EE 5084
Cyber Security

Tools, Firewalls and VPNs

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

BRUCE SCHNEIER, AMERICAN CRYPTOGRAPHER, COMPUTER SECURITY SPECIALIST, AND WRITER

Learning Objectives

- Familiar with security tools
- Important role of access control in computer-based information systems
- Identify and discuss widely used authentication factors
- Firewall technology and the various approaches to firewall implementation
- Approaches to control remote and dial-up access by authenticating and authorizing users
  - Discuss content filtering technology
  - Describe virtual private networks and discuss the technology that enables them

Introduction

- Tools and technology are essential in enforcing policy for many IT functions not under direct human control.
- When properly implemented, technical solutions improve an organization's ability to balance the objectives of making information readily available and preserving information's confidentiality and integrity.

CYBER SECURITY SERVICES

- Authentication
  - Assurance that communicating entity is the one claimed.
- Access Control
  - Prevention of the unauthorized use of online resource.
- Data Confidentiality
  - Protection of data from unauthorized disclosure.
- Data Integrity
  - Assurance that data received is as sent by an authorized entity.
- Non-Repudiation
  - Protection against denial by one of the parties in a communication.
- Availability
  - Resource accessible/usable.
- Security Mechanism
  - Feature designed to detect, prevent, or recover from a security attack.

TOOLS FOR CONFIDENTIALITY (1)

ENCRYPTION

The transformation of information using a secret (encryption) key, so that the transformed information can only be read using another secret (decryption key) which may, in some cases, be the same as the encryption key.

TOOLS FOR CONFIDENTIALITY (2)

ACCESS CONTROL

Rules and policies that limit access to confidential information to those people and/or systems with a "need to know."

This need to know may be determined by identity, such as a person's name or a computer's serial number, or by a role that a person has, such as being a manager or a computer security specialist.

AUTHENTICATION

The determination of the identity or role that someone has.

This determination can be done in a number of different ways, but it is usually based on a combination of

- ✓ something the person has (like a smart card)
- ✓ Something the person knows (like a password)
- ✓ something the person is (like a human with a fingerprint).

TOOLS FOR CONFIDENTIALITY (3)

Something you are

Something you know

Something you have

TOOLS FOR CONFIDENTIALITY (4)

AUTHORIZATION

The determination if a person or system is allowed access to resources, based on an access control policy.

Such authorizations should prevent an attacker from tricking the system into letting him have access to protected resources.

PHYSICAL SECURITY

The establishment of physical barriers to limit access to protected computational resources.

Such barriers include locks on cabinets and doors, the placement of computers in windowless rooms, the use of sound dampening materials, and even the construction of buildings or rooms with walls incorporating copper meshes (called **Faraday cages**) so that electromagnetic signals cannot enter or exit the enclosure.

TOOLS FOR INTEGRITY

INTEGRITY

The property that information has not be altered in an unauthorized way.

TOOLS

- **Backups**

  The periodic archiving of data.
- **Checksums**

  The computation of a function that maps the contents of a file to a numerical value.

  A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.
- **Data Correcting Codes**

  Methods for storing data in such a way that small changes can be easily detected and automatically corrected.

TOOLS FOR AVAILABLITY

- AVAILABILITY

  The property that information is accessible and modifiable in a timely fashion by those authorized to do so.

- TOOLS

  Physical Protections

  Infrastructure meant to keep information available even in the event of physical challenges.

  Computational Redundancies

  Computers and storage devices that serve as fallbacks in the case of failures.

Attacks, Mechanisms and Services

- **Security Attack**

  Any action that compromises the security of information.

- **Security Mechanism**

  A mechanism that is designed to detect, prevent, or recover from a security attack.

- **Security Service**

  A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Access Control

- Method by which systems determine whether and how to admit a user into a trusted area of the organization
- Discretionary access controls (DACs): allow users to control and possibly provide access to information or resources at their disposal
- Nondiscretionary controls: strictly enforced version of MACs that are managed by a central authority
- Mandatory access controls (MACs): use data classification schemes

Figure 6-1 Access control approaches

Identification

- Mechanism whereby unverified entities seeking access to a resource (supplicants) provide a label by which they are known to the system
- Identifiers can be composite identifiers, concatenating elements—department codes, random numbers, or special characters—to make them unique.
- Some organizations generate random numbers.

Authentication (1)

- The process of validating a user purported identity
- Authentication factors

  Something a user knows

  – Password: a private word or a combination of characters that only the user should know

  – Passphrase: a series of characters, typically longer than a password, from which a virtual password is derived

Password security

Rules to harden password protection

- **Never install any application or service with default passwords from the vendor**
- **Make passwords at least 10 characters long**
- **Use numbers, letters, and symbols, such as $, ***
- **Do not use words. Avoid any word in the English and Klingon (from Star Trek) dictionary**
- **Avoid names of sports teams, social security #s, first names, pet or other info that might be in personnel files or displayed on the wall**
- **Change passwords at least once every 4 months**
- **Memorize passwords and keep them secret**

UNSAFE PASSWORD

123456

Despite Internet security breaches, this is world's most popular password

NEW YORK

BACK at the dawn of the Web, the most popular account password was "12345". Today, it's one digit longer but hardly safer: 123456.

Despite all the reports of Internet security breaches over the years, including the recent attacks on Google's e-mail service, many people have reacted to electronic break-ins with a shrug.

According to a new analysis, one out of five Web users is still leaving the digital equivalent of a key under the doormat. They choose simple, easily-guessed passwords like "abc123", "iloveyou" or even "password" to protect their data.

"I guess it's just a genetic flaw in humans," said Mr Amichai Shulman, the chief technology officer at Imperva, which

Facebook and MySpace.

The list was briefly posted on the Web, and hackers and security researchers downloaded it.

RockYou, which had already been widely criticised for lax privacy practices, has advised its customers to change their passwords, as the hacker gained information about customers' e-mail accounts as well.

The trove provided an unusually detailed window into computer users' password habits. Typically, only government agencies, like the Federal Bureau of Investigation or the National Security Agency, have had access to such a large password list.

Said Mr Matt Weir, a doctoral candidate in the e-crimes and investigation technology lab at Florida State University, where researchers are also examining the data: "This was the mother lode."

Imperva found that nearly

'ILOVEYOU' IS HOT TOO

One million RockYou users chose these passwords:

1. 123456
2. 12345
3. 123456789
4. password
5. iloveyou
6. princess
7. rockyou
8. 1234567
9. 12345678
10. abc123
11. nicole
12. daniel
13. babygirl
14. monkey
15. jessica
16. lovely
17. michael
18. ashley
19. 654321
20. qwerty
21. iloveu
22. michelle
23. 111111
24. 0
25. tigger
26. password1
27. sunshine
28. chocolate
29. anthony
30. angel
31. FRIENDS
32. soccer

SOURCE: IMPERVA PHOTO: ISTOCKPHOTO

Authentication (2)

- Authentication factors

  Something a user has

  – Dumb card: ID or ATM card with magnetic stripe

  – Smart card: contains a computer chip that can verify and validate information

  – Synchronous tokens

  – Asynchronous tokens

  Something a user is

  – Relies upon individual characteristics

  – Strong authentication

Dear all,

This announcement is made strictly for international students who are not able to come to Singapore in time for Quiz 1.

Please read the list of students and inform me if I have left out or mistype your name.

IMPORTANT:

- ✓ Please read and follow all the instructions uploaded in the content folder.
- ✓ Please sign the consent form for the online quiz. This is the link for the consent form: https://forms.office.com/r/kVydwCHm2N

Regards,

Dr Chan

Authorization

- Authorization: the matching of an authenticated entity to a list of information assets and corresponding access levels
- Authorization can be handled in one of three ways:
  - Authorization for each authenticated user
  - Authorization for members of a group
  - Authorization across multiple systems
- Authorization tickets

Accountability

- Accountability (auditability): ensures that all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity
- Most often accomplished by means of system logs and database journals, and the auditing of these records
- Systems logs record specific information.
- Logs have many uses.

Biometrics

- Approach based on the use of measurable human characteristics/traits to authenticate identity
- Only fingerprints, retina of eye, and iris of eye are considered truly unique.
- Evaluated on false reject rate, false accept rate, and crossover error rate
- Highly reliable/effective biometric systems are often considered intrusive by users.

Figure 6-5 Biometric recognition characteristics

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Hand Vein	M	M	M	M	M	M	H
Eye: Iris	H	H	H	M	H	L	H
Eye: Retina	H	H	M	L	H	L	H
DNA	H	H	H	L	H	L	L
Odor & Scent	H	H	H	L	L	M	L
Voice	M	L	L	M	L	H	L
Signature	L	L	L	H	L	H	L
Keystroke	L	L	L	M	L	M	M
Gait	M	L	L	H	L	H	M

Table 6-1 Ranking of Biometric Effectiveness and Acceptance

In the table, H = High, M = Medium, and L = Low.

From multiple sources.[3]

Firewalls

- Prevent specific types of information from moving between an untrusted network (the Internet) and a trusted network (organization's internal network)
- May be
  - Separate computer system
  - Software service running on existing router or server
  - Separate network containing supporting devices

Firewalls Processing Modes

- Five processing modes by which firewalls can be categorized:
  - Packet filtering
  - Application gateways
  - Circuit gateways
  - MAC layer firewalls
  - Hybrids

Packet-Filtering Firewalls (1)

- Packet-filtering firewalls examine the header information of data packets.
- Most often based on the combination of:
  - IP source and destination address
  - Direction (inbound or outbound)
  - Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests
- Simple firewall models enforce rules designed to prohibit packets with certain addresses or partial addresses from passing through device.

Figure 6-7 IP packet structure

Figure 6-8 TCP packet structure

Figure 6-9 UDP datagram structure

Figure 6-10 Packet-filtering router

Source address	Destination address	Service (e.g., HTTP, SMTP, FTP)	Action (allow or deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

Table 6-2 Sample Firewall Rule and Format

© Cengage Learning 2015

Packet-Filtering Firewalls (2)

- Three subsets of packet-filtering firewalls:
  - Static filtering

    requires that filtering rules be developed and installed within the firewall
  - Dynamic filtering

    allows firewall to react to emergent event and update or create rules to deal with event
  - Stateful packet inspection (SPI)

    firewalls that keep track of each network connection between internal and external systems using a state table

Source address	Source port	Destination address	Destination port	Time remaining (in seconds)	Total time (in seconds)	Protocol
192.168.2.5	1028	10.10.10.7	80	2725	3600	TCP

Table 6-3 State Table Entries

© Cengage Learning 2015

Application Layer Firewall

- Frequently installed on a dedicated computer; also known as a proxy server
- Since proxy server is often placed in unsecured area of the network (e.g., DMZ), it is exposed to higher levels of risk from less trusted networks.
- Additional filtering routers can be implemented behind the proxy server, further protecting internal systems.

MAC layer firewalls

- Designed to operate at media access control sublayer of network's data link layer
- Make filtering decisions based on specific host computer's identity
- MAC addresses of specific host computers are linked to access control list (ACL) entries that identify specific types of packets that can be sent to each host; all other traffic is blocked.

Figure 6-11 Firewall types and protocol models

Hybrid firewalls

- Combine elements of other types of firewalls, that is, elements of packet filtering and proxy services, or of packet filtering and circuit gateways
- Alternately, may consist of two separate firewall devices; each a separate firewall system, but connected to work in tandem
- Enables an organization to make security improvement without completely replacing existing firewalls

Reminder: Quiz 1

On Site:

Thursday 16 Sept, session 1 or 2 in the lab (check the uploaded file)

Be familiar with the lab location

Online (only for IS students who are not in Singapore):

Thursday 16 Sept, login by 4:30pm

Please read and follow instructions carefully

Please prepare 2 devices

Please download and install Lockdown Browser

Please sign consent form before quiz

Please bring along matric card, or passport if you don't have matric card

Firewall Architectures

- Firewall devices can be configured in several network connection architectures.
- Best configuration depends on three factors:
  - Objectives of the network
  - Organization's ability to develop and implement architectures
  - Budget available for function
- Four common architectural implementations of firewalls: packet-filtering routers, dual-homed firewalls (bastion hosts), screened host firewalls, screened subnet firewalls

Packet-filtering routers

- Most organizations with Internet connection have a router at the boundary between internal networks and external service provider.
- Many of these routers can be configured to reject packets that the organization does not allow into its network.
- Drawbacks include a lack of auditing and strong authentication.

Dual-homed firewalls (bastion hosts)

- Commonly referred to as sacrificial host, as it stands as sole defender on the network perimeter
- Contains two network interface cards (NICs): one connected to external network, one connected to internal network
- Implementation of this architecture often makes use of network address translation (NAT), creating another barrier to intrusion from external attackers.

© Cengage Learning 2015

Figure 6-16 Dual-homed bastion host firewall

Screened host firewalls

- Combines packet-filtering router with separate, dedicated firewall such as an application proxy server
- Allows router to prescreen packets to minimize traffic/load on internal proxy
- Requires external attack to compromise two separate systems before attack can access internal data

Figure 6-17 Screened host firewall

Screened subnet firewall with DMZ (1)

- Is the dominant architecture used today
- Commonly consists of two or more internal bastion hosts behind packet-filtering router, with each host protecting a trusted network:
  - Connections from outside or untrusted network are routed through external filtering router.
  - Connections from outside or untrusted network are routed into and out of routing firewall to separate the network segment known as DMZ.
  - Connections into trusted internal network are allowed only from DMZ bastion host servers.

Screened subnet firewall with DMZ (2)

- Screened subnet performs two functions:
  - Protects DMZ systems and information from outside threats
  - Protects the internal networks by limiting how external connections can gain access to internal systems
- Another facet of DMZs: extranets

Figure 6-18 Screened subnet (DMZ)

Configuring and Managing Firewalls (1)

- The organization must provide for the initial configuration and ongoing management of firewall(s).
- Each firewall device must have its own set of configuration rules regulating its actions.
- Firewall policy configuration is usually complex and difficult.
- Configuring firewall policies is both an art and a science .
- When security rules conflict with the performance of business, security often loses.

Configuring and Managing Firewalls (2)

- Best practices for firewalls
  - All traffic from the trusted network is allowed out.
  - Firewall device is never directly accessed from public network.
  - Simple Mail Transport Protocol (SMTP) data are allowed to pass through firewall.
  - Internet Control Message Protocol (ICMP) data are denied
  - Telnet access to internal servers should be blocked.
  - When Web services are offered outside the firewall, HTTP traffic should be blocked from reaching internal networks.
  - All data not verifiably authentic should be denied.

Configuring and Managing Firewalls (3)

- Firewall rules
  - Firewalls operate by examining data packets and performing comparison with predetermined logical rules.
  - The logic is based on a set of guidelines most commonly referred to as firewall rules, rule base, or firewall logic.
  - Most firewalls use packet header information to determine whether specific packet should be allowed or denied.

Port number	Protocol
7	Echo
20	File Transfer [Default Data] (FTP)
21	File Transfer [Control] (FTP)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
161	Simple Network Management Protocol (SNMP)

Table 6-5 Well-Known Port Numbers

© Cengage Learning 2015

Rule #	Source address	Source port	Destination address	Destination port	Action
1	10.10.10.0	Any	Any	Any	Deny
2	Any	Any	10.10.10.1	Any	Deny
3	Any	Any	10.10.10.2	Any	Deny
4	10.10.10.1	Any	Any	Any	Deny
5	10.10.10.2	Any	Any	Any	Deny
6	Any	Any	10.10.10.0	>1023	Allow
7	Any	Any	10.10.10.6	25	Allow
8	Any	Any	10.10.10.0	7	Deny
9	Any	Any	10.10.10.0	23	Deny
10	Any	Any	10.10.10.4	80	Allow
11	Any	Any	Any	Any	Deny

Table 6-16 **External Filtering Firewall Inbound Interface Rule Set**

© Cengage Learning 2015

Rule #	Source address	Source port	Destination address	Destination port	Action
1	10.10.10.12	Any	10.10.10.0	Any	Allow
2	Any	Any	10.10.10.1	Any	Deny
3	Any	Any	10.10.10.2	Any	Deny
4	10.10.10.1	Any	Any	Any	Deny
5	10.10.10.2	Any	Any	Any	Deny
6	10.10.10.0	Any	Any	Any	Allow
7	Any	Any	Any	Any	Deny

Table 6-17 **External Filtering Firewall Outbound Interface Rule Set**

© Cengage Learning 2015

Content Filters (not a firewall)

- Software filter - allows administrators to restrict content access from within a network
- Essentially a set of scripts or programs restricting user access to certain networking protocols/Internet locations
- Primary purpose to restrict internal access to external material
- Most common content filters restrict users from accessing non-business Web sites or deny incoming spam.

Protecting Remote Connections

- Installing Internetwork connections requires leased lines or other data channels; these connections are usually secured under the requirements of a formal service agreement.
- When individuals seek to connect to an organization's network, a more flexible option must be provided.
- Options such as **virtual private networks (VPNs)** have become more popular due to the spread of Internet.

Remote Access

- Unsecured, dial-up connection points represent a substantial exposure to attack.
- Attacker can use a device called a war dialer to locate the connection points.
- War dialer: automatic phone-dialing program that dials every number in a configured range and records number if modem picks up
- Some technologies (RADIUS systems; TACACS; CHAP password systems) have improved the authentication process.

Virtual Private Networks (VPNs) (1)

- Private and secure network connection between systems; uses data communication capability of unsecured and public network
- Securely extends organization's internal network connections to remote locations
- Three VPN technologies defined:
  - **Trusted VPN** - private circuits leased from a trusted communications provider
  - **Secure VPN** - send encrypted traffic over the public Internet
  - **Hybrid VPN** (combines trusted and secure) - using a secure VPN over a trusted VPN

Virtual Private Networks (VPNs) (2)

- VPN must accomplish:
  - Encapsulation of incoming and outgoing data
  - Encryption of incoming and outgoing data
  - Authentication of remote computer and perhaps remote user as well
- In most common implementation, it allows the user to turn Internet into a private network.

Transport Mode VPN

- Data within IP packet is encrypted, but header information is not.
- Allows user to establish secure link directly with remote host, encrypting only data contents of packet
- Two popular uses:
  - End-to-end transport of encrypted data
  - Remote access worker connects to office network over Internet by connecting to a VPN server on the perimeter.

Figure 6-23 Transport mode VPN

Tunnel Mode VPN

- Establishes two perimeter tunnel servers to encrypt all traffic that will traverse unsecured network
- Entire client package encrypted and added as data portion of packet from one tunneling server to another
- Primary benefit to this model is that an intercepted packet reveals nothing about the true destination system.
- Example of tunnel mode VPN: Microsoft's Internet Security and Acceleration (ISA) Server

Figure 6-24 Tunnel mode VPN

Summary

- Tools
- Firewall technology
- Content filtering technology
- Various approaches to remote and dial-up access protection
- Virtual private networks

EE 5084
Cyber Security

Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools

Do not wait; the time will never be just right. Start where you stand and work with whatever tools you may have at your command, and better tools will be found as you go along.

NAPOLEON HILL (1883–1970) FOUNDER OF THE SCIENCE of SUCCESS

Learning Objectives

- Categories and models of intrusion detection and prevention systems (IDPS)
- Detection approaches employed by IDPS
- Honeypots, honeynets, and padded cell systems
- Categories of scanning and analysis tools, and describe the specific tools used within each category

Introduction

- Protection of organizations assets relies as much on managerial controls as on technical safeguards.
- Technical solutions must be guided by policy
- Advanced technologies can be used to enhance the security of information assets.

Intrusion Detection and Prevention Systems (IDPS) (1)

- Intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an IS
- Intrusion <u>prevention</u> consists of activities that deter an intrusion.
- Intrusion <u>detection</u> consists of procedures and systems that identify system intrusions.
- Intrusion <u>reaction</u> encompasses actions undertaken when intrusion event is detected.

Intrusion Detection and Prevention Systems (IDPS) (2)

- Intrusion correction: complete restoration of operations to a normal state and seek to identify source and method of intrusion
- Intrusion detection systems detect a violation of its configuration and activate alarm.
- IDPSs enable administrators to configure systems to notify them directly of trouble via e-mail or pagers.
- Can also be configured to notify an external security service organization of a “break-in.”

Why Use an IDPS?

- Main purposes
  - To identify and report an intrusion
  - Can quickly contain attack and prevent/mitigate loss or damage
  - Detect and deal with preambles to attacks
- Data collection allows the organization to examine what happened after an intrusion and why.
- Serves as a deterrent by increasing the fear of detection
- Can help management with quality assurance and continuous improvement

Types of IDPSs

- **Network-based systems (NIDPS)** - focus on protecting network information assets.
- **Host-based systems (HIDPS)**
- Wireless IDPS: focuses on wireless networks
- Network behavior analysis IDPS: examines traffic flow on a network in an attempt to recognize abnormal patterns

Figure 7-1 Intrusion detection and prevention systems

NIDPS (1)

- Focused on protecting network information assets.
- Resides on a computer or an appliance connected to a segment of an organization's network; looks for indications of attacks
- When examining packets, a NIDPS looks for attack patterns within network traffic
- Installed at specific place in the network where it can monitor traffic going into and out of a particular network segment

NIDPS (2)

- To determine whether attack has occurred/is under way, compare measured activity to known signatures in knowledge base
- Done by using special implementation of TCP/IP stack:
  - In the process of protocol stack verification, NIDPSs look for invalid data packets.
  - In the application protocol verification, higher-order protocols are examined for unexpected packet behavior or improper use.

Advantages of NIDPS

- Good network design and placement of NIDPS can enable an organization to monitor a large network with few devices.
- NIDPSs are usually passive and can be deployed into existing networks with little disruption to normal network operations.
- **NIDPSs are not usually susceptible to direct attack and may not be detectable by attackers**.

Disadvantages of NIDPS

- Can become overwhelmed by network volume and fail to recognize attacks
- Require access to all traffic to be monitored
- Cannot analyze encrypted packets
- Cannot reliably ascertain if attack was successful or not
- Some forms of attack are not easily discerned by NIDPSs, specifically those involving fragmented packets.

Host-based IDPS (HIDPS)

- Resides on a particular computer or server (host) and monitors activity only on that system
- Benchmarks and monitors the status of key system files and detects when intruder creates, modifies, or deletes files
- Advantage over NIDPS: can access encrypted information traveling over network and make decisions about potential/actual attacks
- Most HIDPSs work on the principle of configuration or change management.

Advantages of HIDPS

- Can detect local events on host systems and detect attacks that may elude a network-based IDPS
- Functions on host system, where encrypted traffic will have been decrypted and is available for processing
- Not affected by use of switched network protocols
- Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs

Disadvantages of HIDPS

- Pose more management issues
- Vulnerable both to direct attacks and attacks against host operating system
- Does not detect multihost scanning, nor scanning of non-host network devices
- Susceptible to some DoS attacks
- Can use large amounts of disk space
- Can inflict a performance overhead on its host systems

Other Types

- Wireless NIDPS
  - Monitors and analyzes wireless network traffic
  - Issues associated with it include physical security, sensor range, access point and wireless switch locations, wired network connections, cost, AP and wireless switch locations.
- Network behavior analysis systems
  - Identify problems related to the flow of traffic
  - Types of events commonly detected include denial-of-service (DoS) attacks, scanning, worms, unexpected application services, and policy violations.
  - Offer intrusion prevention capabilities that are passive, inline, and both passive and inline

IDPS Detection Methods (1)

- Signature-based detection
  - Examines network traffic in search of patterns that match known signatures
  - Widely used because many attacks have clear and distinct signatures
  - Problem with this approach is that new attack patterns must continually be added to IDPS's database of signatures.
    - Slow, methodical attack involving multiple events might escape detection.

IDPS Detection Methods (2)

- Anomaly-based detection
  - Anomaly-based detection (or behavior-based detection) collects statistical summaries by observing traffic known to be normal.
  - When measured activity is outside baseline parameters or clipping level, IDPS sends alert to administrator.
  - IDPS can detect new types of attacks.
  - Requires much more overhead and processing capacity than signature-based detection
  - May generate many false positives

IDPS Detection Methods (3)

- Stateful protocol analysis
  - SPA: process of comparing known normal/benign protocol profiles against observed traffic
  - Stores and uses relevant data detected in a session to identify intrusions involving multiple requests /responses; allows IDPS to better detect specialized, multisession attacks (also called deep packet inspection)
  - Drawbacks: analytical complexity; heavy processing overhead; may fail to detect intrusion unless protocol violates fundamental behavior; may interfere with normal operations of protocol

IDPS Detection Methods (4)

- Log file monitors
  - Log file monitor (LFM) similar to NIDPS
  - Reviews log files generated by servers, network devices, and even other IDPSs for patterns and signatures
  - Patterns that signify attack may be much easier to identify when entire network and its systems are viewed as a whole
  - Requires considerable resources since it involves the collection, movement, storage, and analysis of large quantities of log data

IDPS Response Behavior

- IDPS response to external stimulation depends on the configuration and function; many response options are available.
- IDPS responses can be classified as active or passive.
  - Active response: collecting additional information about the intrusion, modifying the network environment, taking action against the intrusion
  - Passive response: setting off alarms or notifications, collecting passive data through SNMP traps
- Many IDPSs can generate routine reports and other detailed documents.
- Failsafe features protect IDPS from being circumvented.

IDPS Alert Types (1)

- **True Positive**

  A legitimate attack which triggers an IDPS to produce an alarm.[2]
- **False Positive**

  An event signaling an IDPS to produce an alarm when no attack has taken place.
- **False Negative**

  When no alarm is raised when an attack has taken place.[2]
- **True Negative**

  An event when no attack has taken place and no detection is made.

IDPS Alert Types(2)

- A good portion of false-positives and false-negatives can be attributed to lack of knowledge about the environment being monitored
- Knowledge about the environment is not up-to-date as well as inaccurate history

IDPS Alert Types(2)

- A good portion of false-positives and false-negatives can be attributed to lack of knowledge about the environment being monitored
- Knowledge about the environment is not up-to-date as well as inaccurate history
- Incorporate **context** to reduce the rate of both false-positives and false-negatives
- **Context** is additional security event data and information in relation to the environment

Selecting IDPS Approaches and Products

- Technical and policy considerations
  - What is your systems environment?
  - What are your security goals and objectives?
  - What is your existing security policy?
- Organizational requirements and constraints
  - What requirements are levied from outside the organization?
  - What are your organization's resource constraints?

IDPSs product features and quality

- Is the product sufficiently scalable for your environment?
- How has the product been tested?
- What user level of expertise is targeted by the product?
- Is the product designed to evolve as the organization grows?
- What are the support provisions for the product?

Strengths of IDPSs (1)

- 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 patterns of system events corresponding to known attacks
  - Recognizing activity patterns that vary from normal activity

Strengths of IDPSs (2)

- IDPSs perform the following functions well: (cont'd)
  - Managing OS audit and logging mechanisms and data they generate
  - Alerting appropriate staff when attacks are detected
  - Measuring enforcement of security policies encoded in analysis engine
  - Providing default information on security policies
  - Allowing non-security experts to perform important security monitoring functions

Limitations of IDPSs (1)

- IDPSs cannot perform the following functions:
  - Compensating for weak/missing security mechanisms in protection infrastructure
  - Instantaneously detecting, reporting, responding to attack when there is heavy network or processing load
  - Detecting new attacks or variants of existing attacks
  - Effectively responding to attacks by sophisticated attackers
  - Automatically investigating attacks without human intervention

Limitations of IDPSs (2)

- IDPSs cannot perform the following functions (cont'd):
  - Resisting attacks intended to defeat or circumvent them
  - Compensating for problems with fidelity of information sources
  - Dealing effectively with switched networks

Implementation of an IDPS

- An IDPS can be implemented via one of three basic control strategies:
  - Centralized: All IDPS control functions are implemented and managed in a central location.
  - Fully distributed: All control functions are applied at the physical location of each IDPS component.
  - Partially distributed: Combines the two; while individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable organization to detect widespread attacks.

Figure 7-4 Centralized IDPS control[20]

Source: Adapted from Scarfone and Mell, NIST SP 800-94.

© Cengage Learning 2015

Figure 7-5 Fully distributed IDPS control[21]

Source: Adapted from Scarfone and Mell, NIST SP 800-94.

© Cengage Learning 2015

Figure 7-6 Partially distributed IDPS control[22]

Source: Adapted from Scarfone and Mell, NIST SP 800-94.

Deployment of an IDPS (1)

- IDPS deployment
  - Great care must be taken when deciding where to locate components.
  - Planners must select deployment strategy that is based on careful analysis of organization's information security requirements and causes minimal impact.
  - NIDPS and HIDPS can be used in tandem to cover individual systems that connect to an organization's network and networks themselves.

Deployment of an IDPS (2)

- Deploying network-based IDPSs
  - NIST recommends four locations for NIDPS sensors
    - Location 1: Behind each external firewall, in the network DMZ
    - Location 2: Outside an external firewall
    - Location 3: On major network backbones
    - Location 4: On critical subnets

© Cengage Learning 2015

Figure 7-7 Network IDPS sensor locations[23]

Source: Adapted from Scarfone and Mell, NIST SP 800-94.

Deployment of an IDPS (3)

- Deploying host-based IDPSs
  - Proper implementation of HIDPSs can be a painstaking and time-consuming task.
  - Deployment begins with implementing most critical systems first.
  - Installation continues until either all systems are installed or the organization reaches planned degree of coverage it will accept.

Comparison with firewall

- Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network
- An IDPS evaluates a suspected intrusion and signals an alarm

Honeypots, Honeynets, and Padded Cell Systems (1)

- Honeypots: decoy systems designed to lure potential attackers away from critical systems
- Honeynets: several honeypots connected together on a network segment
- Honeypots are designed to:
  - Divert attacker from accessing critical systems
  - Collect information about attacker's activity
  - Encourage attacker to stay on a system long enough for administrators to document the event and perhaps respond

Honeypots, Honeynets, and Padded Cell Systems (2)

- Padded cell system: protected honeypot that cannot be easily compromised
- In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDPS.
- When the IDPS detects attackers, padded cell system seamlessly transfers them to a special simulated environment where they can cause no harm—hence the name *padded cell.*

Advantages of Honeypots, Honeynets, and Padded Cell Systems

- Attackers can be diverted to targets they cannot damage.
- Administrators have time to decide how to respond to an attacker.
- Attackers' actions can be easily and more extensively monitored, and 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.

Disadvantages of Honeypots, Honeynets, and Padded Cell Systems

- Legal implications of using such devices are not well understood.
- 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 aggressive attack against an organization's systems.
- Administrators and security managers need a high level of expertise to use these systems.

Trap-and-Trace Systems

- Use a combination of techniques to detect an intrusion and trace it back to its source
- Trap usually consists of a honeypot or a padded cell and alarm.
- Legal drawbacks to trap and trace
  - Enticement: act of attracting attention to system by placing tantalizing information in key locations
  - Entrapment: act of luring an individual into committing a crime to get a conviction
  - Enticement is legal and ethical, entrapment is not.

Enticement and Entrapment

Enticement (Legal and ethical):

- Making committing a crime more enticing, but the person has already broken the law or at least has decided to do so.
- Honeypots can be a good way to use Enticement.
- Have open ports or services on a server that can be attacked.
- Enticement is not a valid defense.

Entrapment (Illegal and unethical):

- When someone is persuaded to commit a crime that they had no intention to commit and is then charged with it.
- Openly advertising sensitive data and then charging people when they access them.
- Entrapment is a solid legal defense.

If there is a gray area in some cases between enticement and entrapment, it is ultimately up to the jury to decide if it was one or the other.

Active Intrusion Prevention

- Some organizations implement active countermeasures.
- One tool (LaBrea) takes up unused IP address space to pretend to be a computer and allow attackers to complete a connection request, but then holds connection open.

Scanning and Analysis Tools (1)

- Scanning tools typically are used to collect information that an attacker needs to launch a successful attack.
- Attack protocol is a logical sequence of steps or processes used by an attacker to launch an attack against a target system or network.
- Footprinting: process of collecting publicly available information about a potential target

Scanning and Analysis Tools (2)

- Fingerprinting: systematic survey of target organization's Internet addresses collected during the footprinting phase to identify network services offered by hosts in that range
- Fingerprinting reveals useful information about the internal structure and nature of the target system or network to be attacked.
- These tools are valuable to the network defender since they can quickly pinpoint the parts of the systems or network that need a prompt repair to close vulnerabilities.

Port Scanners

- Tools used by both attackers and defenders to identify/fingerprint computers active on a network and other useful information
- Can either perform generic scans or those for specific types of computers, protocols, or resources
- The more specific the scanner is, the more useful its information is to attackers and defenders.

Port number	Protocol
7	Echo
20	File Transfer [Default Data] (FTP)
21	File Transfer [Control] (FTP)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
161	Simple Network Management Protocol (SNMP)

Table 7-1 Commonly Used Port Numbers

© Cengage Learning 2015

Firewall Analysis Tools

- Several tools automate remote discovery of firewall rules and assist the administrator/attacker in analyzing them.
- Administrators who feel wary of using the same tools that attackers use should remember:
  - User intent dictates how gathered information will be used.
  - To defend a computer or network well, administrators must understand ways it can be attacked.
- A tool that can help close an open or poorly configured firewall will help the network defender minimize risk from attack.

Operating System Detection Tools

- Ability to detect a target computer's operating system (OS) is very valuable to an attacker.
  - Once OS is known, the attacker can easily determine the vulnerabilities to which it is susceptible.
- Many tools use networking protocols to determine a remote computer's OS.

Vulnerability Scanners

- Active vulnerability scanners examine networks for highly detailed information and initiate traffic to determine security holes.
- Passive vulnerability scanners listen in on network and identify the vulnerable versions of both server and client software.
- Passive vulnerability scanners have the ability to find client-side vulnerabilities typically not found in active scanners.

Packet Sniffers

- Network tool that captures copies of packets from network and analyzes them
- Can provide 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.
- To use packet sniffers legally, an administrator must be on a network that the organization owns, be under direct authorization of owners of the network, and have knowledge and consent of the content's creators.

Wireless Security Tools

- An organization that spends its time securing a wired network while ignoring wireless networks is exposing itself to a security breach.
- Security professionals 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.

Summary

- Intrusion detection system (IDPS) detects violation of its configuration and activates alarm.
- Network-based IDPS (NIDPS) versus host-based IDPS (HIDPS)
- Selecting IDPS products that best fit an organization's needs is challenging and complex.
- Honeypots are decoy systems; two variations are known as honeynets and padded cell systems.
- Scanning and analysis tools are used to pinpoint vulnerabilities in systems, holes in security components, and unsecured aspects of a network.

EE 8084

CYBER SECURITY

Threat Environment
Plan
Ongoing protection by access control, firewalls, cryptography, etc.
Protect
Respond

Security Management
Firewalls
Encryption
SSL
Network Security Protocols
Virtual Private Networks
Authentication Procedures
Proxy Servers
Anti-Virus Software
Automated Software Updates
Intrusion Detection/ Prevention

CRYPTOGRAPHY

OPEN COMMUNICATIONS

CRYPTOGRAPHY

- Greek kryptós (hidden) and gráphien (to write)
- The study of ways to hide or obscure information, making it unreadable without secret knowledge
- Cryptography is the use of mathematical operations to protect messages traveling between parties or stored on a computer
- It means that someone intercepting your communications cannot read them

CRYPTOGRAPHY

- **CRYPTOGRAPHY:** is the art and science of secret writing, encrypting, or hiding of information from all but the intended recipient.
- **CRYPTANALYSIS:** is the process of attempting to break a cryptographic system and return the encrypted message to its original form.
- **BASIC DEFINITIONS**
  - **PLAINTEXT**: A piece of data that is not encrypted
  - **CIPHERTEXT**: The output of an encryption algorithm
  - **CIPHER**: A cryptographic algorithm
  - **KEY**: A sequence of characters or bits used by an algorithm to encrypt or decrypt a message
  - **ENCRYPTION**: Changing plaintext to ciphertext
  - **DECRYPTION**: Changing ciphertext to plaintext

ENCRYPTION AND DECRYPTION PROCESS

- **NOTATION**
  - **M** = Message, **C** =ciphertext, **E**= encryption, **D** = decrypting
  - E(M) = C (encrypting message = ciphertext)
  - D(C) = M (decrypting ciphertext = message)

ENCRYPTION AND DECRYPTION PROCESS

- **NOTATION USING A KEY**
- **Secret-key (Symmetric) cryptosystem – one key**
  - $E_K(M) = C$ $\quad$ $D_K(C) = M$
- **Public-key (Asymmetric) cryptosystem – two keys**
  - $E_{K1}(M) = C$ $\quad$ $D_{K2}(C) = M$

CRYPTOGRAPHY

- **CRYPTOGRAPHIC ALGORITHMS**
  - The cryptographic algorithm—what is commonly called the encryption algorithm or cipher—is made up of mathematical steps for encrypting and decrypting information.
- **TYPES OF CIPHERS**
  - **Substitution** ciphers (replace)
  - **Transposition** ciphers (rearrange)
  - **Product ciphers** (substitution, permutation, and modular arithmetic)
  - Vigenère
  - One-time pad
- **KEYS**
  - Keys are special pieces of data used in both the encryption and decryption processes.
  - The algorithms stay the same, but a different key is used.
  - The more complex the key, the greater the security of the system.

KEY LENGTH

- **SECURITY = STRENGTH OF ALGORITHM + LENGTH OF KEY**
- Key of 8 bits has 2^8 or 256 possible combinations. Trivial to break even without a computer (50% chance of finding the key after 128 tries)
- Every bit you add, doubles the number of possible combinations.
- Assuming a key of 56 bits, there are 2^{56} possible combinations.
  - If a computer can try 1,000,000 keys a second, it would take (2^{56}/1,000,000*365*24*60*60) 2285 years to find the correct key.
  - A 64-bit key would take 585,000 years.
  - 128 bits requires 10^{25} years.
  - However, computers are much faster than 1M keys/s these days and with hackers using millions of compromised computers in parallel, in reality it is much easy to break it then it is in theory.

CRYPTOGRAPHY

- Plaintext can be encrypted through stream cipher or block cipher method
- **STREAM CIPHER:** A typical stream cipher encrypts plaintext one byte at a time, although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time.
- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code.
- For applications that require encryption/decryption of a stream of data, such as over a data communications channel or a browser/Web link, a stream cipher might be the better alternative.
- RC4, is the most widely used of all stream ciphers.
- It was developed in 1987 by Ron Rivest, one of the developers of the public-key cipher RSA.
- **BLOCK CIPHER:** Message divided into blocks (e.g., sets of 8- or 16-bit blocks) and each is transformed into encrypted block of cipher bits using algorithm and key.

CRYPTOGRAPHY

- A block cipher processes the input one block of elements at a time, producing an output block for each input block.
- For applications that deal with blocks of data, such as file transfer, e-mail, and database, block ciphers may be more appropriate.
- Examples of block cipher are, DES, 3DES, AES, RC5, Blowfish etc.
- **ENCRYPTION MODES:** Different encryption modes may be used. Common modes are:
  - **Electronic Code Book (ECB):** Each block encrypted separately.
  - **Cipher Block Chaining (CBC):** Next input depends on previous output

CRYPTOGRAPHY

- **CRYPTOSYSTEM:** (or Cryptographic system) is the package of all procedures, protocols, cryptographic algorithms and instructions used for enciphering and deciphering messages using cryptography.
- **CHOOSING ALGORITHMS**
- **Depends on the application**
  - Encrypting streams of data in real-time has different requirements than encryption files on your local computer
  - **SYMMETRIC:** Best for data on your hard drive
  - **PUBLIC:** Good for messages
- **Cryptography is Used to Achieve Information**
  - **CONFIDENTIALITY**: only authorized persons can access information
  - **INTEGRITY**: Information that was sent is what was received
  - **AUTHENTICATION**: Guarantee of originator and of electronic transmission (using digital signature)
  - **NON-REPUDIATION:** Originator of information cannot deny content or transmission (using digital signature)

SHIFT OR CAESAR'S CIPHER

- Caesar's cipher uses an algorithm and a key
  - The algorithm specifies that you offset the alphabet either to the right (forward) or to the left (backward)
  - The key specifies how many letters the offset should be.
- The Caesar's cipher is also known as a shift cipher.
- Historically, **additive ciphers** are called shift ciphers.
- **Julius Caesar** used an additive cipher to communicate with his officers.
- For this reason, additive ciphers are sometimes referred to as the Caesar cipher.
- Caesar used a key of 3 for his communications.
- The action of a Caesar cipher is to replace each plaintext letter with one fixed number of places down the alphabet.
- This example is with a shift of three,

so that a **B** in the plaintext becomes **E** in the ciphertext.

SHIFT CIPHER EXAMPLE

Solve this:
LPHKWYBLA

Solution
SWORDFISH

SUBSTITUTION CIPHERS

- Simple Shift ciphers are easy to crack.
  - Simply figure out the number of rotations.
- Substitution ciphers were developed because they are more complex.
- Substitution ciphers work on the principle of substituting a different letter for every letter.
  - a becomes g, b becomes d, and so on.
  - The letters are not in order as they are in shift ciphers.
- **BASIC IDEA** –substitute each block of plaintext by a different block.
- If plaintext is English then
  - **Mona-alphabetic** substitution (one to one relationship).
  - **Poly-alphabetic** substitution (one to many relationship).
- If plaintext is binary string then map one block of bits to another.
  - **Plaintext**: 0011010101010001 …10100101
  - **Ciphertext**: 0100010000011100 …00101001

SUBSTITUTION CIPHERS

- In substitution cipher, the alphabets may be shifted, reversed or scrambled
  - **SHIFTED:** Creating the Caesar Cipher
  - **REVERSED:** Creating Atbash cipher (simple substitution cipher for the Hebrew alphabet)
  - **SCRAMBLED:** Creating a mixed alphabet or deranged alphabet.
- Traditionally, mixed alphabets may be created by first writing out a keyword, removing repeated letters in it, then writing all the remaining letters in the alphabet in the usual order.
- **EXAMPLE**: The keyword "zebras" gives us the following alphabets.

Plaintext alphabet:	**ABCDEFGHIJKLMNOPQRSTUVWXYZ**
Ciphertext alphabet:	**ZEBRASCDFGHIJKLMNOPQTUVWXY**

- **A message of:** flee at once. we are discovered!
- **Enciphers to:** **SIAA ZQ LKBA. VA ZOA RFPBLUAOAR!**

TRANSPOSITION CIPHER

- The order of the letters are changed. 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.
- **EXAMPLE:** "THE UNEXAMINED LIFE IS NOT WORTH LIVING" ,Written vertically over six columns becomes:

```
TX SOV
HAL RI
EMINTN
 IFOHG
UNET
NE  L
EDIWI
```

Then, written horizontally becomes:

```
TX SOVHAL RIEMINTN IFOHGUNET  NE  LEDIWI
```

VIGENÈRE CIPHER

- The Vigenère cipher is a much more complex cipher.
- It corrects the issues with more simplistic keys.
- It works as a poly-alphabetic substitution cipher that depends on a password.
  - Makes the algorithms rather simple
  - But the key rather complex, with the best keys comprising very long and very random data
- A Vigenère cipher is done by setting up a substitution table like this one:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

(etc.)

VIGENÈRE CIPHER

- The password is matched up to the text it is meant to encipher.
- The cipher letter is determined by use of the grid
  - Matching the plaintext character's row
  - With the password character's column,
  - Resulting in a single ciphertext character where the two meet.
- For example – Plain text is "Send Help" and the password is "cabinet."
  - 1st plaintext letter S (column), 1st password letter c (row)
  - Ciphertext is now U

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

(etc.)

EXCLUSIVE OR (XOR)

- Function of Boolean algebra; two bits are compared, and binary result is generated.
- If two bits are identical, the result is binary 0.
- If two bits are not identical, the result is binary 1.
- Very simple to implement and simple to break; should not be used by itself when organization is transmitting/storing sensitive data

First bit	Second bit	Result
0	0	0
0	1	1
1	0	1
1	1	0

ONE-TIME PADS: A PERFECT SUBSTITUTION

- There is one type of substitution cipher that is **absolutely unbreakable**.
  - The one-time pad was invented in 1917 by Joseph Mauborgne and Gilbert Vernam and is also known as Vernam cipher
  - We use a block of shift keys, (k_1, k_2, . . . , k_n), to encrypt a plaintext, M, of length n, with each shift key being chosen uniformly at random.
- Since each shift is random, every ciphertext is equally likely for any plaintext.
- In spite of their perfect security, one-time pads have some weaknesses
- The key has to be as long as the plaintext
- Keys can never be reused
  - Repeated use of one-time pads allowed the U.S. to break some of the communications of Soviet spies during the Cold War
- Such cipher is **difficult to break but not very practical**

MODERN CIPHERS

- Operate on binary plaintext
- Uses binary keys of fixed length
- Different types of ciphers:
  - Symmetric ciphers
    - Stream ciphers (RC4, A5/x, Helix, SEAL)
    - Block ciphers (DES, Triple-DES, Blowfish, AES)
  - Asymmetric ciphers
    - Diffie-Hellman, ElGamal, RSA, ECC
- Two basic operations in modern cipher are:
  - Substitution: Substitutes a code symbol for another.
    - Example: shifts (Vigenere cipher), xor
  - Permutation: Transposes or re-orders the symbols present in the code
- Both steps are needed for security

SYMMETRIC KEY ENCRYPTION

SYMMETRIC KEY ENCRYPTION FOR CONFIDENTIALITY

Note:
A single key is used to encrypt and decrypt in both directions

SECRET-KEY CRYPTOGRAPHY (SKC)

- **ADVANTAGES OF SKC**
  - Symmetric-key ciphers can be designed to have high rates of data throughput.
  - Some hardware and software implementations achieve encrypt rates of hundreds of megabytes per second.
  - Keys for symmetric-key ciphers are relatively short.
    - For example, 128-bit keys are considered very safe.
- **DISADVANTAGES OF SKC**
  - In a two-party communication, the key must remain secret at both ends.
  - In a large network, there are many key pairs to be managed. Consequently, effective key management requires the use of an trusted third-party (TTP).
- **POPULAR SYMMETRIC ENCRYPTION ALGORITHMS**
  - **DES, 3DES, AES**, CAST, RIVEST, Blowfish, IDEA

DATA ENCRYPTION STANDARD (DES)

- In 1973, the National Bureau of Standards (NBS) now National Institute of Standards and Technology (NIST) requested proposals for national symmetric-key cryptosystem.
- A proposal from IBM, a modification of a project called Lucifer, was accepted as DES and adopted in 1976-77.

DATA ENCRYPTION STANDARD (DES)

- DES once was the most popular symmetric encryption cryptosystems.
- It was the first crypto system to have been used in commercial applications.
- It is a block cipher with 64-bit block size and 56-bit key.
- The algorithm takes the plain text in 64-bit blocks and converts them into 64-bit blocks of ciphertext using 56-bit keys.
- Since it's a symmetric-key algorithm, it employs the same key in both encrypting and decrypting the data.
- DES was adopted by NIST in 1976 as federal standard for encrypting non-classified information.
- After becoming the approved federal encryption standard in November 1976, it was subsequently reaffirmed as the standard in 1983, 1988, and 1999.
- The NIST had to replace the DES algorithm because its 56-bit key lengths were too small, considering the increased processing power of newer computers.
- DES's dominance came to an end in 2002 and the NIST officially withdrew the 1999 reaffirmation in May 2005.

SOMEONE BROKE DES, SO WHAT?

- Use DES multiple times?
- How many Times?

3DES

- Triple DES is a symmetric key-block cipher which applies the DES cipher in triplicate. It encrypts with the first key (k1), decrypts using the second key (k2), then encrypts with the third key (k3). There is also a two-key variant, where k1 and k3 are the same keys.

- Note:
  - If Key1 = Key2 = Key3, this is similar to DES
  - Usually, Key1 = Key3

AES (ADVANCED ENCRYPTION STANDARD)

- Originally called Rijndael, the cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen.
- It is block size is 128 and key size varies according to the version.
- Three versions are known as AES-128, AES-192 and AES-256, respectively.
- Although no efficient attacks exist against AES, in 2011, the trio of CRYPTOGRAPHY RESEARCHERS (working at Microsoft and European Universities) identified a weakness in AES security algorithm that can crack secret keys faster than before.
- However, recovering a key is no five-minute job and despite being four times easier than other methods the number of steps required to crack AES-128 is an 8 followed by 37 zeroes.

Vincent Rijmen
born in 1970

Joan Daemen
born in 1965

PUBLIC (ASYMMETRIC) KEY CRYPTOGRAPHY

- SYMMETRIC ALGORITHMS ARE **IMPORTANT BECAUSE**
  - They are comparatively fast and have few computational requirements
- THEIR **MAIN WEAKNESSES**
  - Two geographically distant parties both need to have a key that matches the other key exactly.
  - Secure key exchange can be an issue.
- Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations, which wanted to securely store the classified communication.
- However, the symmetric key was found to be non-practical when two parties want to securely communicate. This gave rise to public cryptosystem.
- **PUBLIC KEY** (ALSO KNOWN AS ASYMMETRIC-KEY ENCRYPTION)
  - Uses two different but related keys
  - Either key can encrypt or decrypt message
  - If Key A encrypts message, only Key B can decrypt
  - One key serves as private key and the other serves as public

PUBLIC-KEY CRYPTOGRAPHY (PKC)

- PKC was invented by Whitfield **Diffie** and Martin **Hellman** in 1976
  - PhD students at Stanford University

- Some give credit to Ralph Merkle (in 2002, he was recognized)

- NSA says that they knew PKC back in 60's
  - Uses two different but related keys
  - Either key can encrypt or decrypt message
  - If Key A encrypts message, only matching Key B can decrypt
  - One key serves as private key and the other serves as public key
- **PUBLIC KEY ALGORITHMS**
  - DIFFIE-HELLMAN, El-Gamal, RSA and Elliptic Curve (**used in Bitcoin)**

PUBLIC-KEY CRYPTOGRAPHY (PKC)

PUBLIC KEY ENCRYPTION
(CONFIDENTIALITY)

PUBLIC KEY AUTHENTICATION

PRIME NUMBERS AND MOD

- **PRIME NUMBERS**
- Prime numbers only have divisors of 1 and self
  - they cannot be written as a product of other numbers
  - note: 1 is prime, but is generally not of interest
- eg. 2,3,5,7 are prime, 4,6,8,9,10 are not.
- **MOD:** Example 1: 15 mod 20
  - Since 15 < 20, answer = 15 (i.e. 15 is remainder)
- **Example 2: 320 MOD 9**
  - Use MOD key on the calculator

    320 | MOD | 9 | = 5
  - If your calculator doesn't have MOD key, you can use division
  - 320/**9** = **3 5 . 5 5 5 5 5 5**
  - Now take the value after decimal point, which is **0.5555** and **multiply** it with **9**
  - **0.5555 * 9** = **5** This is the MOD value

PUBLIC KEY ALGORITHMS

- **RSA CRYPTOSYSTEM**
- This cryptosystem is one the first which provided complete solution.
  - How to generate public and private key
  - How to encrypt and decrypt the data
  - How to generate and verify digital signature

- It remains the most employed cryptosystem even today.
- The system was invented by three scholars Ron Rivest, Adi Shamir, and Len Adleman and hence, it is termed as RSA cryptosystem in 1978.
- The security of RSA algorithm is based on factorizing large prime numbers.
- The fact that it is easy to calculate the product of two numbers, while it is extremely difficult (if not impossible) to find the factor of two numbers, when the size is extremely large.
- This is called one way function, which means easy to compute but it is very difficult to compute their inverse functions, unless you know the secrete (private key).

PUBLIC KEY ALGORITHMS

- **ELGAMAL**
- It was designed by Taher Elgamal in 1985
  - Based on original ideas of Diffie and Hellman
  - Security based on assumed difficulty of discrete log
  - Consists of both encryption and signature algorithms
  - Cipher text is twice the size of plain text
  - It is slow
- **ELLIPTIC CURVE CRYPTOGRAPHY (ECC)**
  - In 1985, Neal Koblitz and Victor Miller - proposed using elliptic curves, however it only saw wide use in 2005
  - Majority of public-key crypto (RSA, D-H) uses large numbers and imposes a significant load in storing and processing keys and messages
  - ECC on the other hand uses elliptic curves and offers same security with smaller bit sizes
  - Even though RSA is still widely used, in recent times, ECC is becoming very popular, particularly after its use in crypto currencies

PUBLIC KEY + SYMMETRIC

- **PROBLEM**: Public key systems are powerful but slow, while symmetric systems are inflexible but fast.
- **SOLUTION**: A hybrid system!
  - Sender generates random symmetric session key
  - Sender encrypts session key using receivers' public key
  - Receiver decrypts it using his/her private key and now both have the shared session key
- **RESULT**: A fast, flexible system
- **HYBRID SCHEME**
- Combine advantages of symmetric and asymmetric ciphers
  - Throughput of symmetric cipher
  - Key management of asymmetric cipher
- A two-stage approach is used
  - In the first step public key cryptography is used to derive a session key.
  - Subsequently, the session key is used to encrypt the actual message.

HYBRID SYSTEM

DIGITAL SIGNATURES

- A digital signature ("digital thumbprint") is a message digest used to cryptographically sign a message.
- Digital signatures rely on asymmetric (public key) cryptography.
- To create a digital signature, you sign the message with your private key. The digital signature then becomes part of the message.
- This has two effects:
  - Any changes to the message can be detected, due to the message digest algorithm.
  - You can not deny signing the message, because it was signed with your private key.
- These two features, message integrity and non-repudiation, make digital signatures a very useful component for e-commerce applications.
- Digital signature can be used in all electronic communications
- It is an electronic stamp or seal that is append to the document.
- Ensure that the document remains unchanged during the transmission

KEY SIZE

- When deploying ciphers, the size of key is very important.
- The strength of many encryption applications and cryptosystems is measured by key size.
- For cryptosystems, the security of encrypted data is not dependent on keeping the encrypting algorithm secret.
- Cryptosystem security depends on keeping some or all of elements of key secret.
- **There are two keys**
- Private and Public key: These keys are used to exchange the symmetric key. For RSA algorithms, a key size of 2048 (2K) is considered safe.
- **Session key**: This is secret key (symmetric key), which is used during the communication between client and server. A key size of 128 or more is considered very reasonable. A key size of 256 is considered very safe and secure, however it will be slower than the algorithm with key size of 128. The key size also depend on the actual algorithm, as some algorithms use fixed key size, while others like AES, has different versions for different key sizes.

PROPERTIES OF DIGITAL SIGNATURES

- Only private-key holder can compute signatures.
- Any holder of matching public-key can verify signature.
- Digital signature schemes work with two major steps:
  - Prepare a message representative
  - Apply a signature transform.
- The general verifying method is generally similar to the signing method
  - Undo the signature transformation
  - Check the message digest for any issues
- **HOW DOES DIGITAL SIGNING WORK?**
- We extract a value (binary string) from the message with a hash function.
- We use a digital signature algorithm to produce the signature from the hash value and the private key.
- The message can now be authenticated with the public key and the signature

HOW DIGITAL SIGNATURE WORKS?

DIGITAL SIGNATURE

- **DIGITAL SIGNATURE SCHEME:** Two components
  - A private signing algorithm which permits a user to securely sign a message
  - A public verification algorithm which permits anyone to verify that the signature is authentic.
- **HASHING**
- A hashing algorithm is applied to a bit string of any length
- It is designed in such a way that every bit in the message has some effect on the resulting message digest.
- The message digest can then be input to the Digital Signature Algorithm (DSA) which generates or verifies the signature for the message

HASH FUNCTION PROPERTIES

Can be applied to a block of data of any size

Produces a fixed-length output

H(x) is relatively easy to compute for any given x

One-way or pre-image resistant

- Computationally infeasible to find x such that H(x) = h

Computationally infeasible to find y ≠ x such that H(y) = H(x)

Collision resistant or strong collision resistance

- Computationally infeasible to find any pair (x,y) such that H(x) = H(y)

Note that even small changes in the source input (here in the word "over") drastically change the resulting output.

Input		Digest
Fox	Cryptographic hash function	DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog	Cryptographic hash function	0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog	Cryptographic hash function	8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog	Cryptographic hash function	FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog	Cryptographic hash function	8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6AC6

DIGITAL SIGNATURE
(WITHOUT MESSAGE PROTECTION)

DIGITAL SIGNATURE
(WITH MESSAGE PROTECTION)

DIGITAL SIGNATURE EXAMPLE 1

(WITH MESSAGE PROTECTION)

DIGITAL SIGNATURE EXAMPLE 2

(WITH MESSAGE PROTECTION)

DIGITAL CERTIFICATES & CERTIFICATE AUTHORITIES

- 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 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
- For digital signatures to work, a trusted third party known as a Certification Authority (CA) is needed to issue digital certificates that certify the electronic identities of users and organisations.
- Some Trusted CA operating in Singapore
  - Verisign
  - GlobalSign
  - **Netrust Pte Ltd**

DIGITAL CERTIFICATE

- **Digital certificate includes:**
  - Name of subject/company
  - Subject's public key
  - Digital certificate serial number
  - Expiration date, issuance date
  - Digital signature of CA

I hereby certify that the public key
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
belongs to
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Birthday: July 4, 1958
Email: bob@superdupernet.com

SHA-1 hash of the above certificate signed with the CA's private key

1. Generate Key-pair

2. User-A requests CA Certificate

3. CA responds with its CA Certificate including its Public Key

4. Gather information

5. Request the Certificate which has User-A's identity and Public Key

6. CA verifies the identity of User-A

7. Issue the Certificate for User-A

Public-Key Infrastructure (PKI)

- Integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely
- PKI systems are based on public-key cryptosystems
- PKI protects information assets in several ways:
  - Authentication
  - Integrity
  - Privacy
  - Authorization
  - Nonrepudiation
- Typical PKI solution protects the transmission and reception of secure information by integrating:
  - A certificate authority (CA)
  - A registration authority (RA)
  - Certificate directories
  - Management protocols
  - Policies and procedures

WEB SECURITY

- Web is widely used by business, government and individuals. However, Internet & Web are vulnerable as it uses HTTP protocol.
- **HTTP IS NOT A SECURE PROTOCOL**
  - It is a simple and stateless client/server application running over TCP/IP.
- **WHAT ARE THE THREATS**
  - **INTEGRITY**
    - Data modification, insertion
  - **CONFIDENTIALITY**
    - Eavesdropping on the net
    - Theft from server machine
  - **AUTHENTICATION**
    - Impersonation, data forgery
  - **DENIAL OF SERVICE**
    - Hacked web servers

WEB SECURITY

- **ADDED SECURITY MEASURES NEEDED**
  - The SSL (Secure Socket Layer, originated by Netscape) and TLS (Transport Layer Security) was designed for web security. First version of TLS can be viewed as an SSLv3.1
- **HTTPS**
  - Secure HTTP protocol = HTTP+ SSL

SSL (SECURE SOCKET LAYER)

- Can provide server authentication with digital certificate (X509).
- It can authenticate client (rare).
- Can provide privacy by encryption.
- Can be used with any TCP app (**but mainly http, email**).
- **HISTORY**
  - Internal Netscape design, early 1994.
  - SSLv1 was broken by members of audience while it was being presented.
  - SSLv2 was shipped with Navigator 1.0, in November 1994, however it was vulnerable to man-in-the-middle attack.
  - SSLv3 was designed by **Netscape and Paul Kocher**, in November 1996 and was designed with public input/feedback.
  - SSL is easy to apply and use because it is built in all major Web browsers (IE, Opera, Chrome, Mozilla, Firefox) and servers.

TRANSPORT LAYER SECURITY (TLS)

- By the end of the 1990s, Netscape handed SSL over to the IETF(Internet Engineering Task Force).
- The (IETF), renamed SSL 3 as Transport Layer Security (TLS) in 1999 and made SSL obsolete in 2015.
  - SSL version 3.0 was adopted by Internet Engineering Task Force (IETF) as TLS version 1.0.
  - All TLS versions up to 1.2 were backward-compatible with SSL 3.0, however, backward compatibility with SSL was removed from TLS 1.3.
  - The latest version: TLS1.3 (Finalized on March 21st, 2018).
  - Many people still refer to web encryption as SSL, even though the vast majority of services have switched over to supporting TLS only.

ONLINE CREDIT CARD TRANSACTION (SSL)

ISSUES WITH SSL/TLS

- It slows down servers.
- It protects data in transit, but not databases.
- SSL/TLS **Cannot**:
  - Authenticate the actual operator of a computer
  - Authenticate the owner of an online shop (merchant)
  - Authenticate the actual online consumer
  - Authenticate other parties involved in online payment system
  - Protect the use of stolen credit cards online

Securing Wireless Networks with WEP and WPA

- Wired Equivalent Privacy (WEP): Early attempt to provide security with the 8002.11 network protocol. 1999 -2004: Easy to break and hard to configure.
- Wi-Fi Protected Access (WPA, WPA2 and WPA3): Created to resolve issues with WEP.
- WPA was used as a temporary enhancement for WEP. Easy to break and moderate configuration difficulty.
- WPA2 (version 2): Provides good security and offers normal level of configuration. It was introduced in 2004. It used AES for encryption.
- WPA3: Next Generation Wireless Protocols: Offers excellent security and easy to configure.

SUMMARY

- Cryptography and encryption provide sophisticated approach to security.
- Many security-related tools use embedded encryption technologies.
- Encryption converts a message into a form that is unreadable by the unauthorized.
- Many tools are available and can be classified as symmetric or asymmetric, each having advantages and special capabilities.
- Strength of encryption tool is dependent on the key size but even more dependent on following good management practices.
- Cryptography is used to secure most aspects of Internet and Web today.