, the entire IP packet is encrypted and is then placed as the payload in another IP packet.

The IPSec protocol

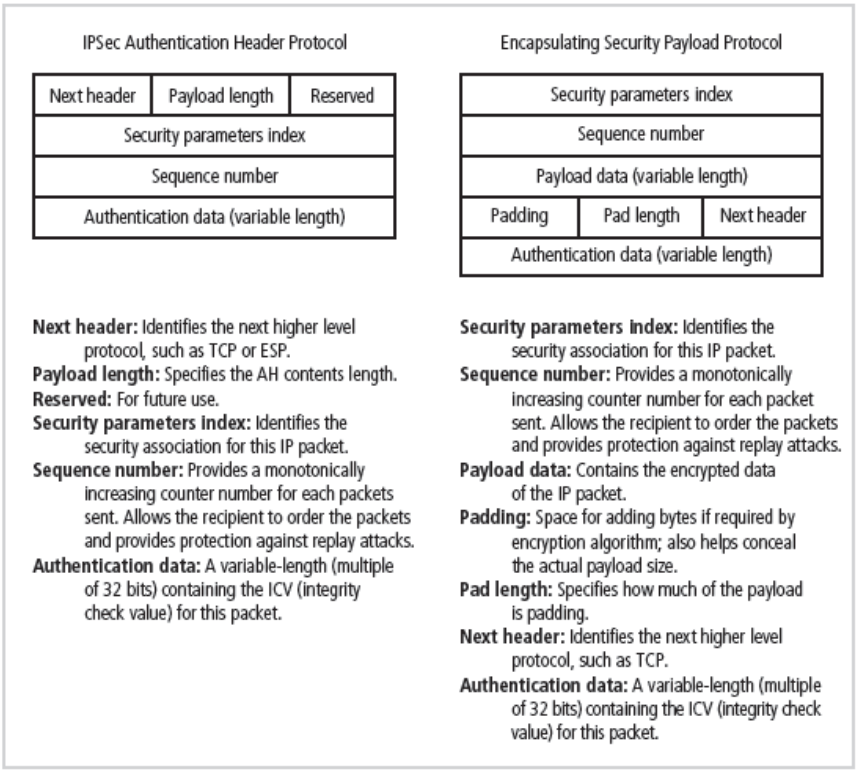

Figure: IPSec Headers

- IPSec combines several different cryptosystems in its operations:
    - 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
- IP layer security is obtained by using an application header protocol or an encapsulating security payload protocol.

- The application header (AH) protocol provides system-to-system authentication and data integrity verification, but it does not provide secrecy for the content of a network communication.
- The encapsulating security payload (ESP) protocol provides secrecy for the contents of network communications as well as system-to-system authentication and data integrity verification.

The PGP protocol

- 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, which 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 he or she is certain 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. The 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 in, 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

Note that 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 Against 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. Key management is not so much the management of technology, but rather the management of people.