Protecting Information Assets
- Week 13 -

Review: Security Threats and Mitigation

MIS5206 Week 14

- Cases Study
- Review of Week 7 – 12 Materials
  - Physical and Environmental Security
  - Business Continuity and Disaster Recovery Planning
  - Network Security
  - Identity Management and Access Control
  - Application Development Security
  - Cryptography, Public Key Encryption and Digital Signatures
- Quiz

Physical and Environmental Security

Physical security addresses the physical protection of the resources of an organization, which include people, data, facilities, equipment, systems, etc. It concerns with people safety, how people can physically enter an environment and how the environmental issues affect equipment and systems. People safety always takes precedence over the other security factors.

Physical Control Types

Administrative Controls	Facility selection, facility construction and management, personnel control, evacuation procedure, system shutdown procedure, fire suppression procedure, handling procedures for other exceptions such as hardware failure, bomb threats
Physical Controls	Facility construction material, key and lock, access card and reader, fences, lighting
Technical Controls	Physical access control and monitoring system, intrusion detection and alarm system, fire detection and suppression system, uninterrupted power supply, heating / ventilation / air conditioning system (HVAC), disk mirroring, data backup

Sources of Physical Threats

- ***Weather*** *- temperature, humidity, water, flood, wind, snow, lightening*
- ***Fire and Chemical*** *- explosion, smoke, toxic material, industrial pollution*
- ***Earth Movement*** *- earthquake, volcano, mud slide*
- ***Object Movement*** *- building collapse, falling object, car, truck, plane*
- ***Energy*** *- electricity, magnetism, radio wave anomalies*
- ***Equipment*** *- mechanical or electronic component failure*
- ***Organism*** *- virus, bacteria, animal, insect*
- ***Human*** *- strike, war, sabotage*

Facilities – Site Selection

- **Visibility** - surrounding terrain, markings and signs
- **Local Considerations** - crime rate, adjacent neighbors, proximity to police and fire station
- **Transportation** - road access and traffic condition, proximity to airport and train station
- **Natural Threats** - likelihood of flood, earthquake, or other natural threats.

Facilities – Data Center

- Should not be located on the top floor because of risk of fire
- Should not be in the basement - flooding risk
- Ideally in the core of a building - provides protection from natural disasters and intrusion
- Should not be close to a public area – to ease security

Design Considerations

Walls - fire rating (level of fire protection and combustibility), load (the maximum weight it can hold), floor to ceiling barrier, reinforcement for secured area.

Partitions – considerations similar to those of wall, plus the requirement of extension above drop ceiling (if there is no extension, an intruder can lift the ceiling panels and climb above the partition).

Doors – fire rating (should be equal to that of the surrounding walls), emergency marking, directional opening, resistance from being forced open, intrusion detection alarm, fail-soft vs fail-safe lock (i.e. lock that is unlocked or locked in a power outage), placement of doors.

Windows – characteristics of windows material (opaque, translucent, transparent,shatterproof, bulletproof), intrusion detection alarm, placement of windows.

Ceilings – fire rating, load, waterproof (preventing water leakage from the upper floor), drop ceiling.

Floor – fire rating, load, raised floor, electrical grounding (for raised floor), non-conducting material.

Heating, ventilation, and air conditioning (HVAC) – independent power source, positive air pressure to avoid contamination of the room, protected intake vents to prevent tampering, monitoring of environmental condition, emergency power off, placement of HVAC

Power supplies – backup power supply, clean power supply, circuit breaker, access to power distribution panels, placement of power sockets.

Liquid and gas lines – shutoff valve, positive flow, leakage sensor, placement of liquid and gas lines.

Fire detection and suppression – fire or smoke detector and alarm, sprinkler, gas discharge system, placement of detectors and sprinkler heads.

Emergency lighting – essential power supply and battery for emergency lighting

Access Control and Auditing

Physical access control mechanisms include:

- Lock and key
- Access card and reader
- Fence
- Lighting
- Doorway and Man-trap

Perimeter Control

Fencing is another physical access control mechanism. Fences of different heights can serve different purposes:

- 3 – 4 feet – deter casual trespassers
- 6 – 7 feet – deter general intruders
- 8 feet with strands of barbed wire (slant at a 45 angle) to deter more determined intruders

PIDAS - Perimeter intrusion and detection assessment system is a fencing system with mesh wire and passive cable vibration sensors that can detect if an intruder is approaching and damaging the fence. However, it may generate many false alarms.

Bollards are small and round concrete pillars that are constructed and placed around a building to protect it from being damaged by someone running a vehicle into the side of the building.

Lighting - streetlight, floodlight or searchlight is a good deterrent for unauthorized access. It can also provide safety for personnel. The National Institute of Standards and Technology (NIST) standard requires critical areas to be illuminated 8 feet in height with 2-foot candle power.

Physical Access Monitoring

- **Patrol force / security guard**
  - Good deterrent to intrusion
  - Can provide flexible security and safety response
  - Can be expensive.
  - Reliability of security guards is an issue.
  - Re-employment screening and other background checking are required.
  - Training against social engineering is

- **Dogs**
  - Very effective in detecting intruders
  - They are loyal, intelligent
  - Can be trained to recognize specific smells like smoke, for instance

Fire Protection

Combustion elements which can sustain a fire are:

Fuel - wood, paper, wiring, etc. - can be suppressed by CO2 or Soda acid

Oxygen - can be suppressed by CO2 or Soda acid

Temperature - can be reduced by water

Chemical - can be suppressed by Halon, which interferes with the chemical reaction

Fire Protection

The 4 classes of fire are:

Class	Description	Element of fire	Suppression method
A	Common combustibles	Miscellaneous, e.g. wood, paper, etc.	Water, Soda acid
B	Liquid	Petroleum products, coolants, etc.	Halon, CO_2, Soda acid
C	Electrical	Electrical equipment, wires, etc.	Halon, CO_2
D	Combustible metal	Magnesium, sodium, etc.	Dry powder

Power Protection

Uninterrupted Power Supply (UPS) to protect against a short duration power failure.

There are two types of UPS:

- Online UPS – It is in continual use because the primary power source goes through it to the equipment. It uses AC line voltage to charge a bank of batteries. When the primary power source fails, an inverter in the UPS will change DC of the batteries into AC.
- Standby UPS – It has sensors to detect for power failures. If there is a power failure, the load will be switched to the UPS. It stays inactive before a power failure, and takes more time than online UPS to provide power when the primary source fails.

Protecting Information Assets
- Week 8 -

Business Continuity and Disaster Recovery Planning

Business Continuity and Disaster Recovery Planning

Operating disruptions can occur with or without warning. The results may be predictable or unanticipated. It is important that the mission of the enterprise is sustained during any emergency. The first priority is always the safety of the people: Employees, Service and Support Staff and Visitors.

Business Continuity
- versus -
Disaster Recovery

Business Continuity Planning	Planning for the purpose of developing a "Roadmap" for continuing operations under adverse conditions after a natural or human-induced interruption
Disaster Recovery Planning	Planning in preparation for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster

BCP Process

- Project Initiation & Management
- Business Impact Analysis (BIA)
- Recovery Strategies Development
- Plan Design & Development
- Testing, Maintenance, Awareness, Training

… Repeat

Disaster Recovery Planning

- Establish a planning group
- Perform risk assessment and audits
- Establish priorities for applications and networks
- Develop recovery strategies
- Prepare inventory and documentation of the plan
- Develop verification criteria and procedures
- Implement the plan

Computer Operations

Areas of Focus:

- Sites/ Locations/ Facilities
- Computers and Infrastructure (Hardware)
- Operating Systems
- Applications (software)
- Data
- Supplies
- Documentation
- Personnel

Application Systems

Classification of Applications*

Classification		Description
1	Mission Critical	Mission Critical to accomplishing the mission of the organization Can be performed only by computers No alternative manual processing capability exists Must be restored within 36 hours
2	Critical	Critical in accomplishing the work of the organization Primarily performed by computers Can be performed manually for a limited time period Must be restored starting at 36 hours and within 5 days
3	Essential	Essential in completing the work of the organization Performed by computers Can be performed manually for an extended time period Can be restored as early as 5 days, however it can take longer

* From SANS

Audit Focus Areas

Areas for audit evaluation:

Figure 3—Possible Tests/Procedures for Backup and Recovery	
Data	• Review or observe backup procedures. • Review documentation of a successful restore (within the last year). • Verify restoration personally (when risk is high or restoration is an audit objective).
Site/computers/ OS	• Review the provisions of the BCP/DRP. • Review a contract (hot site, cold site, mutual aid, etc.). • Verify the ability to restore these aspects.
Applications	• Review the plan's provisions. • Review the critical applications list, including ranking. • Verify the ability to restore (personally, when risk is high or restoration is an audit objective). • Observe or inquire about the backups of application software and location.
Supplies/ documentation	• Review the plan's provisions. • Observe or inquire about the provisions and location.
Recovery team	• Review the plan's provisions. • Interview one or more members of the team, and ask about roles and responsibilities. • Gain assurance that there is provision for adequate personnel for a successful restoration.

DRP Testing Approaches

- Conducting a structured walk-through
- Conduct Dry-Run tests
  - Can be conducted on a function by function basis
  - Do not have test all functions for each cycle
  - Tests should involve actual interruptions and recoveries
- A tracking matrix should be created and maintained to track performance across multiple periods
- Business Process changes must be tracked and specific test scenarios created to ensure the existing recovery processes will support the new scenarios
- Test should demonstrate and document that roles are clearly defined and understood

Network Security

The purpose of network security, quite simply, is to protect the network and its component parts from unauthorized access and misuse.

What do we mean by "Network?"

Private Network

The company's Intranet is a private network. But, more often than not, companies depend on 3rd party service providers to carry their private network traffic in an encrypted form over their networks. So, the definition of Private Network refers to a logical network used for secure company only traffic. The growing popularity of Cloud computing has led to the development of "private clouds" that extend the company's private network into other 3rd party domains.

Public Network

The Internet refers to the public portions of the network. Many companies depend on public network connections with their clients in order to do business. The popularity of the public Cloud continues to complicate the extent to which the public network may be a vehicle for company specific communications.

Network Components

Networks are complex electronic communications systems with a very large number of possible components. This makes this systems potentially open to many vulnerabilities. The list below, while largely comprehensive is not complete.

- Gateways
- Routers
- Network bridges
- Switches
- Hubs
- Repeaters
- Multilayer switches
- Protocol converters
- Bridge routers
- Proxy servers
- Firewalls
- NAT - network address translators
- Multiplexers
- Network interface controllers
- Wireless network interface controllers
- Modems
- ISDN terminal adapters
- Wireless access points

Types of Network Attacks

Eavesdropping	The majority of network communications occur in an unsecured or "clear text" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.
Data Modification	After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if you do not require confidentiality for all communications, you do not want any of your messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.
Identity Spoofing (IP Address Spoofing)	Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data. The attacker can also conduct other types of attacks, as described in the following sections.
Password-Based Attacks	Most operating systems and network security use password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password. Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user. When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.

Types of Network Attacks

Denial-of-Service Attack

The the denial-of-service attack prevents normal use of your computer or network by valid users. After gaining access to your network, the attacker can do any of the following:

- Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

Man-in-the-Middle Attack

As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data. Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying as you to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section.

Compromised-Key Attack

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

Types of Network Attacks

Sniffer Attack

A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key.

Using a sniffer, an attacker can do any of the following:

- Analyze your network and gain information to eventually cause your network to crash or to become corrupted
- Read your communications

Application-Layer Attack

An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

- Read, add, delete, or modify your data or operating system.
- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
- Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.
- Abnormally terminate your data applications or operating systems.
- Disable other security controls to enable future attacks.

Firewalls

Used to filter packets based on a combination of features

- These are called packet filtering firewalls
- Can use any combination of IP/UDP/TCP header information
- Ex. Drop packets with destination port of 23 (Telnet)

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Network Port Designations

Service	Port	Function Name
FTP	20, 21	File Transfer Protocol
SSH	22	Secure Shell
Telnet	23	Telnet
SMTP	25	Simple Mail Transfer Protocol
DNS	53	Domain Name Services
DHCP	67, 68	Dynamic Host Configuration Protocol
TFTP	69	Trivial File Transfer Protocol
HTTP	80	Hyper-Text Transfer Protocol
POP3	110	Post Office Protocol 3
NNTP	119	Network News Transport Protocol
NTP	123	Network Time Protocol
IMAP4	143	Internet Message Access Protocol
LDAP	389	Lightweight Access Directory Protocol
HTTPS	443	Secure Hyper-Text Transfer Protocol
IMAPS	993	Secure Internet Message Access Protocol
RADIUS	1812	Remote Authentication Dial In User Service
AIM	5190	AOL Instant Messenger

Intrusion Detection

Used to monitor for "suspicious activity" on a network

- Can protect against known software exploits, like buffer overflows

Uses "intrusion signatures"

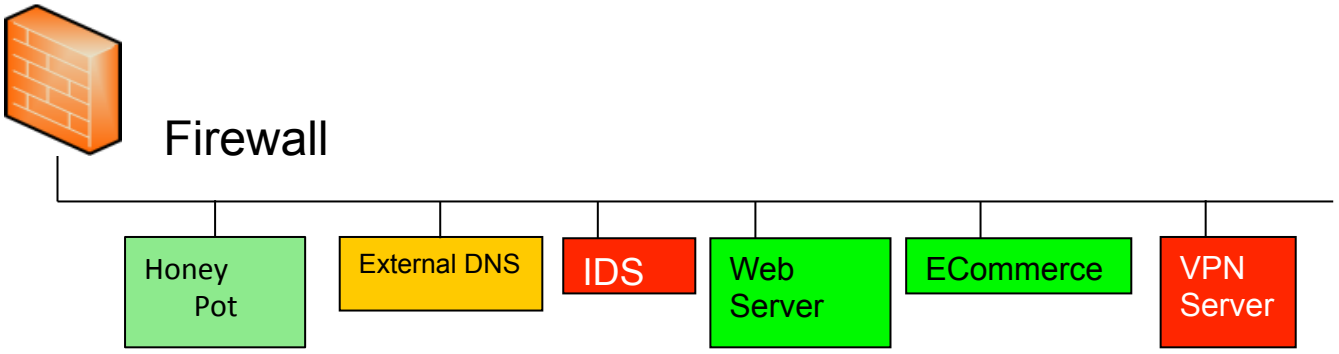
- Well known patterns of behavior
  - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc.

Honeypots & Honeynets

Honeypot: A system with a special software application which appears easy to break into

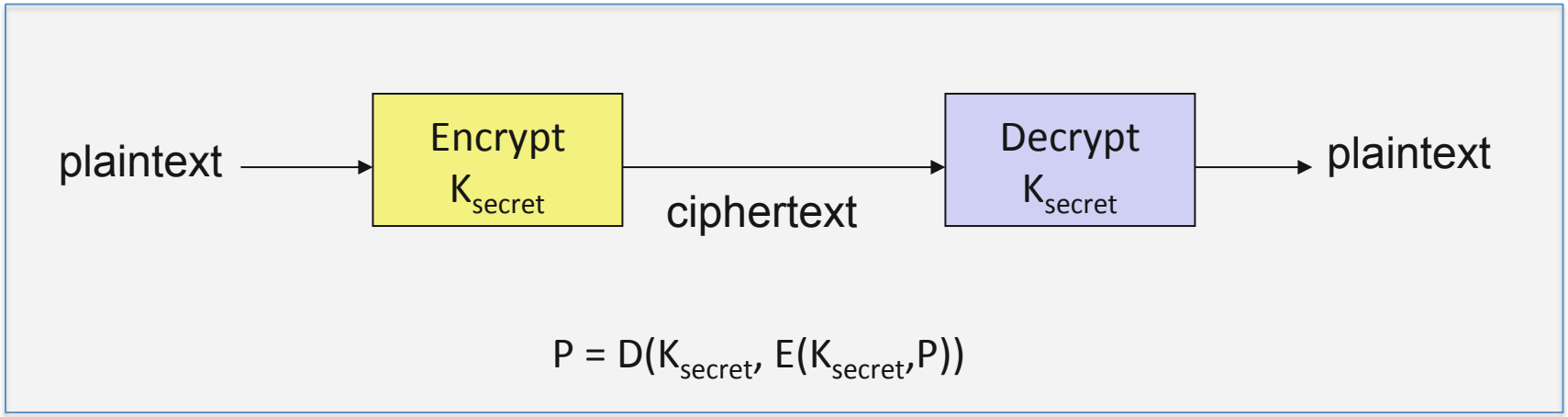
Honeynet: A network which appears easy to break into

- Purpose: Catch attackers
- All traffic going to honeypot/net is suspicious
- If successfully penetrated, can launch further attacks
- Must be carefully monitored



Encryption

Encryption is more and more becoming the standard for data transmission *and* storage in large companies



Identity Management and Access Control

Business owners and managers are constantly identifying areas of security risk and taking steps to mitigate that risk. In an IT environment, risk takes the form of access.

What do we mean by “Access Control”

- Access is the ability to create a flow of information between user and system

- Access Controls are security features that control how users and systems communicate and interact with one another

Access Control Principles

Three main security principles apply to access control:

Confidentiality
Integrity
Availability

What's the difference between Identification, Authentication and Authorization?

Identification, Authentication and Authorization are distinct functions

Identification: Who you say you are

Authentication: Confirmation that you are who you say you are

Authentication: What privileges you are allowed based on who you are

Identification

Identification

Method of establishing the subject's (user, program, process) identity

- Use of user name or other public information
- Know identification component requirements

Authentication

- Authentication
  - Method of proving the identity.
    - Something a person is, has, or does.
    - Use of biometrics, passwords, passphrase, token, or other private information.

Authentication

Most common biometric systems:

- Fingerprint
- Palm Scan
- Hand Geometry
- Iris Scan
- Signature Dynamics
- Keyboard Dynamics
- Voice Print
- Facial Scan
- Hand Topography

Authentication

- Biometric systems can be hard to compare
- Type I Error: False rejection rate
- Type II Error: False acceptance rate
  - This is an important error to avoid

Authentication

Passwords

- User name + password most common identification, authentication scheme
- Weak security mechanism, must implement strong password protections

Authentication

Techniques to attack passwords

- Electronic monitoring
- Access the password file
- Brute Force Attacks
- Dictionary Attacks
- Social Engineering

Authentication

Passphrase

- Is a sequence of characters that is longer than a password
- Takes the place of a password
- Can be more secure than a password because it is more complex

Authentication

Token Devices

- Synchronous
  - Time Based
  - Counter Synchronization
- Asynchronous

Authentication

Hashing & Encryption

- Hash or encrypting a password to ensure that passwords are not sent in clear text (means extra security)
- Salts: Random values added to encryption process for additional complexity.

Authentication

- Cryptographic Keys
  - Use of private keys or digital signatures to prove identity
- Private Key
- Digital Signature
  - Beware digital signature vs. digitized signature.

Authorization

Authorization

– Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources

Authorization

Access Criteria can be based on:

- Roles
- Groups
- Location
- Time
- Transaction Types

Authorization

Authorization Concepts

- Authorization Creep
- Default to Zero
- Need to Know Principle
- Access Control Lists

Authorization

Complexity leads to problems in controlling access:

- Different levels of users with different levels of access
- Resources may be classified differently
- Diverse identity data
- Corporate environments keep changing

Authorization

Advantages of centralized administration and single sign on:

- User provisioning
- Password synchronization and reset
- Self service
- Centralized auditing and reporting
- Integrated workflow (increase in productivity)
- Regulatory compliance

Authorization

- Single Sign On Capabilities
  - Allow user credentials to be entered one time and the user is then able to access all resources in primary and secondary network domains
- SSO technologies include:
  - Kerberos
  - Sesame
  - Security Domains
  - Directory Services

Access Control Models

Access Control Models:

- Discretionary
- Mandatory
- Role Based

Access Control Models

- Discretionary Access Control (DAC)
  - A system that uses discretionary access control allows the owner of the resource to specify which subjects can access which resources.
  - Access control is at the discretion of the owner.

Access Control Models

Mandatory Access Control (MAC)

- Access control is based on a security labeling system. Users have security clearances and resources have security labels that contain data classifications.
- This model is used in environments where information classification and confidentiality is very important (e.g., the military).

Access Control Models

- Role Based Access Control Models
  - Role Based Access Control (RBAC) uses a centrally administered set of controls to determine how subjects and objects interact.
  - Is the best system for an organization that has high turnover.

Access Control Techniques

Different access controls and technologies available to support the different models

- Rule Based Access Control
- Constrained User Interfaces
- Access Control Matrix
- Content Dependent Access Control
- Context Dependent Access Control

Access Control Techniques

Types of Centralized Access Control

- Radius - Remote Authentication Dial In User Service
- TACACS -Terminal access controller access control system
- Diameter - name is a pun on the RADIUS protocol

Application Development Security

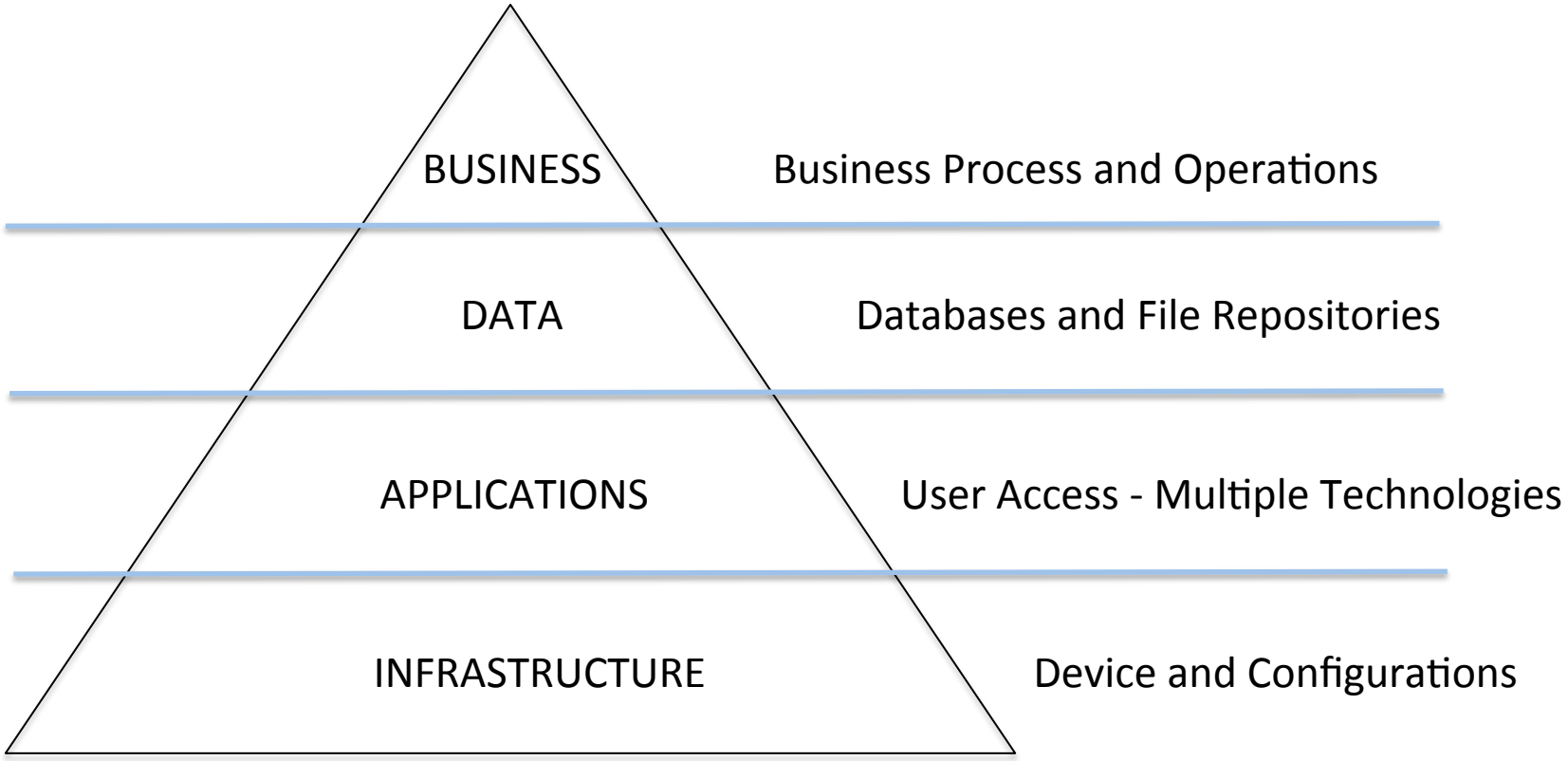
As applications become more accessible though the web, cloud and mobile devices, companies are being forced to abandon their reactive approach to security and, instead, to take a proactive approach by minimizing risk directly in the software they buy and create to serve their customers.

Best Practice: Build Security In

Security Architecture	Creation of, communications of and enforcement of System Architecture standards provides the basic building blocks for developing, implementing and maintaining secure application
Systems Development Life Cycle	Attention to security throughout the Systems Development Lifecycle is the key to creating secure, manageable applications regardless of platform or technologies
Procurement Standards	Describing the process and detailed criteria that will be used assess the security level of third party software enables companies to make strategic, security-sensitive decisions about software purchases

Security Architecture

Security strategy needs to be a consideration at each level of the architecture



Security System Development Lifecycle

- Phase 1: Initiation
- Phase 2: Development/Acquisition
- Phase 3: Implementation
- Phase 4: Operations/Maintenance
- Phase 5: Disposal

Phase 1: Initiation

- Data Sensitivity Assessment
- Preliminary Risk Assessment (RA)
- Review Solicitations (e.g. Request for Proposals - RFPs)

Phase 2: Development/Acquisition

- Functional and Technical Features/ Requirements
- Staff background Checks
- Operational Practices
- Test Plans, Scripts, and Scenarios
- Security Controls in Specifications

Phase 2: Development/Acquisition

In-House Concerns:

- Security features
- Development process
- Changing requirements
- Threats
- Vulnerabilities
- Malicious insiders

Phase 2: Development/Acquisition

- COTS Applications
- Operational Practices
  - System Security Plan (SSP)
  - Contingency Plan (BCP/DRP)
  - Awareness
  - Training
  - Documentation

Phase 3: Implementation

- Testing and Accreditation
  - Test Data
  - Test unit, subsystem, and entire system
  - Technical evaluation
- Security Management - administrative controls and safeguards

Phase 3: Implementation

- Physical facilities
- Personnel, responsibilities, job functions, and interfaces
- Procedures (e.g. backup, labeling)
- Use of commercial or in-house services

Phase 3: Implementation

- Disaster Recovery Plan (DRP)
- COTS products (security patches?)
- Remove installation programs
- Machine content/intent
- File and program overlay settings and privileges

Phase 3: Implementation

- Backup, restore, and restart instructions and procedures
- Implementation backups (could server as benchmark)
- Ensure implementation of only approved/accredited systems

Phase 4: Operations/Maintenance

- Backup and restoration parameters
- Performing backups
- Support training classes
- Cryptography keys
- User administration and access privileges
- Audit logs

Phase 4: Operations/Maintenance

- Log file analysis
- Security software
- Physical protection
- Off-site storage
- Output distribution
- Software & hardware warrantees
- Registration/Deregistration

Phase 4: Operations/Maintenance

- Operational Assurance Activities:
  - Review runtime operation
  - Review technical controls
  - Verify documentation of access permissions
  - Review system interdependencies
  - Verify that documentation is current
  - Verify proper use of deregistration
  - Verify that documentation is accurate

Phase 5: Disposal

- Storage of cryptographic keys
- Legal requirements of records retention
- Archiving federal information
- Sanitize media

Procurement Security Considerations

Differ based on type of procurement

- Software purchase
  - Commercial Off-The-Shelf (COTS)
  - Custom development
- Outsourcing of services
  - Not just software
- Software as a service
  - e.g. Online Tax Services

COTS Software

- Clout is key
  - Big markets: U.S. Government?
- Security requirements definition in RFP is important
  - Possible product differentiator
- Contract security language
  - Growing importance and emphasis
- Major vendors starting to “see the light”

Custom Software

- Software security and vendor requirements need to be specific and detailed
- Education may be necessary
- Possible vendor differentiator
- Ongoing patching and support is important

Outsourcing

- Services and hosting as well as software
- Define security goals and policies
- Ensure outsourcing maintains the same level of compliance
- Beware of sub-outsourcing

Software as a service

- Who controls the data?
- Is security adequate for all types of data?
  - Map to data classification
- Ensure service maintains compliance with policies and security goals
- Don't forget e-Discovery

Cryptography, Public Key Encryption and Digital Signatures

Cryptography allows people to carry over the confidence found in the physical world to the electronic world. It allows people to do business electronically without worries of deceit and deception. Every day hundreds of thousands of people interact electronically, whether it is through e-mail, e-commerce, ATM machines or cellular phones using Cryptography.

Cryptography Overview

- Reasons for Cryptography
- Terms
- Symmetric and Asymmetric Algorithms
- Hashing
- PKI Concepts
- Attacks on Cryptosystems

Reasons to Use Cryptography

Reason	Explanation
Confidentiality	Only authorized entities are allowed to view
Integrity	Ensures the message was not altered by unauthorized individuals
Authenticity	Sequence that controls the operation and behavior of the cryptographic algorithm
Nonrepudiation	Establishes sender identity so that the entity cannot deny having sent the message
Access Control	Access to an object requires access to the associated crypto keys in many systems (e.g. login)

Cryptography Terms

TERM	DEFINITION
Plaintext	A message in its natural format readable by an attacker
Ciphertext	Message altered to be unreadable by anyone except the intended recipients
Key	Sequence that controls the operation and behavior of the cryptographic algorithm
Keyspace	Total number of possible values of keys in a crypto algorithm
Initialization Vector	Random values used with ciphers to ensure no patterns are created during encryption
Cryptosystem	The combination of algorithm, key, and key management functions used to perform cryptographic operations

Symmetric versus Asymmetric Encryption

Symmetric

- Same key used for encryption and decryption
- Secure key distribution is a problem

Asymmetric

- Mathematically related key pairs for encryption and decryption
- Public and private keys

Cryptographic Methods

Hybrid

- Combines strengths of both methods
- Asymmetric distributes symmetric key
  - Also known as a ***session key***
- Symmetric provides bulk encryption
- Example:
  - SSL negotiates a hybrid method

Attributes of Strong Encryption

Confusion

- Change key values each round
- Performed through substitution
- Complicates plaintext/key relationship

Diffusion

- Change location of plaintext in ciphertext
- Done through transposition

Common Symmetric Algorithms

TERM	DEFINITION
DES (Data Encryption Standard)	- 64 bit key that is effectively 56 bits in strength - Algorithm is called DEA (Data Encryption Algorithm) - DES Modes • Electronic Code Book • Cipher Block Chaining (most commonly used for general purpose encryption) • Cipher Feedback • Output Feedback • Counter Mode (used in IPSec)
3DES	- 112-bit effective key length - Uses either 2 or 3 different smaller keys in one of several modes - Modes • EEE2/3 • EDE2/3
IDEA	- International Data Encryption Algorithm - Operates on 64 bit blocks in 8 rounds with 128 bit key - Considered stronger than DES and is used in PGP

Common Symmetric Algorithms

TERM	DEFINITION
AES	- NIST replaced DES in 1997 with this - Uses the Rijndael algorithm - Supports key/block sizes of 128, 192, and 256 bits - Uses 10/12/14 rounds as block size increases
Blowfish	64 bit block cipher with up to 448 bit key and 16 rounds

The Rijndael encryption algorithm was designed to replace the aging DES algorithm. Like DES, it is a block cipher. It uses 128-bit, 192-bit or 256-bit keys. This implementation encrypts 128-bit blocks. (DES used 56-bit keys and 64-bit blocks.)

Common Asymmetric Algorithms

TERM	DEFINITION
Diffie-Hellman	- First widely known public key cryptography algorithm - Computes discrete logarithms over a finite field - Provides means for secure key exchange over insecure channel
RSA	- Stands for inventors names, Rivest, Shamir, and Adleman - Relies on difficulty of finding prime factorization of large numbers
El Gamal	- Based on Diffie-Hellman method of computing discrete logarithms - Can also be used for message confidentiality and digital signature services
Elliptic Curve Cryptography	- Relies on computing discrete logarithms over elliptic curve group - Due to difficulty of problem, key sizes can be much smaller than RSA and still retain strength - Used in Mobile phone systems

What is Hashing?

A hash function is any algorithm that maps large data sets of variable length to smaller data sets of a fixed length.

The values returned by a hash function are called hash values, hash codes, hash sums, checksums or simply hashes.

Common Hashing Algorithms

MD5

- Computes 128-bit hash value
- Widely used for file integrity checking

SHA-1

- Computes 160-bit hash value
- NIST approved message digest algorithm

Birthday Attack

- Collisions
  - Two messages with the same hash value
- Based on the "birthday paradox"
- Hash algorithms should be resistant to this attack

The birthday paradox, also known as the birthday problem, states that in a random group of 23 people, there is about a 50 percent chance that two people have the same birthday.

Is the Birthday Attack Real?

- There are multiple reasons why this seems like a paradox.
- One is that when in a room with 22 other people, if a person compares his or her birthday with the birthdays of the other people it would make for only 22 comparisons—only 22 chances for people to share the same birthday.

When all 23 birthdays are compared against each other, it makes for much more than 22 comparisons. How much more? Well, the first person has 22 comparisons to make, but the second person was already compared to the first person, so there are only 21 comparisons to make. The third person then has 20 comparisons, the fourth person has 19 and so on. If you add up all possible comparisons (22 + 21 + 20 + 19 + … +1) the sum is 253 comparisons, or combinations. Consequently, each group of 23 people involves 253 comparisons, or 253 chances for matching birthdays.

Message Authentication Codes

- Small block of data generated with a secret key and appended to a message
- HMAC (RFC 2104)
  - Uses hash instead of cipher for speed
  - Used in SSL/TLS and IPSec

Digital Signatures

- Hash of message encrypted with private key
- Digital Signature Standard (DSS)
  - DSA/RSA/ECD-SA plus SHA
- DSS provides
  - Sender authentication
  - Verification of message integrity
  - Nonrepudiation

Encryption Management

- Key Distribution Center (KDC)
  - Uses master keys to issue session keys
  - Example: Kerberos
- ANSI X9.17
  - Used by financial institutions
  - Hierarchical set of keys
  - Higher levels used to distribute lower

ANSI X9.17-1985, Financial Institution Key Management (Wholesale), is a voluntary standard that utilizes the Data Encryption Standard (DES) to provide key management solutions for a variety of operational environments.

Public Key Infrastructure

- All components needed to enable secure communication
  - Policies and Procedures
  - Keys and Algorithms
  - Software and Data Formats
- Assures identity to users
- Provides key management features

PKI Components

Digital Certificates

- Contains identity and verification info

Certificate Authorities

- Trusted entity that issues certificates

Registration Authorities

- Verifies identity for certificate requests

Certificate Revocation List (CRL)

PKI Cross Certification

- Process to establish a trust relationship between CAs
- Allows each CA to validate certificates issued by the other CA
- Used in large organizations or business partnerships

Cryptanalysis

- The study of methods to break cryptosystems
- Often targeted at obtaining a key
- Attacks may be passive or active

Although the actual word "cryptanalysis" is relatively recent (it was coined by William Friedman in 1920), methods for breaking codes and ciphers are much older. The first known recorded explanation of cryptanalysis was given by 9th-century Arabian polymath, Al-Kindi (also known as "Alkindus" in Europe), in A Manuscript on Deciphering Cryptographic Messages. This treatise includes a description of the method of frequency analysis

Cryptanalysis

- Kerckhoff's Principle
  - The only secrecy involved with a cryptosystem should be the key
- Cryptosystem Strength
  - How hard is it to determine the secret associated with the system?

Cryptanalysis Attacks

- Brute force
  - Trying all key values in the keyspace
- Frequency Analysis
  - Guess values based on frequency of occurrence
- Dictionary Attack
  - Find plaintext based on common words

Cryptanalysis Attacks

- Replay Attack
  - Repeating previous known values
- Factoring Attacks
  - Find keys through prime factorization
- Known Plaintext
  - Format or content of plaintext available

Cryptanalysis Attacks

- Chosen Plaintext
  - Attack can encrypt chosen plaintext
- Chosen Ciphertext
  - Decrypt known ciphertext to discover key
- Differential Power Analysis
  - Side Channel Attack
  - Identify algorithm and key length

Cryptanalysis Attacks

- Social Engineering
  - Humans are the weakest link
- RNG Attack
  - Predict IV used by an algorithm
- Temporary Files
  - May contain plaintext

Early versions of Netscape's Secure Socket Layer (SSL) encryption protocol used pseudo-random quantities derived from a PRNG seeded with three variable values: the time of day, the process ID, and the parent process ID. These quantities are often relatively predictable, and so have little entropy and are less than random, and so that version of SSL was found to be insecure as a result.

Practical Cryptanalysis

- DES Cracker:
  - A DES key search machine
  - contains 1536 chips
  - Cost: $250,000.
  - could search 88 billion keys per second
  - won RSA Laboratory's "**DES Challenge II-2**" by successfully finding a DES key in 56 hours.

E-mail Security Protocols

- Privacy Enhanced Email (PEM)
- Pretty Good Privacy (PGP)
  - Based on a distributed trust model
  - Each user generates a key pair
- S/MIME
  - Requires public key infrastructure
  - Supported by most e-mail clients

Network Security

Link Encryption

- Encrypt traffic headers + data
- Transparent to users

End-to-End Encryption

- Encrypts application layer data only
- Network devices need not be aware

Network Security

SSL/TLS

- Supports mutual authentication
- Secures a number of popular network services

IPSec

- Security extensions for TCP/IP protocols
- Supports encryption and authentication
- Used for VPNs

Quiz