Introduction to Computer Security

What Is Computer Security?

- The protection of the assets of a computer system
  - Hardware
  - Software
  - Data

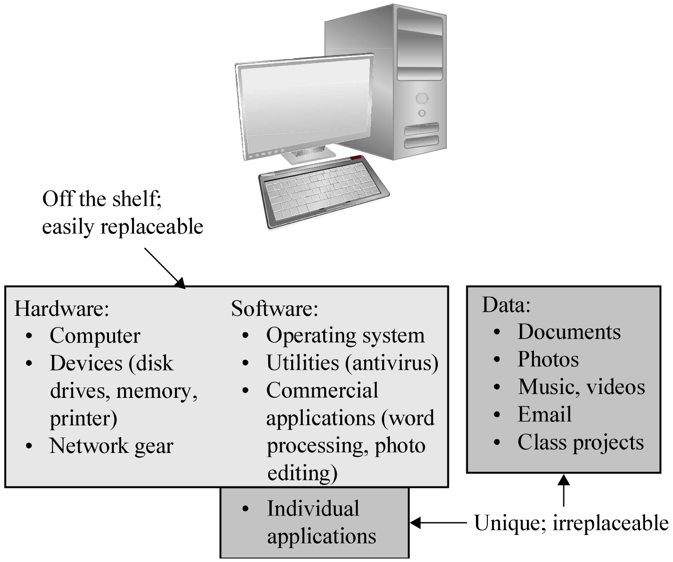
Assets

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

Values of Assets



Off the shelf; easily replaceable

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

Unique; irreplaceable

Basic Terms

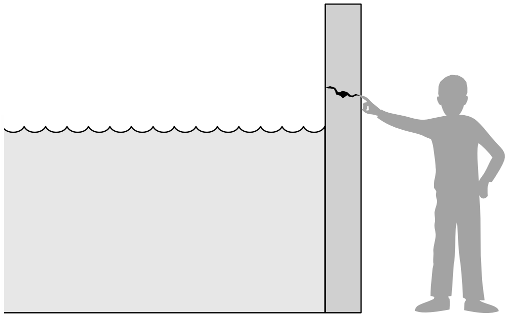
- Vulnerability
- Threat
- Attack
- Countermeasure or control

Threat and Vulnerability

Relationship among threats, controls, and vulnerabilities:

- A threat is blocked by control of a vulnerability.
- To devise controls, we must *know as much about threats as possible*.

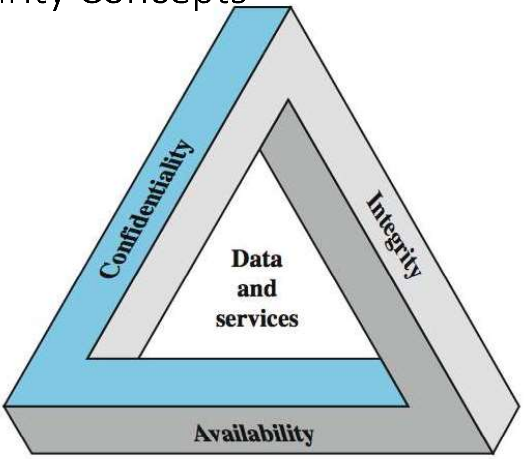
The fact that the violation might occur means that the actions that might cause it should be guarder against.



Vulnerabilities, Threats, Attacks, Controls

- **Vulnerability** is a weakness in the security system
  - (i.e., in procedures, design, or implementation), that might be exploited to *cause loss or harm*.
- **Threat** to a computing system is a set of circumstances that has the *potential to cause loss or harm*.
  - a potential violation of security
- A human (*criminal*) who exploits a vulnerability perpetrates an **attack** on the system.
- How do we address these problems?
  - We use a **control** as a protective measure.
  - That is, a control is an action, device, procedure, or technique that *removes or reduces a vulnerability*.

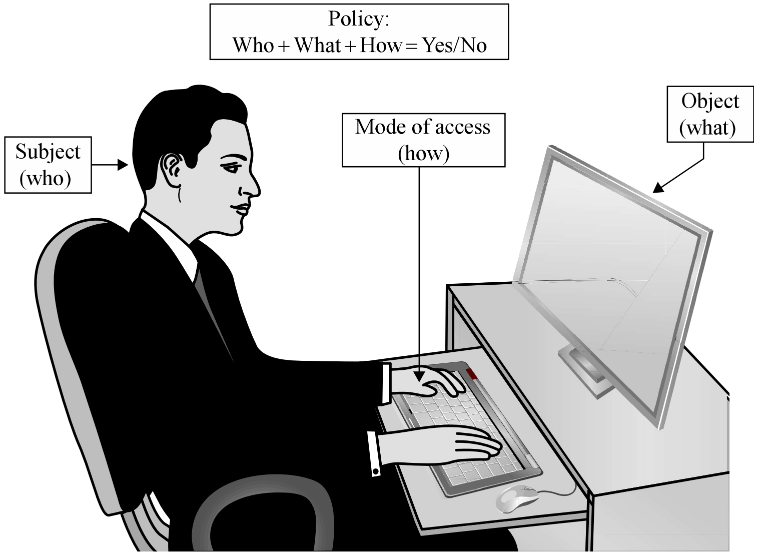
Key Security Concepts



C-I-A Triad

- Confidentiality
- Integrity
- Availability
- Sometimes two other desirable characteristics:
  - Authentication
    - the process or action of proving or showing something to be true, genuine, or valid.
  - Nonrepudiation
    - is the assurance that someone cannot deny something.
    - i.e. **nonrepudiation** refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated

Access Control



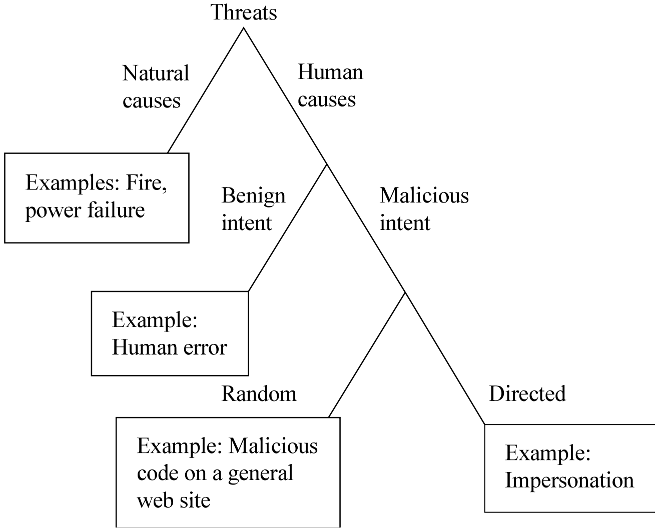
Policy:
Who + What + How = Yes/No

Subject
(who)

Mode of access
(how)

Object
(what)

Types of Threats



Threats

Natural causes

Human causes

Examples: Fire, power failure

Benign intent

Malicious intent

Example: Human error

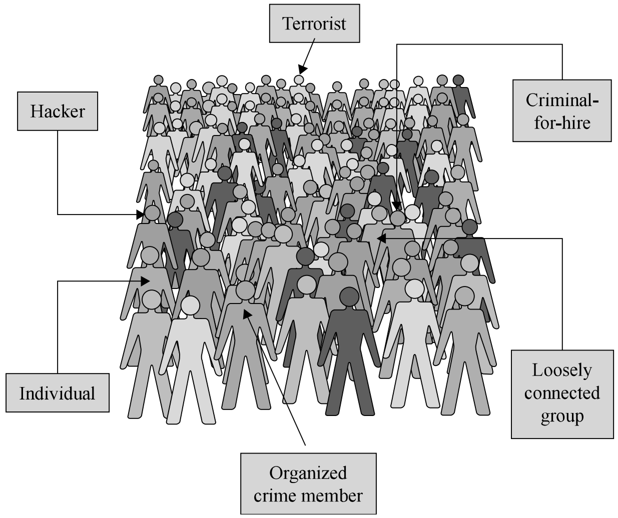
Random

Directed

Example: Malicious code on a general web site

Example: Impersonation

Types of Attackers



Terrorist

Hacker

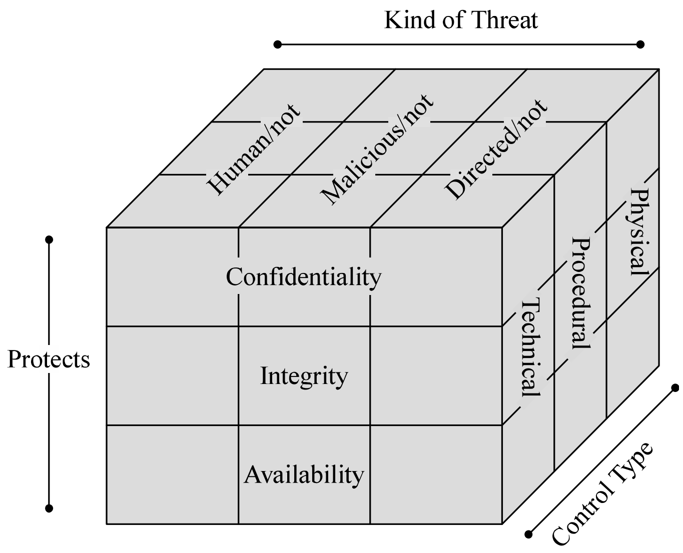
Criminal-for-hire

Individual

Loosely connected group

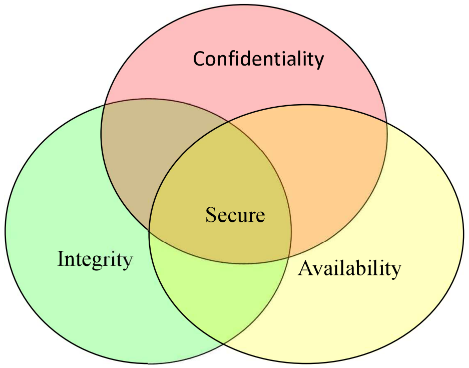
Organized crime member

Controls/Countermeasures



Relationship between Confidentiality Integrity and Availability

- In fact, these three characteristics can be independent, can overlap, and can even be mutually exclusive.



Security Goals

- When we talk about computer security, we mean that we are addressing three important aspects of any computer-related system: **confidentiality**, **integrity,** & **availability (CIA)**
  - **Confidentiality** ensures that computer-related assets are accessed only by authorized parties.
    - **i.e**. reading, viewing, printing, or even knowing their existence
    - Secrecy or privacy
  - **Integrity** means that assets can be modified only by authorized parties or only in authorized ways.
    - **i.e**. writing, changing, deleting, creating
  - **Availability** means that assets are accessible to authorized parties at appropriate times.
    - i.e. often, availability is known by its opposite, denial of service.

Goals of Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers’ violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

Computer Security Challenges

1. not simple
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms
6. battle of wits between attacker / admin
7. not perceived on benefit until fails
8. requires regular monitoring
9. too often an after-thought
10. regarded as impediment to using system

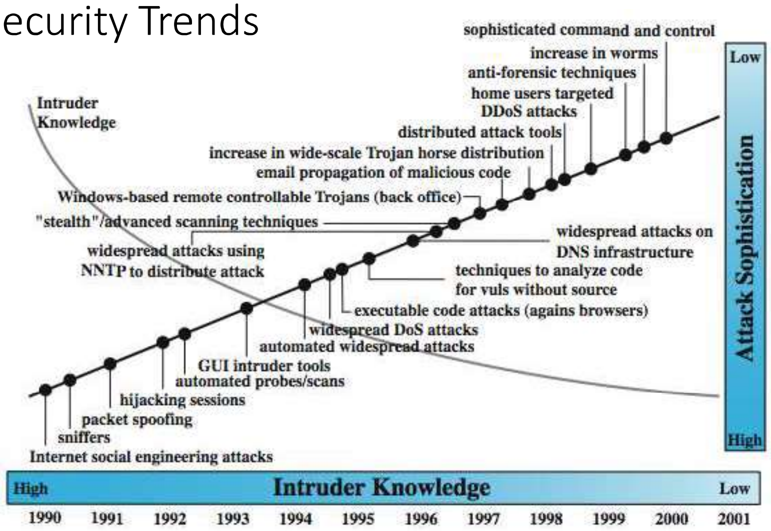
Security functional requirements (FIPS 200)

- Technical measures
  - Access control; identification & authentication; system & communication protection; system & information integrity
- Management controls and procedures
  - Awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition
- Overlapping technical and management
  - Configuration management; incident response; media protection

Examples of Security Requirements

- confidentiality – student grades
- integrity – patient information
- availability – authentication service

Security Trends



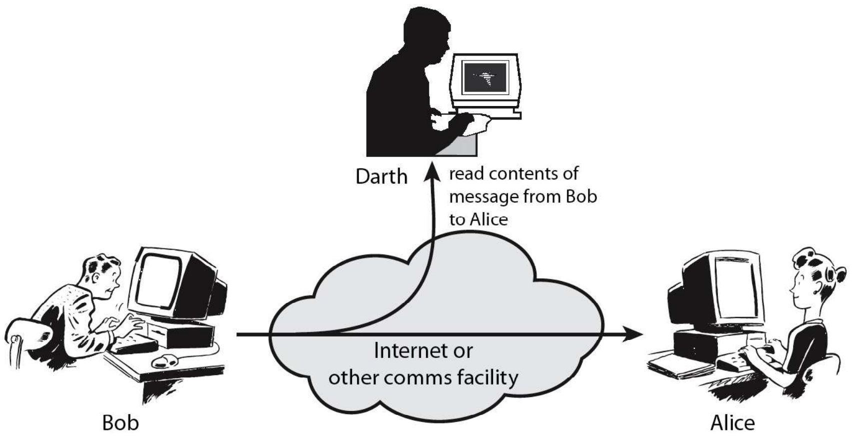
OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

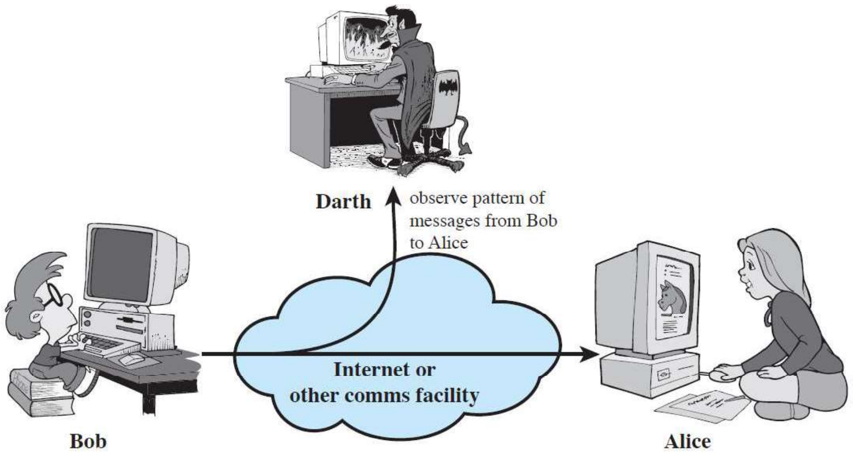
Aspects of Security

- 3 aspects of information security:
  - **security attack**
  - **security mechanism: detect, prevent, recover**
  - **security service**
- terms
  - *threat* – a potential for violation of security
  - *attack* – an assault on system security, a deliberate attempt to evade security services

Passive Attacks (1)
Release of Message Contents

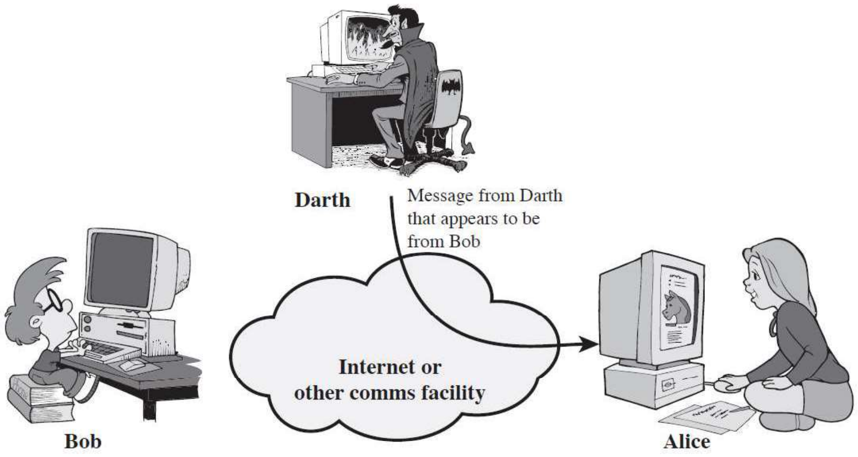

Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Passive Attacks (2)
Traffic Analysis

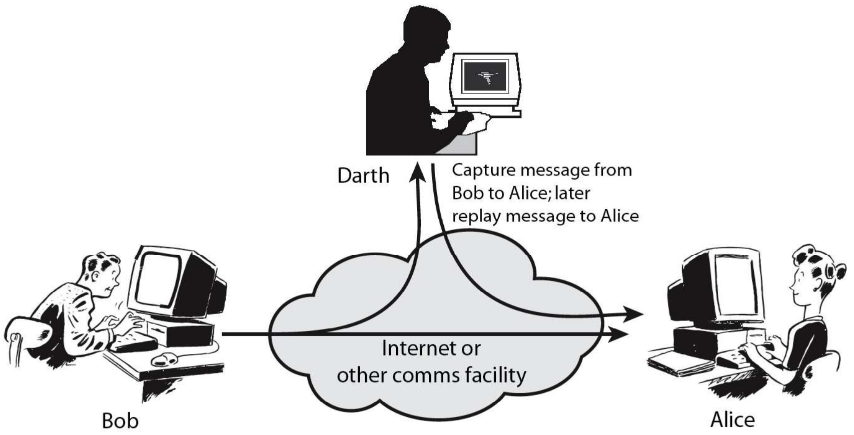

Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

- Passive attacks do not affect system resources
  - Eavesdropping, monitoring
- Two types of passive attacks
  - Release of message contents
  - Traffic analysis
- Passive attacks are very difficult to detect
  - Message transmission apparently normal
    - No alteration of the data
  - Emphasis on prevention rather than detection
    - By means of encryption

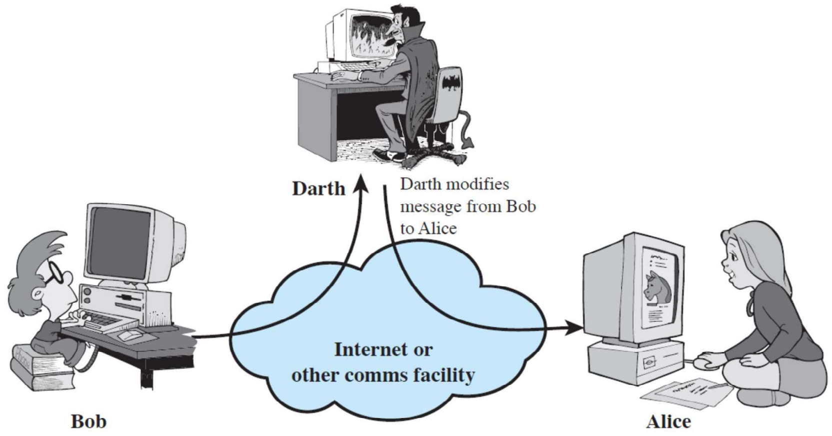
Active Attacks (1)
Masquerade


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

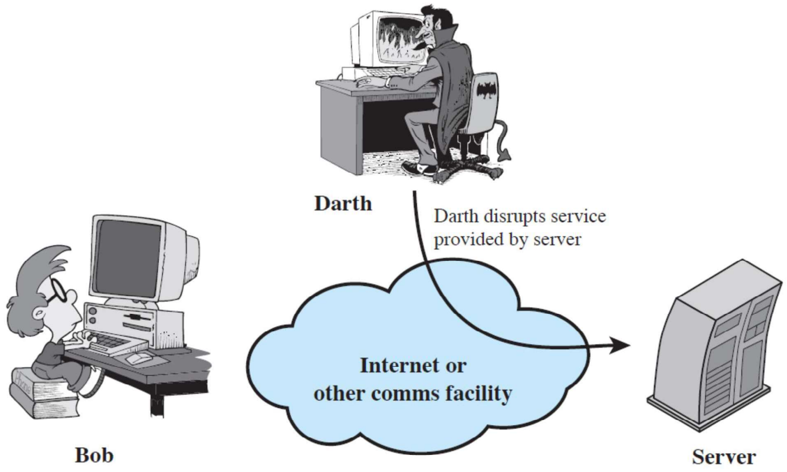
Active Attacks (2)
Replay


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Active Attacks (3)
Modification of Messages


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Active Attacks (4)
Denial of Service


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

- Active attacks try to alter system resources or affect their operation
  - Modification of data, or creation of false data
- Four categories
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of service: preventing normal use
    - A specific target or entire network
- Difficult to prevent
  - The goal is to detect and recover

Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services

- X.800:

  "a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"

- RFC 2828:

  "a processing or communication service provided by a system to give a specific kind of protection to system resources"

Security Services (X.800)

- **Authentication** - assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication
- **Access Control** - prevention of the unauthorized use of a 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

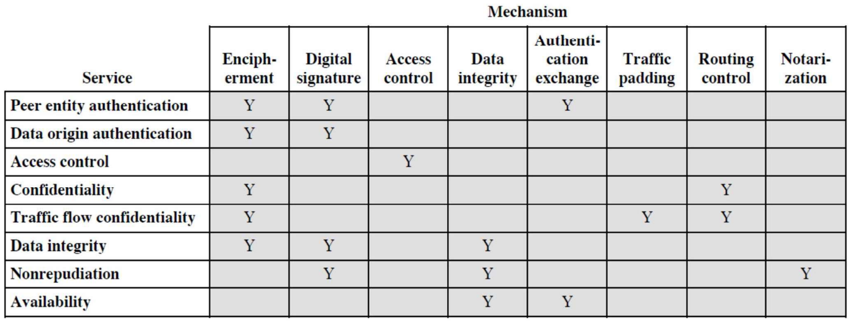
Security Mechanisms (X.800)

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- hence our focus on this topic

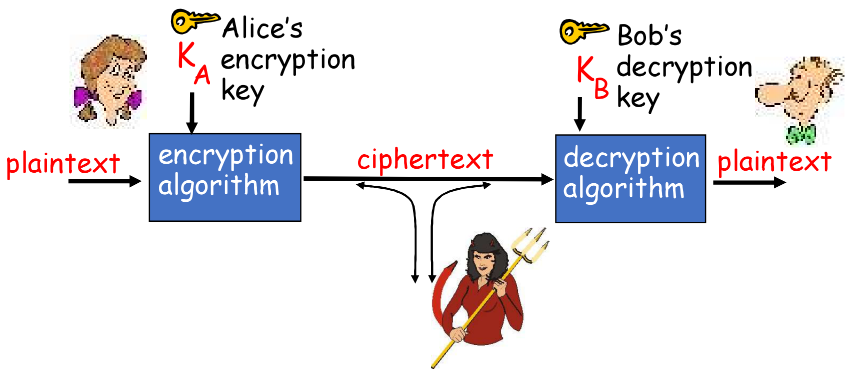
Table 1.4 Relationship Between Security Services and Mechanisms



	Mechanism							
Service	**Enciph-erment**	**Digital signature**	**Access control**	**Data integrity**	**Authenti-cation exchange**	**Traffic padding**	**Routing control**	**Notari-zation**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Introduction to Cryptography

The language of cryptography



symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret* (private)

What is Cryptography

- Cryptography
  - In a narrow sense
    - Mangling information into apparent unintelligibility
    - Allowing a secret method of un-mangling
  - In a broader sense
    - Mathematical techniques related to information security
    - About secure communication in the presence of adversaries
- Cryptanalysis
  - The study of methods for obtaining the meaning of encrypted information without accessing the secret information
- Cryptology
  - Cryptography + cryptanalysis

Security Attacks

- Passive attacks
  - Obtain message contents
  - Monitoring traffic flows
- Active attacks
  - Masquerade of one entity as some other
  - Replay previous messages
  - Modify messages in transmit
  - Add, delete messages
  - Denial of service

Objectives of Information Security

- Confidentiality (secrecy)
  - Only the sender and intended receiver should be able to understand the contents of the transmitted message
- Authentication
  - Both the sender and receiver need to confirm the identity of other party involved in the communication
- Data integrity
  - The content of their communication is not altered, either maliciously or by accident, in transmission.
- Availability
  - Timely accessibility of data to authorized entities.

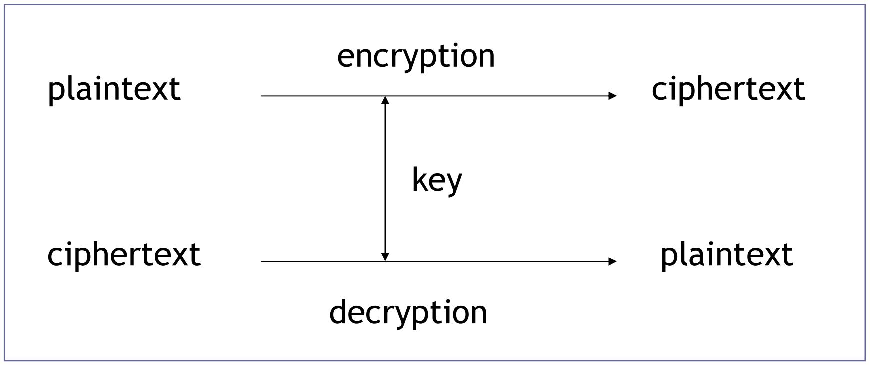
Objectives of Information Security

- Non-repudiation
  - An entity is prevented from denying its previous commitments or actions
- Access control
  - An entity cannot access any entity that it is not authorized to.
- Anonymity
  - The identity of an entity if protected from others.

Types of Cryptographic Functions

- Secret key functions
- Public key functions
- Hash functions

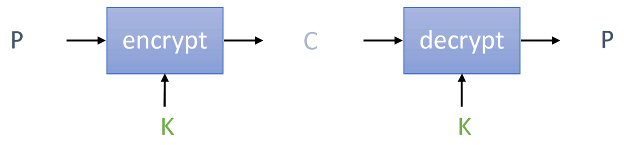
Secret Key Cryptography



- Using a single key for encryption/decryption.
- The plaintext and the ciphertext having the same size.
- Also called *symmetric* key cryptography

Symmetric Cryptosystem

- Scenario
  - Alice wants to send a message (plaintext P) to Bob.
  - The communication channel is insecure and can be eavesdropped
  - If Alice and Bob have previously agreed on a symmetric encryption scheme and a secret key K, the message can be sent encrypted (ciphertext C)
- Issues
  - What is a good symmetric encryption scheme?
  - What is the complexity of encrypting/decrypting?
  - What is the size of the ciphertext, relative to the plaintext?



Basics

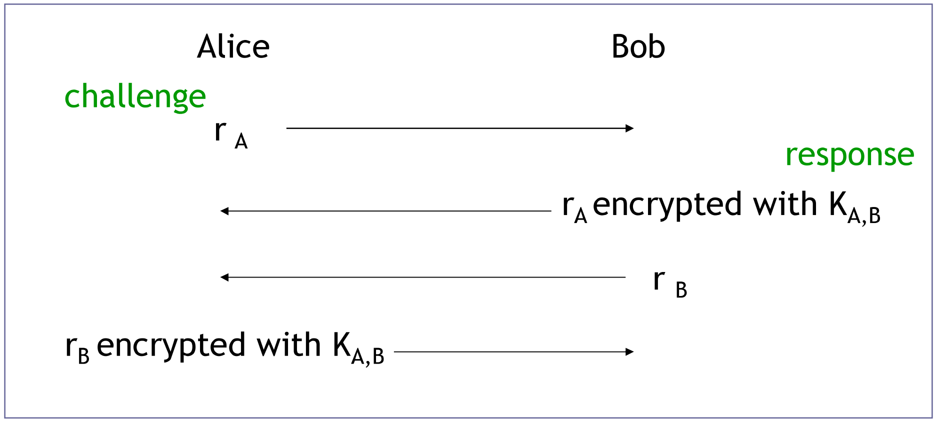
- Notation
  - Secret key K
  - Encryption function $E_K(P)$
  - Decryption function $D_K(C)$
  - Plaintext length typically the same as ciphertext length
  - Encryption and decryption are one-one mapping functions on the set of all n-bit arrays
- Efficiency
  - functions E_K and D_K should have efficient algorithms
- Consistency
  - Decrypting the ciphertext yields the plaintext
  - $D_K(E_K(P)) = P$

SKC: Security Uses

- Transmitting over an insecure channel
  - The transmitted message is encrypted by the sender and can be decrypted by the receiver, with the same key
  - Prevent attackers from eavesdropping
- Secure storage on insecure media
  - Data is encrypted before being stored somewhere
  - Only the entities knowing the key can decrypt it

SKC: Security Uses

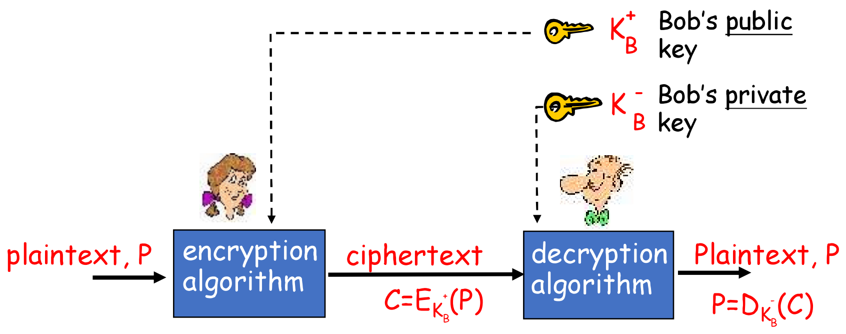
- Authentication
  - Strong authentication: proving knowledge of a secret without revealing it.


Alice
Bob
challenge
r_A
response
r_A encrypted with $K_{A,B}$
r_B
r_B encrypted with $K_{A,B}$

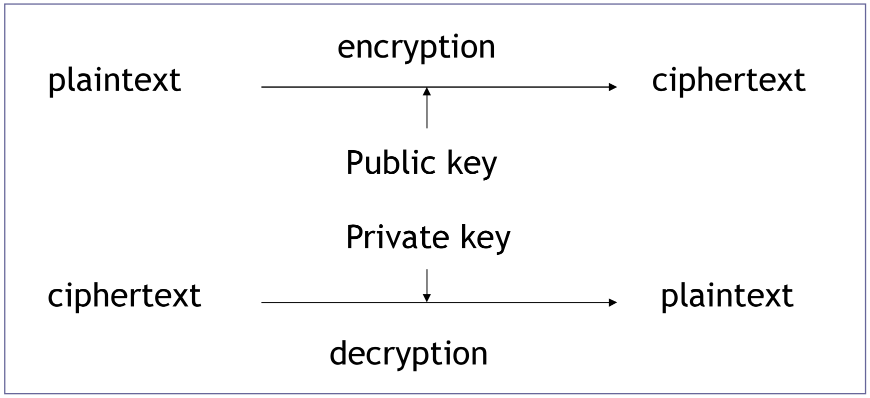
Secret Key Cryptography: Security Uses

- Integrity Check
  - Noncryptographic checksum
    - Using a well-known algorithm to map a message (of arbitrary length) to a fixed-length checksum
    - Protecting against accidental corruption of a message
    - Example: CRC
  - Cryptographic checksum
    - A well-know algorithm
    - Given a key and a message
    - The algorithm produces a fixed-length message authentication code (MAC) that is sent with the message

Public key cryptography



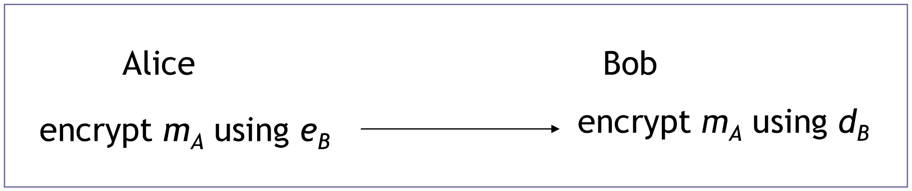
Public Key Cryptography



- Each individual has two keys
  - a private key (d): need not be reveal to anyone
  - a public key (e): preferably known to the entire world
- Public key crypto is also called asymmetric crypto.

Public Key Cryptography: Security Uses

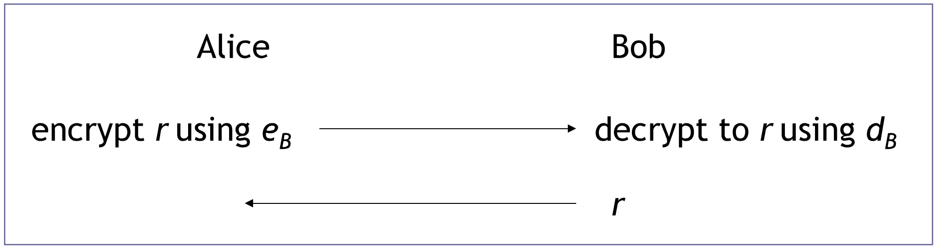
- Transmitting over an insecure channel



- Secure storage on insecure media
  - Data is encrypted with the public key of the source, before being stored somewhere
  - Nobody else can decrypt it (not knowing the private key of the data source)

Public Key Cryptography: Security Uses

- Authentication


Alice

Bob

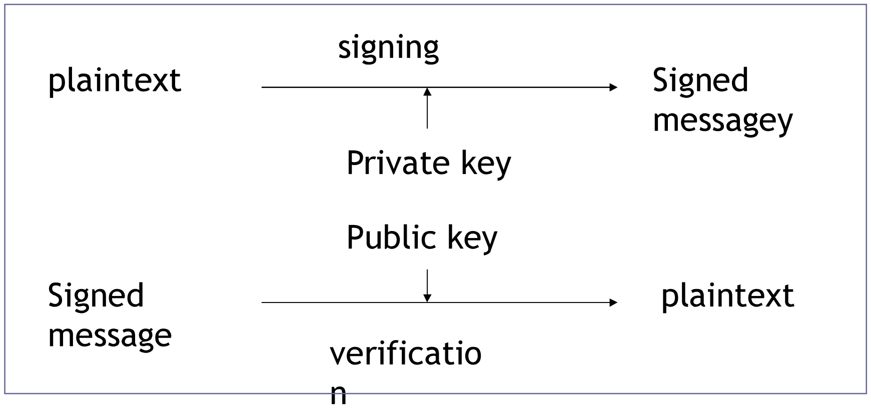
encrypt r using e_B

decrypt to r using d_B

r

Public Key Cryptography: Security Uses

- Digital Signatures
  - Proving that a message is generated by a particular individual
  - Non-repudiation: the signing individual can not be denied, because only him/her knows the private key.


plaintext

signing

Signed messagey

Private key

Public key

Signed message

plaintext

verificatio
n

Hash Functions

▶ Cryptographic hash function

▶ A mathematical transformation that takes a message of arbitrary length and computes it a fixed-length (short) number.

▶ Properties

(Let the hash of a message *m* be *h(m)*)

▶ For any *m*, it is relatively easy to compute *h(m)*

▶ Given *h(m)*, there is no way to find an m that hashes to *h(m)* in a way that is substantially easier than going through all possible values of m and computing *h(m)* for each one.

▶ It is computationally infeasible to find two values that hash to the same thing.

Hash Functions: Security Uses

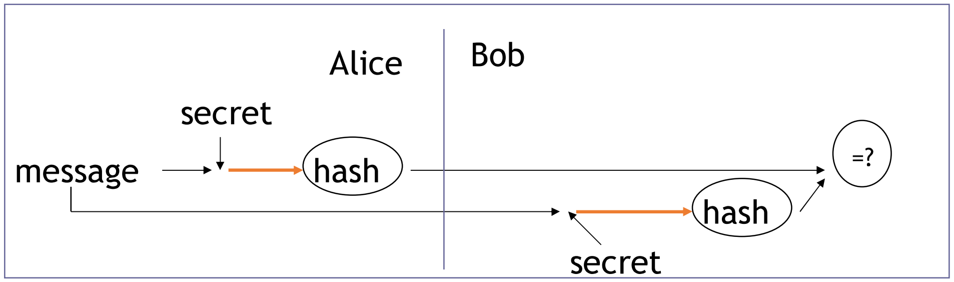
▶ Password hashing

▶ The system store a hash of the password (not the password itself)

▶ When a password is supplied, it computes the password's hash and compares it with the stored value.

▶ Message integrity

▶ Using cryptographic hash functions to generate a MAC


Alice

Bob

secret

message

hash

hash

=?

secret

Hash Functions: Security Uses

- Message fingerprint
  - Save the message digest of the data on a tamper-proof backing store
  - Periodically re-compute the digest of the data to ensure it is not changed.
- Downline load security
  - Using a hash function to ensure a download program is not modified
- Improving signature efficiency
  - Compute a message digest (using a hash function) and sign that.

Message Security Requirements

- masquerade
- content modification
- sequence modification
- timing modification
- source repudiation

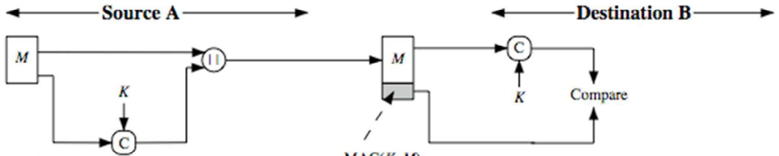
Message Authentication

Message Authentication Code (MAC)

and secret key

need not be reversible

Message Authentication Code



(a) Message authentication

Message Authentication Codes

- authentication

- separate keys

MAC Properties

Authentication

Authentication

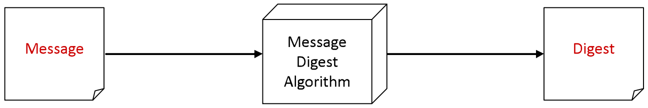
Basics

- Authentication is the process of validating the identity of a user or the integrity of a piece of data.
- There are three technologies that provide authentication
  - Message Digests / Message Authentication Codes
  - Digital Signatures
  - Public Key Infrastructure
- There are two types of user authentication:
  - Identity presented by a remote or application participating in a session
  - Sender's identity is presented along with a message.

Authentication

Message Digests

- A message digest is a fingerprint for a document
- Purpose of the message digest is to provide proof that data has not altered
- Process of generating a message digest from data is called hashing
- Hash functions are one way functions with following properties
  - Infeasible to reverse the function
  - Infeasible to construct two messages which hash to same digest
- Commonly used hash algorithms are
  - MD5 – 128 bit hashing algorithm by Ron Rivest of RSA
  - SHA & SHA-1 – 162 bit hashing algorithm developed by NIST



Message

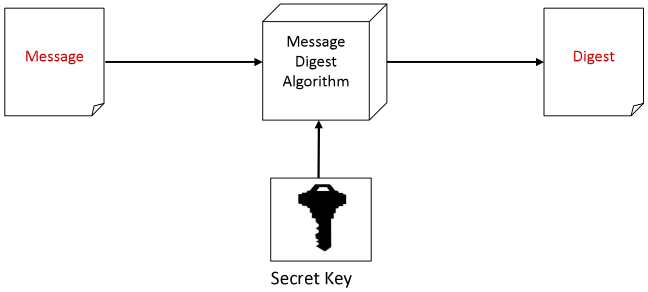
Message Digest Algorithm

Digest

Message Authentication Codes

Basics

- A message digest created with a key
- Creates security by requiring a secret key to be possesses by both parties in order to retrieve the message



Message

Message Digest Algorithm

Digest

Secret Key

Password Authentication

Basics

- Password is secret character string only known to user and server
- Message Digests commonly used for password authentication
- Stored hash of the password is a lesser risk
  - Hacker can not reverse the hash except by brute force attack
- Problems with password based authentication
  - Attacker learns password by social engineering
  - Attacker cracks password by brute-force and/or guesswork
  - Eavesdrops password if it is communicated unprotected over the network
  - Replays an encrypted password back to the authentication server

Authentication Protocols

Kerberos

- Kerberos is an authentication service that uses symmetric key encryption and a key distribution center.
- Kerberos Authentication server contains symmetric keys of all users and also contains information on which user has access privilege to which services on the network

Authentication Protocols

Basics

- Set of rules that governs the communication of data related to authentication between the server and the user
- Techniques used to build a protocol are
  - Transformed password
    - Password transformed using one way function before transmission
    - Prevents eavesdropping but not replay
  - Challenge-response
    - Server sends a random value (challenge) to the client along with the authentication request. This must be included in the response
    - Protects against replay
  - Time Stamp
    - The authentication from the client to server must have time-stamp embedded
    - Server checks if the time is reasonable
    - Protects against replay
    - Depends on synchronization of clocks on computers
  - One-time password
    - New password obtained by passing user-password through one-way function n times which keeps incrementing
    - Protects against replay as well as eavesdropping

Authentication

Personal Tokens

- Personal Tokens are hardware devices that generate unique strings that are usually used in conjunction with passwords for authentication
- Different types of tokens exist
  - Storage Token: A secret value that is stored on a token and is available after the token has been unlocked using a PIN
  - Synchronous one-time password generator: Generate a new password periodically (e.g. each minute) based on time and a secret code stored in the token
  - Challenge-response: Token computes a number based on a challenge value sent by the server
  - Digital Signature Token: Contains the digital signature private key and computes a computes a digital signature on a supplied data value
- A variety of different physical forms of tokens exist
  - e.g. hand-held devices, Smart Cards, PCMCIA cards, USB tokens

Authentication

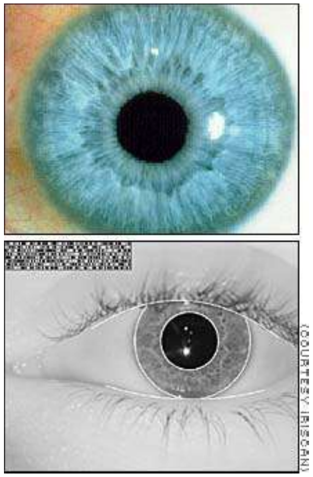
Biometrics

- Uses certain biological characteristics for authentication
  - Biometric reader measures physiological indicia and compares them to specified values
  - It is not capable of securing information over the network
- Different techniques exist
  - Fingerprint Recognition
  - Voice Recognition
  - Handwriting Recognition
  - Face Recognition
  - Retinal Scan
  - Hand Geometry Recognition

Random Numbers

Authentication

Iris Recognition



(COURTESY IRISCAN)

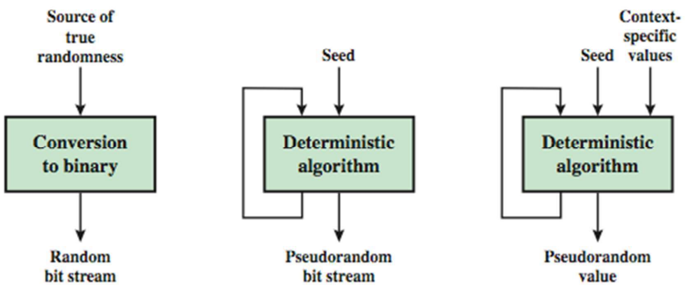
The scanning process takes advantage of the natural patterns in people's irises, digitizing them for identification purposes

Facts

- Probability of two irises producing exactly the same code: 1 in 10 to the 78th power
- Independent variables (degrees of freedom) extracted: 266
- IrisCode record size: 512 bytes
- Operating systems compatibility: DOS and Windows (NT/95)
- Average identification speed (database of 100,000 IrisCode records): one to two seconds

Pseudorandom Number Generators (PRNGs)

Random & Pseudorandom Number Generators



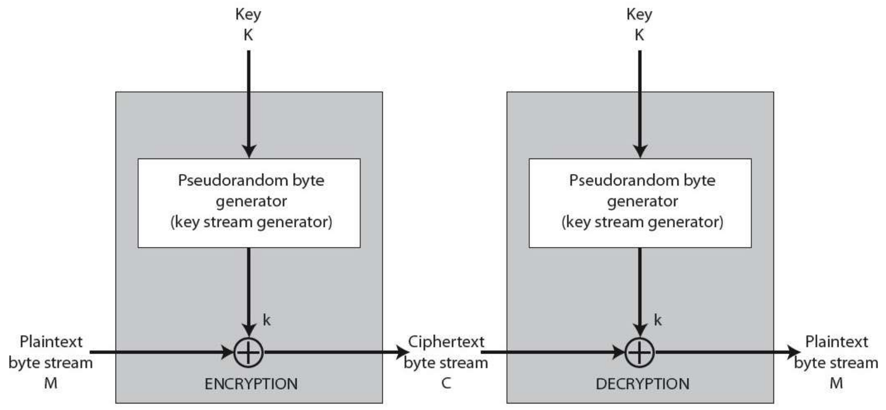
(a) TRNG (b) PRNG (c) PRF

PRNG Requirements

PRNG Requirements

Stream Ciphers

Stream Cipher Structure


Key
K
Pseudorandom byte generator (key stream generator)
k
Plaintext byte stream M
ENCRYPTION
Ciphertext byte stream C
Key
K
Pseudorandom byte generator (key stream generator)
k
DECRYPTION
Plaintext byte stream M

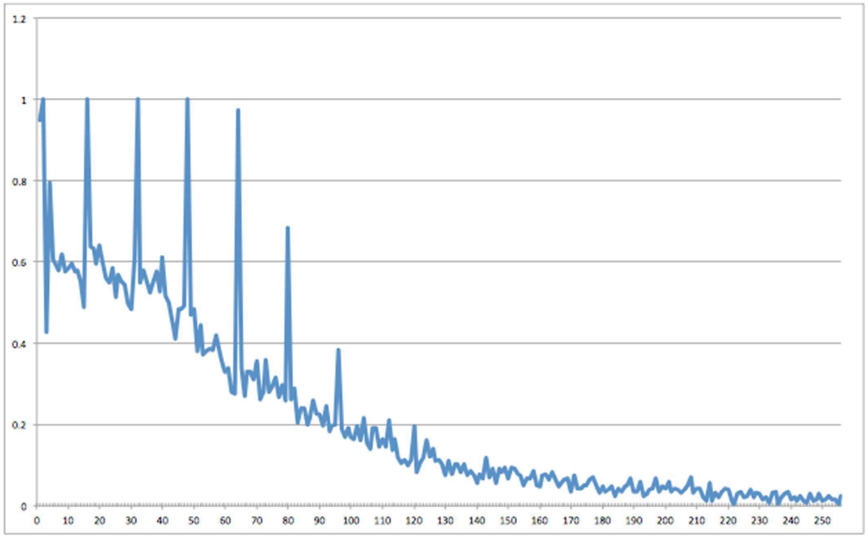
RC4

Stream Cipher Properties

RC4 Key Schedule

RC4 Encryption

RC4 Security



RC4 Security

Natural Random Noise

Encrypting stored data

Personal data should be stored in an encrypted form to protect against unauthorized access or processing, especially if the loss of the personal data is reasonably likely to occur and would cause damage or distress to individuals.

Simple file encryption

- User enters passphrase
- Passphrase hashed with a cryptographic hash function to produce a key
- File encrypted with the key
- E.g. AES in CBC mode
- Decryption with the same key

Limitations of file encryption

- Encrypting a file normally creates an encrypted copy; what happens to the old plaintext file?
- No guarantee that the plaintext is not left on the disk
- Word processors and other software create temporary files and backup copies
- Unencrypted versions and fragments of the file may be left in locations that the user does not even know about
- There are tools for deleting temporary files and for wiping free disk space, but none is completely reliable
- Cloud storage keep all old data

Windows encrypting file system (EFS)

- Encryption is a file attribute
- Possible to enable encryption for all files in a folder new files encrypted
- Files are readable only when the user is logged in
- Encryption and decryption are transparent to applications
- Similar products exist for Unix

Full disk encryption

- Protects all information on disk
- Easier to use correctly than EFS
- Products are available from various hardware and software vendors including hard disk manufacturers
- Password, key or physical token required to boot or to mount disk; thereafter transparent
- Usability and reliability issues?
- Requires user/admin to be present at boot time
- In software-based products:
- Password must be strong enough to resist brute-force guessing
- Hibernation is a problem
- Hardware solution would be better

Windows BitLocker Full-volume encryption in Windows

- Uses TPM for key management
- Optional PIN input and/or USB dongle at boot time
- System volume must be NTFS, data disks can also be FAT
- Sealing the entire system partition:
- Encrypt data with a symmetric key
- Seal the key; store sealed key on disk; unseal when booting
- TPM checks the OS integrity before unsealing the key
- Can boot to another OS but then cannot unseal the Windows partition cannot bypass OS access controls
- For a stolen laptop, forces the thief to hardware attack against TPM

Trusted platform module

- Trusted hardware enables some things that otherwise would be impossible
- Trusted platform module (TPM) is a smart-card-like module on the computer motherboard
- Holds crypto keys and platform measurements in platform configuration registers (PCR)
- Useful TPM operations:
- TMP_Seal: encrypt data — in any platform configuration
- TPM_Unseal: decrypt the data, but only if the platform configuration is the same as when sealing

Principals of Cryptography

Week 3

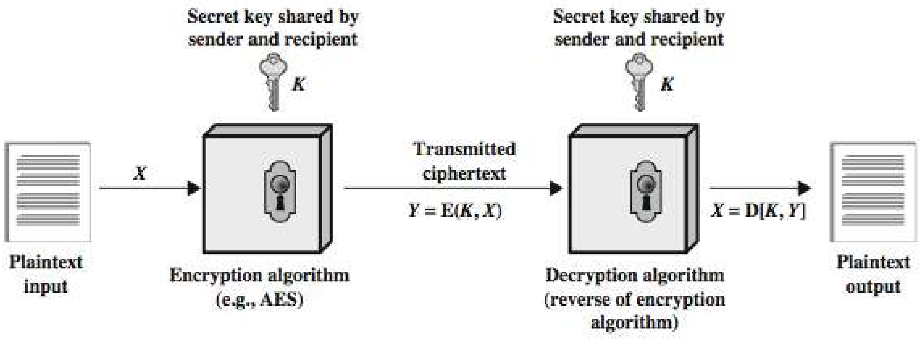
Some Basic Terminology

- **plaintext** - original message
- **ciphertext** - coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - field of both cryptography and cryptanalysis

Symmetric Encryption

- or conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- was only type prior to invention of public-key in 1970's
- and by far most widely used

Symmetric Cipher Model



Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Requirements

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically have:

  $Y = \mathrm{E}(\mathrm{K}, X)$

  $X = \mathrm{D}(\mathrm{K}, Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Cryptanalysis

- objective to recover key not just message
- general approaches:
  - cryptanalytic attack
  - brute-force attack
- if either succeed all key use compromised

Cryptography

- can characterize cryptographic system by:
  - type of encryption operations used
    - substitution
    - transposition
    - product
  - number of keys used
    - single-key or private
    - two-key or public
  - way in which plaintext is processed
    - block
    - stream

Cryptanalytic Attacks

- **ciphertext only**
  - only know algorithm & ciphertext, is statistical, know or can identify plaintext
- **known plaintext**
  - know/suspect plaintext & ciphertext
- **chosen plaintext**
  - select plaintext and obtain ciphertext
- **chosen ciphertext**
  - select ciphertext and obtain plaintext
- **chosen text**
  - select plaintext or ciphertext to en/decrypt

Classical Substitution Ciphers

- where letters of plaintext are replaced by other letters or by numbers or symbols
- or if plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Caesar Cipher

- can define transformation as:

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
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

- mathematically give each letter a number

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- then have Caesar cipher as:

$c = \mathrm{E}(\mathrm{k}, p) = (p + k) \bmod (26)$

$p = \mathrm{D}(\mathrm{k}, \mathrm{c}) = (\mathrm{c} – k) \bmod (26)$

Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter on
- example:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

Use in Cryptanalysis

- key concept - monoalphabetic substitution ciphers do not change relative letter frequencies
- discovered by Arabian scientists in 9th century
- calculate letter frequencies for ciphertext
- compare counts/plots against known values
- if caesar cipher look for common peaks/troughs
  - peaks at: A-E-I triple, NO pair, RST triple
  - troughs at: JK, X-Z
- for monoalphabetic must identify each letter
  - tables of common double/triple letters help

Example Cryptanalysis

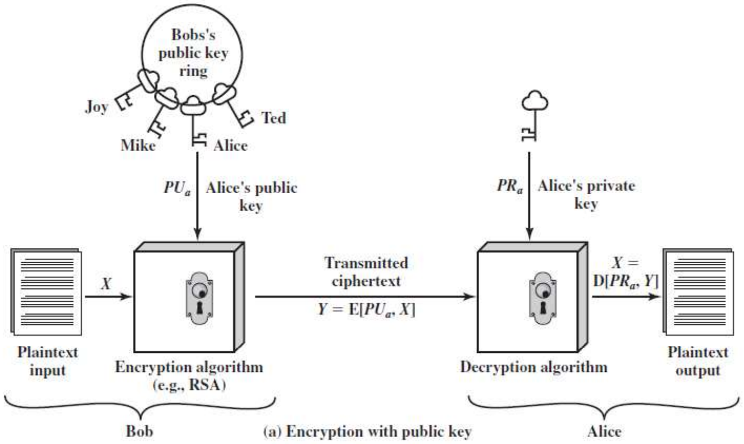
- given ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

- count relative letter frequencies (see text)
- guess P & Z are e and t
- guess ZW is th and hence ZWP is the
- proceeding with trial and error finally get:

```
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow
```

Asymmetric Key Encryption



(a) Encryption with public key

Summary

- have considered:
  - classical cipher techniques and terminology
  - monoalphabetic substitution ciphers
  - cryptanalysis using letter frequencies
  - product ciphers and rotor machines
  - stenography

- The essential steps are the following:
  1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
  2. Each user places one of the two keys in a public register or other accessible file.This is the public key.The companion key is kept private.As the previous figure suggests, each user maintains a collection of public keys obtained from others.
  3. If Bob wishes to send a private message to Alice, Bob encrypts the message using Alice’s public key.
  4. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice’s private key.

- The two keys used for public-key encryption are referred to as the **public key** and the **private key**.
- Invariably, the **private key is kept secret**, but it is referred to as a private key rather than a secret key to avoid confusion with conventional encryption.

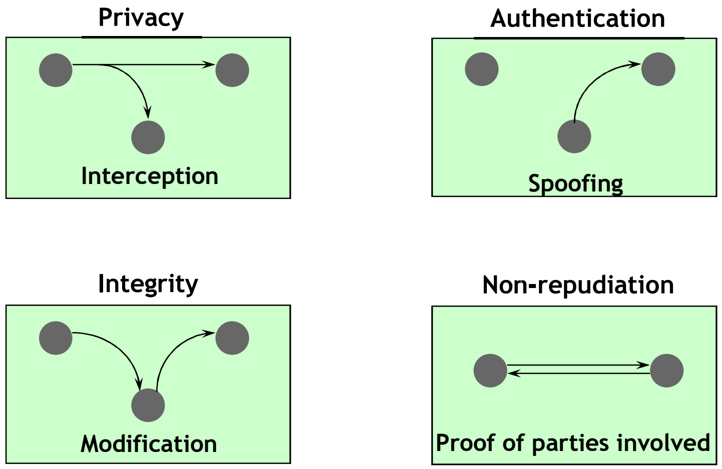
References

- William Stallings, Chapter 2, Fifth Edition,Cryptography and Network Security

  ,

Public Key Infrastructure and Digital Signatures

Multiple Security Issues



Privacy

Interception

Authentication

Spoofing

Integrity

Modification

Non-repudiation

Proof of parties involved

What’s the problem?

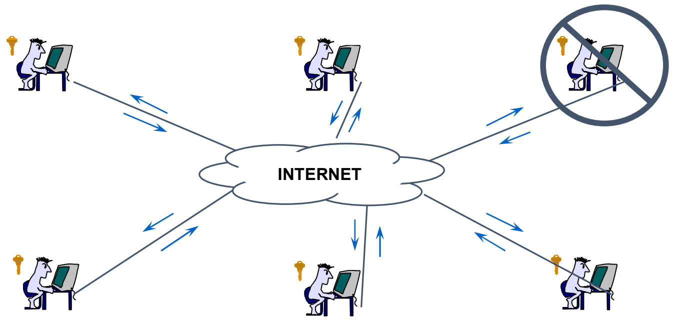
- Information over the Internet is Free, Available, Unencrypted, and Untrusted.
- Not desirable for many Applications
  - Electronic Commerce
  - Software Products
  - Financial Services
  - Corporate Data
  - Healthcare
  - Subscriptions
  - Legal Information

Security Algorithms

- Symmetric Algorithms
  - Triple-DES, DES, CAST, RC2, IDEA
- Public Key Algorithms
  - RSA, DSA, Diffie-Hellman, Elliptic Curve
- Hashing Algorithms
  - SHA-1, MD5, RIPEMD

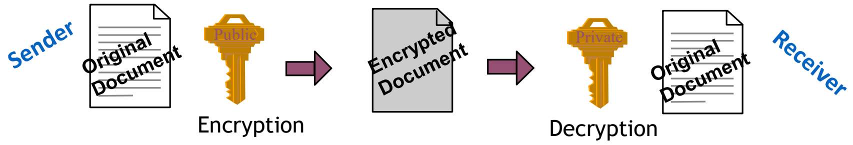
Symmetric Key Encryption

- If any one's key is compromised, all keys need to be replaced
- Not practical or cost effective for Internet environments



Public Key Cryptography

- Public-Key Cryptography is an encryption scheme that uses **mathematically** related, but **not identical** keys.
- Each user has a key pair (public key/private key).

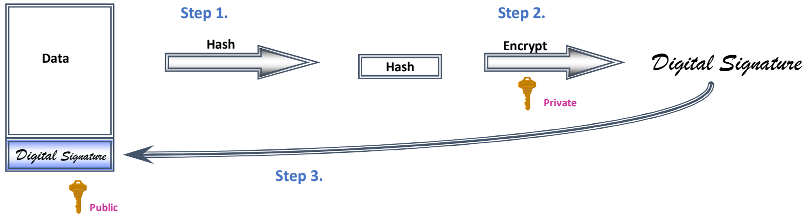


- Information encrypted with the public key can only be decrypted using the private key.

What is a Digital Signature ?

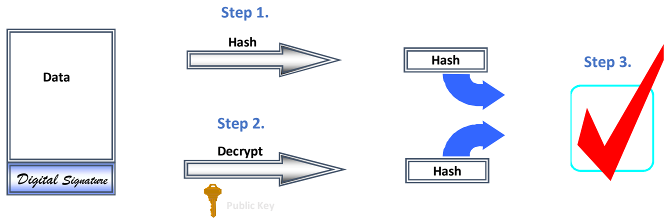
- A Digital Signature is the result of **encrypting** the Hash of the data to be exchanged.
- A Hash (or Message Digest) is the process of mathematically reducing a data stream down to a fixed length field.
- The Hash uniquely represents the original data.
- The probability of producing the same Hash with two sets of different data is <.001%.
- Signature Process is opposite to Encryption Process
  - Private Key is used to Sign (encrypt) Data
  - Public Key is used to verify (decrypt) Signature

Digital Signature Process



- Step 1. Hash (digest) the data using one of the supported Hashing algorithms, e.g., MD2, MD5, or SHA-1.
- Step 2. Encrypt the hashed data using the sender's private key.
- Step 3. Append the signature (and a copy of the sender's public key) to the end of the data that was signed.

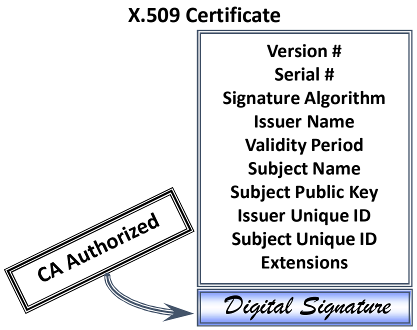
Signature Verification Process



- Step 1. Hash the original data using the same hashing algorithm.
- Step 2. Decrypt the digital signature using the sender’s public key. All digital signatures contain a copy of the signer’s public key.
- Step 3. Compare the results of the hashing and the decryption. If the values match then the signature is verified. If the values do not match, then the data or signature was probably modified in transit.

Digital Certificates

- A Digital Certificate is simply an X.509 defined data structure with a Digital Signature. The data represents who owns the certificate, who signed the certificate, and other relevant information



X.509 Certificate

Version #
Serial #
Signature Algorithm
Issuer Name
Validity Period
Subject Name
Subject Public Key
Issuer Unique ID
Subject Unique ID
Extensions

Digital Signature

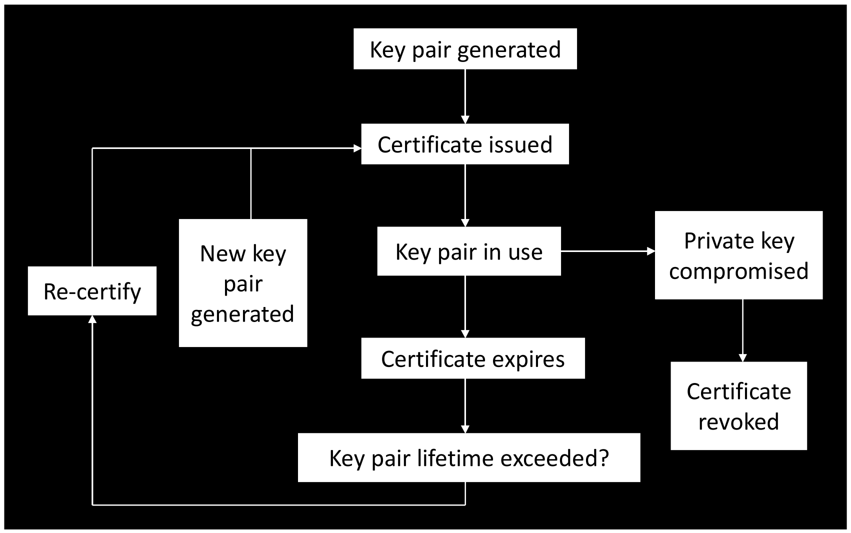
CA Authorized

- When the signature is generated by a Certification Authority (CA), the signature can be viewed as trusted.
- Since the data is signed, it can not be altered without detection.
- Extensions can be used to tailor certificates to meet the needs of end applications.

Digital Certificates

- Before two parties exchange data using Public Key cryptography, each wants to be sure that the other party is authenticated
- Before B accepts a message with A’s Digital Signature, B wants to be sure that the public key belongs to A and not to someone masquerading as A on an open network
- One way to be sure, is to use a trusted third party to authenticate that the public key belongs to A. Such a party is known as a **Certification Authority (CA)**
- Once A has provided proof of identity, the Certification Authority creates a message containing A’s name and public key. This message is known as a **Digital Certificate**.

Certificate Life Cycle



Key pair generated

Certificate issued

New key pair generated

Re-certify

Key pair in use

Private key compromised

Certificate expires

Certificate revoked

Key pair lifetime exceeded?

Certificate Revocation Lists

- CA periodically publishes a data structure called a certificate revocation list (CRL).
- Described in X.509 standard.
- Each revoked certificate is identified in a CRL by its serial number.
- CRL might be distributed by posting at known Web URL or from CA's own X.500 directory entry.

Certification Authority (CA)

Certification Authority

- Trusted (Third) Party
- Enrolls and Validates Subscribers
- Issues and Manages Certificates
- Manages Revocation and Renewal of Certificates
- Establishes Policies & Procedures

What's Important

- Operational Experience
- High Assurance Security Architecture
- Scalability
- Flexibility
- Interoperability
- Trustworthiness

Certification Authority = Basis of Trust

PKI Players

- Registration Authority (RA) to identity proof users
- Certification Authorities (CA) to issue certificates and CRL's
- Repositories (publicly available databases) to hold certificates and CRLs

Registration Authority (RA)

- Enrolling, de-enrolling, and approving or rejecting requested changes to the certificate attributes of subscribers.
- Validating certificate applications.
- Authorizing requests for key-pair or certificate generation and requests for the recovery of backed-up keys.
- Accepting and authorizing requests for certificate revocation or suspension.
- Physically distributing personal tokens to and recovering obsolete tokens from people authorized to hold and use them.

Certificate Policy (CP) is ...

- the basis for trust between unrelated entities
- not a formal “contract” (but implied)
- a framework that both informs and constrains a PKI implementation
- a statement of what a certificate means
- a set of rules for certificate holders
- a way of giving advice to Relying Parties

Authentication/Access Control

- Can Public Key Technology be used to perform Authentication and Access Control?

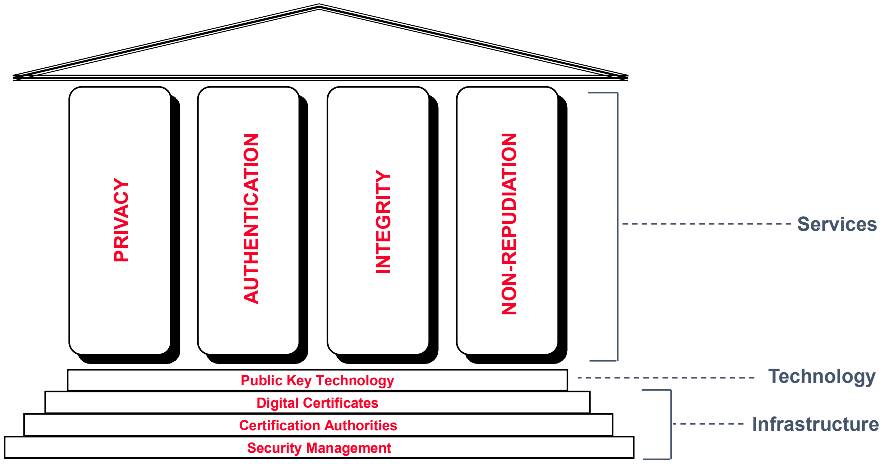
Sure Can

How?

Using Digital Signatures

and Digital Certificates

Public Key Security



PRIVACY

AUTHENTICATION

INTEGRITY

NON-REPUDIATION

Services

Public Key Technology

Digital Certificates

Certification Authorities

Security Management

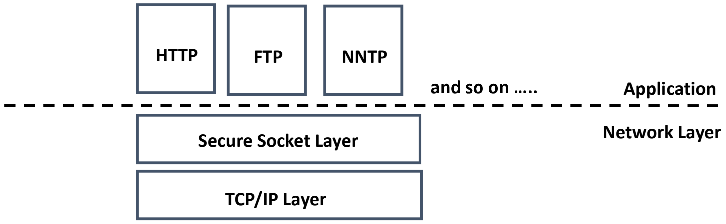
Technology

Infrastructure

- Public Key Technology Best Suited to Solve Business Needs
- Infrastructure = Certification Authorities

SSL Protocol

- Secure Socket Layer (SSL) is a Network Layer protocol used to secure data on TCP/IP networks.



HTTP

FTP

NNTP

and so on .....

Application

Network Layer

Secure Socket Layer

TCP/IP Layer

SSL / TLS

- SSLv3.1 = TLS v1.0; NB: WTLS -- TLS for Wireless Links
- Works over TCP; Application Independent.

SSL/TLS allows client/server apps to communicate via a protected channel.

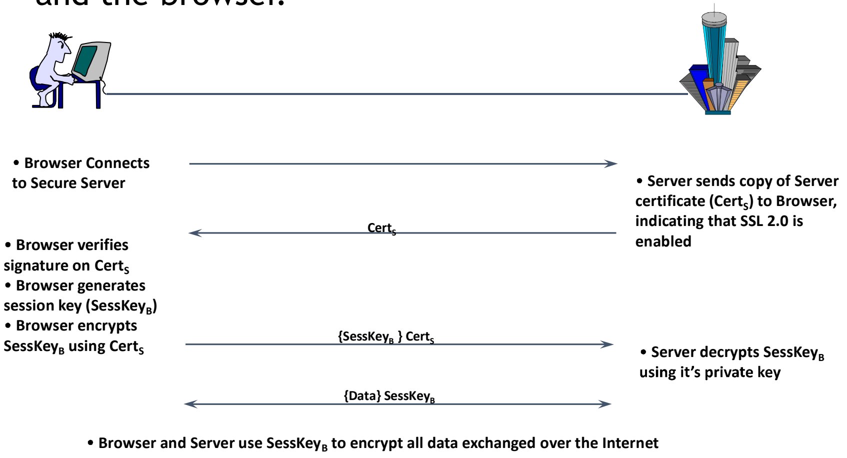
- Common example -- HTTP over SSL/TLS, e.g.

https://www.entrust.com

M.Thompson, O.Kolesnikov, Berkeley National Laboratory

SSL 2.0 Protocol

- SSL 2.0 provides encryption between the server and the browser.



• Browser Connects to Secure Server

• Server sends copy of Server certificate (Cert$_S$) to Browser, indicating that SSL 2.0 is enabled

Cert$_S$

• Browser verifies signature on Cert$_S$
• Browser generates session key (SessKey$_B$)
• Browser encrypts SessKey$_B$ using Cert$_S$

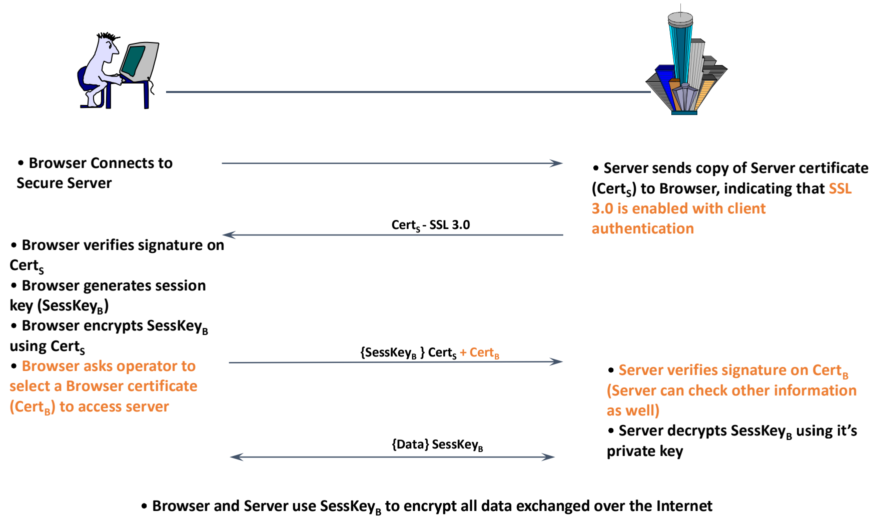
{SessKey$_B$ } Cert$_S$

• Server decrypts SessKey$_B$ using it's private key

{Data} SessKey$_B$

• Browser and Server use SessKey$_B$ to encrypt all data exchanged over the Internet

SSL 3.0 with Client Authentication



• Browser Connects to Secure Server

• Server sends copy of Server certificate (Cert$_S$) to Browser, indicating that SSL 3.0 is enabled with client authentication

Cert$_S$ - SSL 3.0

• Browser verifies signature on Cert$_S$
• Browser generates session key (SessKey$_B$)
• Browser encrypts SessKey$_B$ using Cert$_S$
• Browser asks operator to select a Browser certificate (Cert$_B$) to access server

{SessKey$_B$ } Cert$_S$ + Cert$_B$

• Server verifies signature on Cert$_B$ (Server can check other information as well)
• Server decrypts SessKey$_B$ using it's private key

{Data} SessKey$_B$

• Browser and Server use SessKey$_B$ to encrypt all data exchanged over the Internet

Smart Cards

- Microprocessor with memory that can generate and store keys and certificates
- Different form factors and interface mechanisms
- Cryptographic functions using private key are processed on the card itself

Smart Cards and PKI

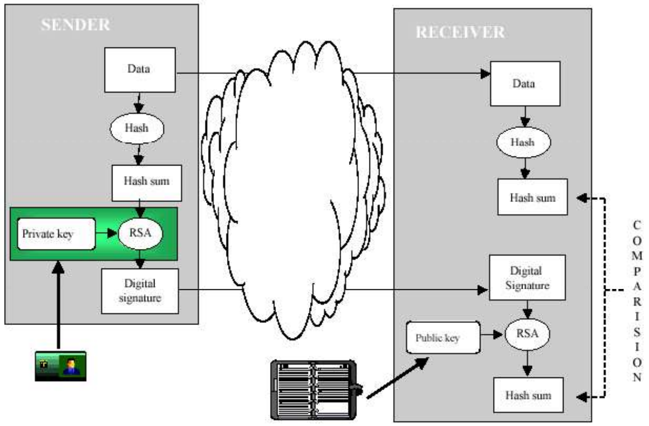
- Smart cards are «certificate wallets»

- Secure storage for:
  - Owner private key

- Smart Cards are a «PC-in-your-Pocket»
  - Generation of owner's digital signature

- Smart cards provide:
  - Mobility
  - Security
  - Transparency

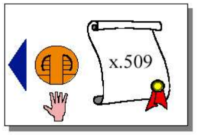
Smart card application example: Digital Signature



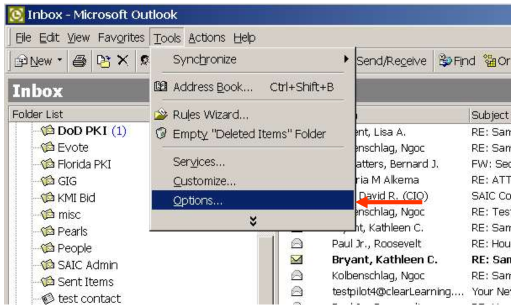
Digital ID

- Asymmetric key-pair
  - public key
  - private key

- X.509 certificate
  - ISO standard
  - public key
  - credentials

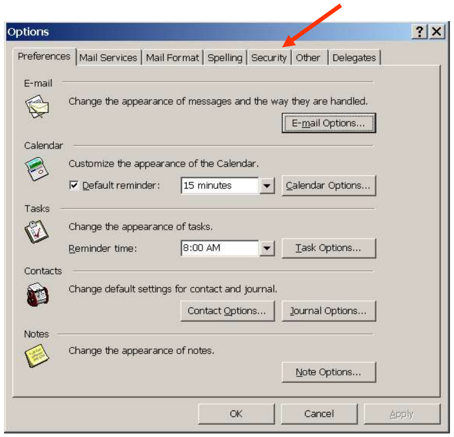


Using PKI Certificates in Outlook (1)



1 Open **Outlook**. Select **Tools** from the main menu then choose **Options** from the drop-down menu.

Using PKI Certificates in Outlook (2)



Options
Preferences | Mail Services | Mail Format | Spelling | Security | Other | Delegates

E-mail

Change the appearance of messages and the way they are handled. [E-mail Options...]

Calendar

Customize the appearance of the Calendar.

☑ Default reminder: 15 minutes [Calendar Options...]

Tasks

Change the appearance of tasks.

Reminder time: 8:00 AM [Task Options...]

Contacts

Change default settings for contact and journal. [Contact Options...] [Journal Options...]

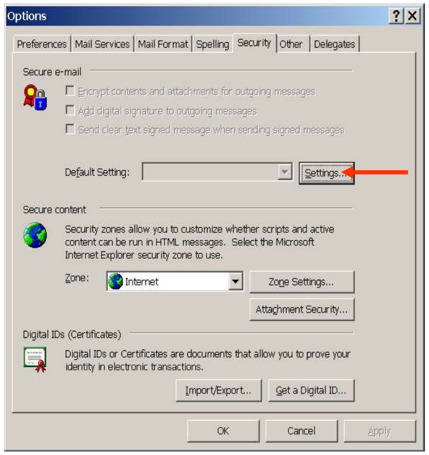
Notes

Change the appearance of notes. [Note Options...]

2

Click on the **Security** tab.

Using PKI Certificates in Outlook (3)



Options
Preferences | Mail Services | Mail Format | Spelling | Security | Other | Delegates

Secure e-mail

☐ Encrypt contents and attachments for outgoing messages

☐ Add digital signature to outgoing messages

☐ Send clear text signed message when sending signed messages

Default Setting: [Settings...]

Secure content

Security zones allow you to customize whether scripts and active content can be run in HTML messages. Select the Microsoft Internet Explorer security zone to use.

Zone: Internet [Zone Settings...] [Attachment Security...]

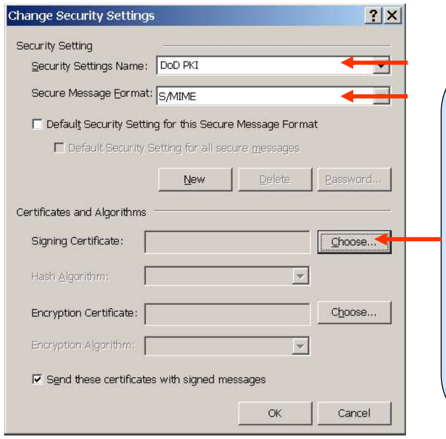
Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions. [Import/Export...] [Get a Digital ID...]

3

Click the **Settings** button.

Using PKI Certificates in Outlook (4)



Security Setting

Security Settings Name: DoD PKI

Secure Message Format: S/MIME

☐ Default Security Setting for this Secure Message Format

☐ Default Security Setting for all secure messages

Certificates and Algorithms

Signing Certificate: [Choose...]

Hash Algorithm:

Encryption Certificate: [Choose...]

Encryption Algorithm:

☑ Send these certificates with signed messages

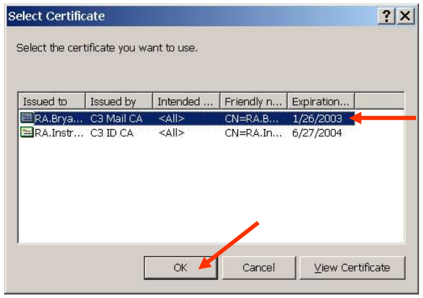
4

In the **Security Settings Name** field, enter a name for the new Security Setting .

Type **S/MIME** in the **Secure Message Format** field.

Click the **Choose** button next to the Signing Certificate field.

Using PKI Certificates in Outlook (5)



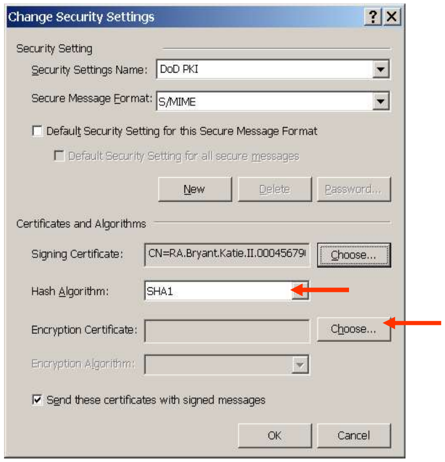
Select the certificate you want to use.

Issued to	Issued by	Intended ...	Friendly n...	Expiration...
RA.Brya...	C3 Mail CA	<All>	CN=RA.B...	1/26/2003
RA.Instr...	C3 ID CA	<All>	CN=RA.In...	6/27/2004

5

Click on the certificate issued by **C3 Mail CA**. This is your Email Signing certificate. Click **OK**.

Using PKI Certificates in Outlook (6)



Security Setting

Security Settings Name: DoD PKI

Secure Message Format: S/MIME

☐ Default Security Setting for this Secure Message Format

☐ Default Security Setting for all secure messages

Certificates and Algorithms

Signing Certificate: CN=RA.Bryant.Katie.II.00045679

Hash Algorithm: SHA1

Encryption Certificate:

Encryption Algorithm:

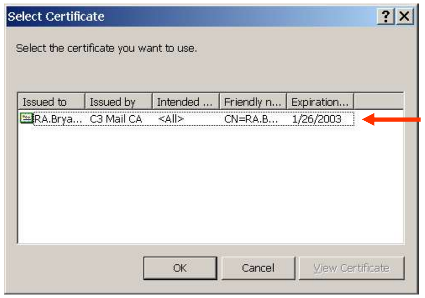
☑ Send these certificates with signed messages

6

Choose **SHA1** from the **Hash Algorithm** drop down menu.

Click on the **Choose** button next to the **Encryption Certificate** field.

Using PKI Certificates in Outlook (7)



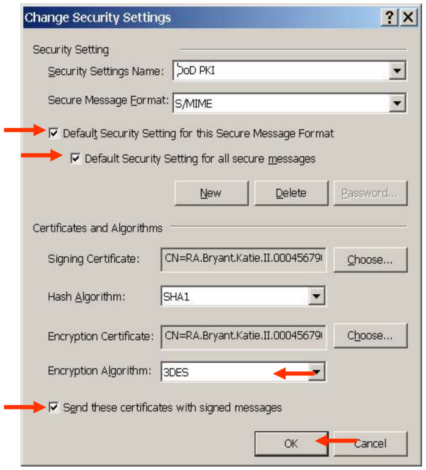
Select the certificate you want to use.

Issued to	Issued by	Intended ...	Friendly n...	Expiration...
RA.Brya...	C3 Mail CA	<All>	CN=RA.B...	1/26/2003

7

Click on the certificate issued by **C3 Mail CA**. This is your Email Encryption certificate. Click **OK**.

Using PKI Certificates in Outlook (8)



Security Setting

Security Settings Name: DoD PKI

Secure Message Format: S/MIME

☑ Default Security Setting for this Secure Message Format

☑ Default Security Setting for all secure messages

Certificates and Algorithms

Signing Certificate: CN=RA.Bryant.Katie.II.00045679

Hash Algorithm: SHA1

Encryption Certificate: CN=RA.Bryant.Katie.II.00045679

Encryption Algorithm: 3DES

☑ Send these certificates with signed messages

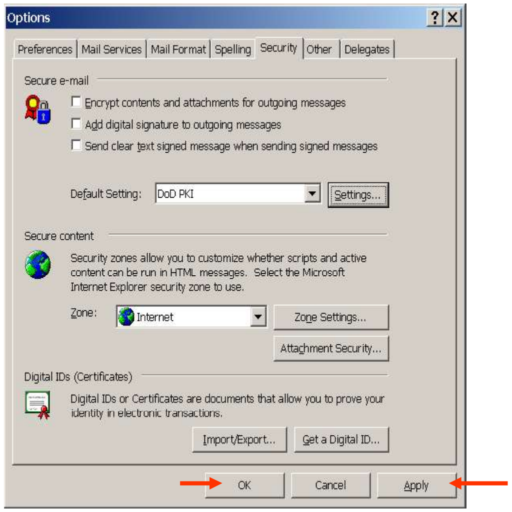
8

Choose **3DES** from the Encryption Certificate drop down box.

Check all 3 boxes in the Change Security Settings window.

Click **OK**.

Using PKI Certificates in Outlook (9)



Secure e-mail

☐ Encrypt contents and attachments for outgoing messages

☐ Add digital signature to outgoing messages

☐ Send clear text signed message when sending signed messages

Default Setting: DoD PKI

Secure content

Security zones allow you to customize whether scripts and active content can be run in HTML messages. Select the Microsoft Internet Explorer security zone to use.

Zone: Internet

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

9

Click the **Apply** button then click **OK**.

Authentication

What is authentication?

- Positive verification of identity (man or machine)
- Verification of a person’s claimed identity
- Who are you? Prove it.
- 3 Categories:
  - What you know
  - What you have
  - Who you are

What you know

- Password
- Passphrase
- PIN

What you have

- Digital authentication
  - physical devices to aid authentication
- Common examples:
  - eToken
  - smart cards
  - RFID

eToken

- Can be implemented on a USB key fob or a smart card
- Data physically protected on the device itself
- On the client side, the token is accessed via password
- Successful client-side authentication with the password invokes the token to generate a stored or generated **passcode**, which is sent to the server-side for authentication.

eToken

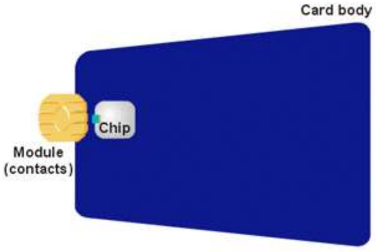
- May store credentials such as passwords, digital signatures and certificates, and private keys
- Can offer on-board authentication and digital signing

Smart cards

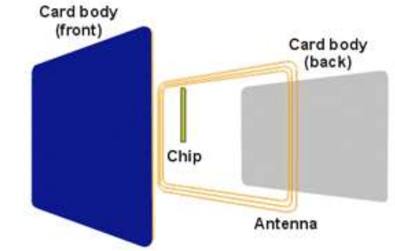
- Size of a credit card
- Usually an embedded microprocessor with computational and storage capabilities
- Programmable platforms:
  - C/C++
  - Visual Basic
  - Java
  - .Net (beta)

Smart Cards cont'd

- Contact vs. contactless
- Memory vs. microprocessor



Source: Gemplus - All About Smart Cards



Source: Gemplus - All About Smart Cards

RFID

- RFID - Radio Frequency IDentification
- Integrated circuit(s) with an antenna that can respond to an RF signal with identity information
- No power supply necessary—IC uses the RF signal to power itself
- Susceptible to replay attacks and theft
- Examples:
  - Smart Tag, EZPass
  - Garage parking permits

RFID

- 13.56Mhz read/write support
- May communicate with a variety of transponders (ISO15693, ISO14443 Type A & B, TagIt, Icode, etc.)
- Reader is controlled via PCMCIA interface using an ASCII protocol

Who you are

- Biometric authentication
  - Use of a biometric reading to confirm that a person is who he/she claims to be
- Biometric reading
  - A recording of some physical or behavioral attribute of a person

Physical Biometrics

- Fingerprint
- Iris
- Hand Geometry
- Finger Geometry
- Face Geometry
- Ear Shape
- Retina
- Smell
- Thermal Face
- Hand Vein
- Nail Bed
- DNA
- Palm Print

Behavioral Biometrics

- Signature
- Voice
- Keystroke
- Gait

Fingerprint Basics

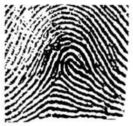
- Global features
  - Features that can be seen with the naked eye
  - Basic ridge patterns
- Local features
  - Minutia points
  - Tiny unique characteristics of fingerprint ridges used for positive identification

Fingerprints

- Vast amount of data available on fingerprint pattern matching
- Data originally from forensics
- Over 100 years of data to draw on
  - Thus far all prints obtained have been unique

Basic Ridge Patterns

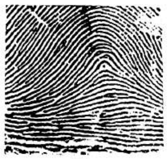
- Loop
  - 65% of all fingerprints

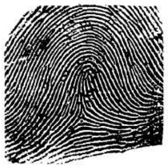

89s. Loop.

89t. Loop.

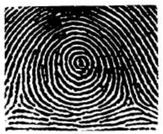
89u. Loop.

- Arch
  - Plain and tented arch


106


89w. Tented arch.

- Whorl
  - 30% of all fingerprints
  - One complete circle


92b

92c

92d

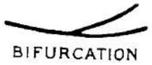
Local Features

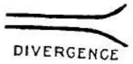
- Also known as *minutia points*
- Used for positive identification
- Two or more individuals may have the same global features, but different minutia
- Minutia points do not have to be inside the pattern area

Minutia Characteristics

- Orientation
  - The direction the minutia is facing
- Spatial frequency
  - How far apart the ridges are around the point
- Curvature
  - Rate of change of orientation
- Position
  - X,Y location relative to some fixed points

Types of Minutia

- Ridge ending
- Ridge bifurcation 

- Ridge divergence 

- Dot or island – ridge so short it appears to be a dot
- Enclosure – ridge separates and then reunites around an area of ridge-less skin
- Short ridge – bigger than a dot

Algorithms

- Image-based
- Pattern-based
- Minutia-based

Fingerprint Scanners

Digital Persona U.are.U Pro

HP IPAQ

IBM Thinkpad T42

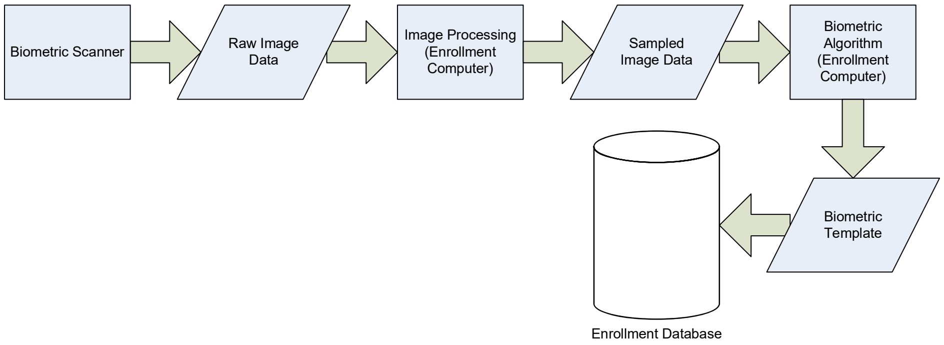
Review: Three Categories

- What you know
  - Password
  - PIN
- What you have
  - e-Token
  - RFID
- Who you are
  - Biometrics

Biometric Authentication Terms

- False Acceptance Rate (FAR)
  - False Match Rate (FMR)
  - Percentage of access attempts by unauthorized individuals which are nevertheless successful
- False Rejection Rate (FRR)
  - False Non-Match Rate (FNMR)
  - Percentage of access attempts by enrolled individuals who are nevertheless rejected
- Equal Error Rate
  - FAR = FRR

Enrollment



Biometric Scanner

Raw Image Data

Image Processing (Enrollment Computer)

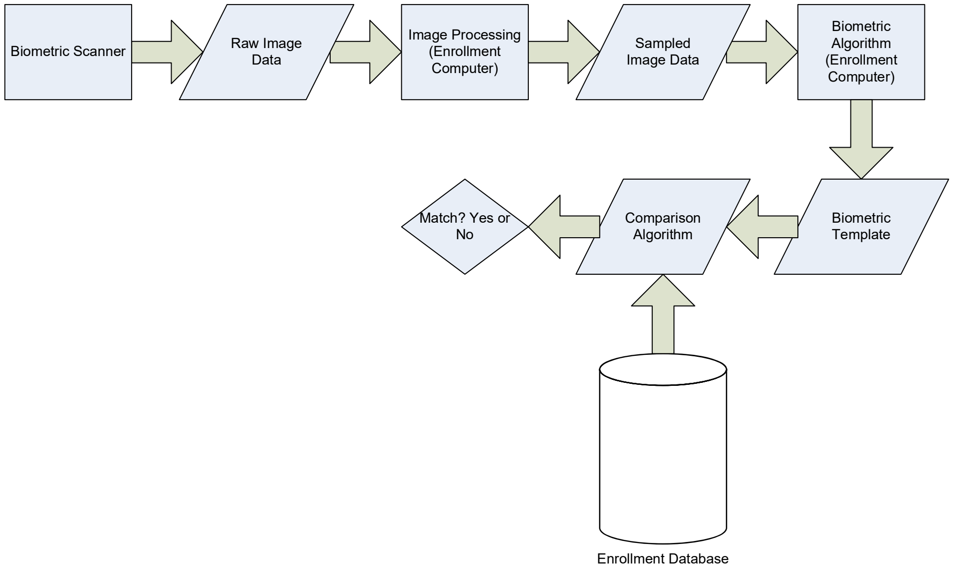
Sampled Image Data

Biometric Algorithm (Enrollment Computer)

Biometric Template

Enrollment Database

Verification



Motivation

- Real-world considerations:
  - What you know and what you have
    - Can be stolen or forgotten
    - Susceptible to replay attacks
  - Who you are
    - Unique biometrics that hinder replay attacks and imposters
    - Privacy issues arise

Authentication Token Formats

- A security token (authentication token) is a representation of security-related data (not to be confused with an e-Token)
- Examples:
  - X.509 certificates
  - Kerberos tickets
  - Custom security tokens

X.509 Certificates

- Use of digital certificates issued by a trusted Certificate Authority (e.g. VeriSign)
- A Digital Certificate contains information to assert an identity claim
  - Name
  - Serial number
  - Expiration dates
  - Certificate holder’s public key (used for encrypting/decrypting messages and digital signatures)
  - Digital signature of Certificate Authority (so recipient knows that the certificate is valid)
- The recipient may confirm the identity of the sender with the Certificate Authority

Kerberos Tickets

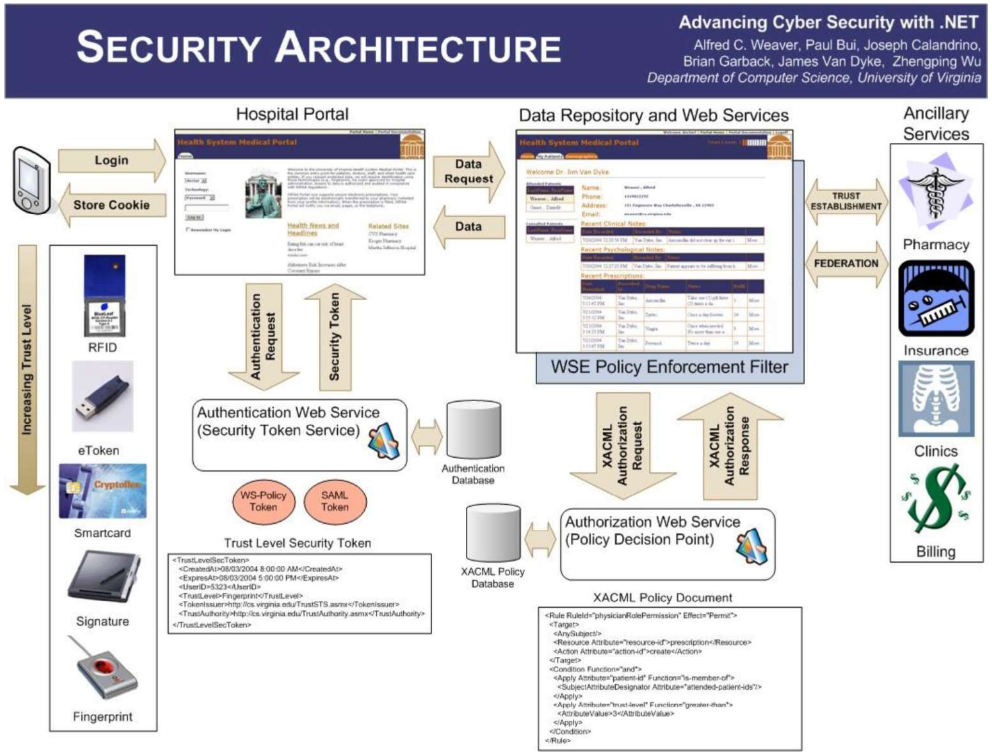
- Clients share secret symmetric key with server
- Clients login to authentication server
- Server returns a Ticket-Granting Ticket (TGT) encrypted with client’s key
- Client sends decrypted TGT to Ticket Granting Service
- TGS sends ticket authorizing network access and certain services
- Session ticket data:
  - Name
  - Network address
  - Time stamp
  - Expiration dates
  - Session key

Trust Level Extension

- Different trust levels for devices with different levels of implementation reliability
- Still very abstract and should be further developed
  - definition
  - representation
  - storage
  - exchange
  - verification
  - translation across trust domains

Custom Security Tokens

- May contain additional context information:
  - Access method
    - wired, local terminal
    - wired remote terminal
    - wireless PDA
  - Authentication method
    - Password
    - e-Token
    - Fingerprint
  - Trust level



Security Architecture

Advancing Cyber Security with .NET

Alfred C. Weaver, Paul Bui, Joseph Calandrino, Brian Garback, James Van Dyke, Zhengping Wu

Department of Computer Science, University of Virginia

Trust Level Security Token

```
<TrustLevelSecToken>
  <CreatedAt>08/03/2004 8:00:00 AM</CreatedAt>
  <ExpiresAt>08/03/2004 5:00:00 PM</ExpiresAt>
  <UserID>5323</UserID>
  <TrustLevel>Fingerprint</TrustLevel>
  <TokenIssuer>http://cs.virginia.edu/TrustSTS.asmx</TokenIssuer>
  <TrustAuthority>http://cs.virginia.edu/TrustAuthority.asmx</TrustAuthority>
</TrustLevelSecToken>
```

XACML Policy Document

```
<Rule RuleId="physicianRolePermission" Effect="Permit">
 <Target>
  <AnySubject/>
  <Resource Attribute="resource-id">prescription</Resource>
  <Action Attribute="action-id">create</Action>
 </Target>
 <Condition Function="and">
  <Apply Attribute="patient-id" Function="is-member-of">
   <SubjectAttributeDesignator Attribute="attended-patient-ids"/>
  </Apply>
  <Apply Attribute="trust-level" Function="greater-than">
   <AttributeValue>3</AttributeValue>
  </Apply>
 </Condition>
</Rule>
```

Example Authentication (Security) Token Request

```
<AuthenticationToken>
    <CreatedAt>08/03/2004 8:00:00 AM</CreatedAt>
    <ExpiresAt>08/03/2004 5:00:00 PM</ExpiresAt>
    <Username>Weaver</Username>
    <KeyStr>FINGERPRINT_KEY_STRING</KeyStr>
    <Technology>Fingerprint</Technology>
</AuthenticationToken>
```

Example Authentication (Security) Token Reply

```
<TrustLevelSecToken>
  <CreatedAt>08/03/2004 8:00:00 AM</CreatedAt>
  <ExpiresAt>08/03/2004 5:00:00 PM</ExpiresAt>
  <UserID>5323</UserID>
  <TrustLevel>Fingerprint</TrustLevel>
  <TokenIssuer>http://cs.virginia.edu/TrustSTS.asmx</TokenIssuer>
  <TrustAuthority>http://cs.virginia.edu/TrustAuthority.asmx</TrustAuthority>
</TrustLevelSecToken>
```

Remote User Authentication

- Remote user authentication is a kind of authentication that enables our users to identify themselves for using e-resources when they are off-campus.
- Approaches
  - Direct Dial-in
  - Referer URL Authentication
  - Authenticated Proxy-server

Referrer URL

- Also called Referring or Referral URL
- Steps for referrer URL authentication
  - A controlled-access web page registered with e-resource venders
    - Users must have a valid username/password to enter the page
  - Vendor allows access if user selects database URL from that page
    - Library has to register the page to each vendor
    - Vendor has to support HTTP environment variable HTTP_REFERER
  - When a user clicks a database URL from that page, a request with HTTP_REFERER (=URL of that controlled-access page) is sent to vendor

Referrer URL (Cont.)

- Advantages
  - Easy to set up
    - No additional software
    - Authentication is done by the web server
    - No additional hardware
  - Simple user training issues
    - No client-side setup involved
    - No browser version issues
    - Just train them to login

- Disadvantages
  - Not very flexible
    - Can't bookmark
    - Difficult to link from multiple pages
    - Multiple database URLs from vendor
  - Vendor may not support Referrer URLs
  - Vendor may not support multiple Referrer URLs
  - Not scale well

Proxy Servers

- Perform web retrievals on behalf of a web browser
- Most often used to speed up Internet access and reduce bandwidth by caching frequently used pages
- Libraries use proxy servers to make off-campus web clients look like on-campus ones
- Authenticated users are allowed to relay requests through our IP address space

Proxy Servers (Cont.)

- Advantages
  - Can place database links anywhere
  - A single URL from the database vendor
  - Proxy servers scale better
- Disadvantages
  - Problems with auto-configuration proxy
  - Problems with multiple proxy servers
  - Problems with firewalls
  - All traffic goes through proxy server (single point of failure)
  - User has to manually configure and un-configure settings

Bibliography

- Authentication
  - L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-2040.
- Kerberos
  - http://www.computerworld.com/computerworld/records/images/pdf/kerberos_chart.pdf

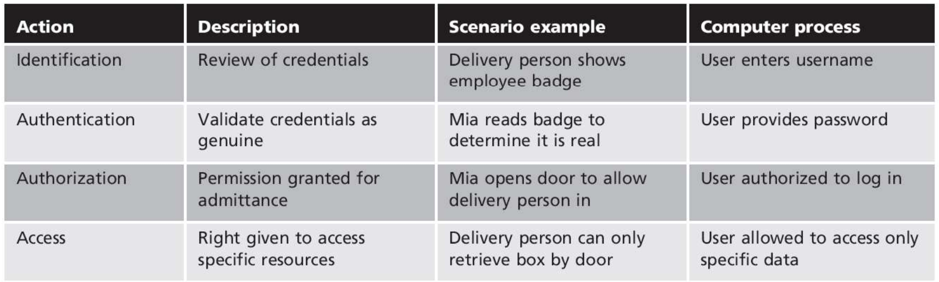
Access Control

What Is Access Control?

- Granting or denying approval to use specific resources
- Information system’s mechanism to allow or restrict access to data or devices
- Four standard models
- Specific practices used to enforce access control

Access Control Terminology

- Identification
  - Presenting credentials
  - Example: delivery driver presenting employee badge
- Authentication
  - Checking the credentials
  - Example: examining the delivery driver’s badge
- Authorization
  - Granting permission to take action
  - Example: allowing delivery driver to pick up package

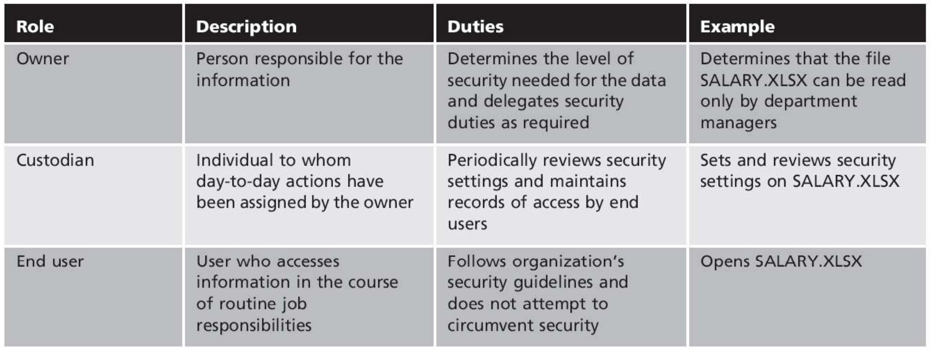


Action	Description	Scenario example	Computer process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Mia reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Mia opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data

Basic steps in access control

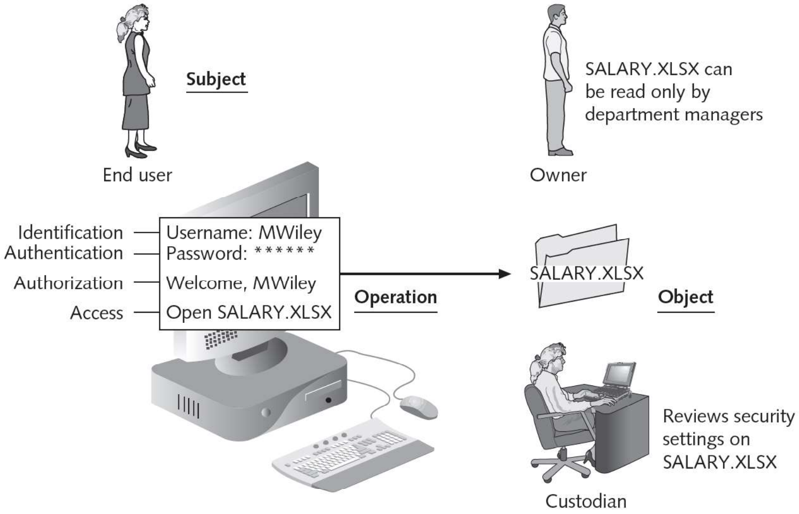
Access Control Terminology (cont’d.)

- Object
  - Specific resource
  - Example: file or hardware device
- Subject
  - User or process functioning on behalf of a user
  - Example: computer user
- Operation
  - Action taken by the subject over an object
  - Example: deleting a file



Role	Description	Duties	Example
Owner	Person responsible for the information	Determines the level of security needed for the data and delegates security duties as required	Determines that the file SALARY.XLSX can be read only by department managers
Custodian	Individual to whom day-to-day actions have been assigned by the owner	Periodically reviews security settings and maintains records of access by end users	Sets and reviews security settings on SALARY.XLSX
End user	User who accesses information in the course of routine job responsibilities	Follows organization’s security guidelines and does not attempt to circumvent security	Opens SALARY.XLSX

Roles in access control



Access control process and terminology

Access Control Models

- Standards that provide a predefined framework for hardware or software developers
- Used to implement access control in a device or application
- Custodians can configure security based on owner’s requirements
- Four major access control models
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)

Access Control Models (cont’d.)

- Four major access control models (cont’d.)
  - Role Based Access Control (RBAC)
  - Rule Based Access Control (RBAC)
- Mandatory Access Control
  - Most restrictive access control model
  - Typically found in military settings
  - Two elements
    - Labels
    - Levels

Access Control Models (cont’d.)

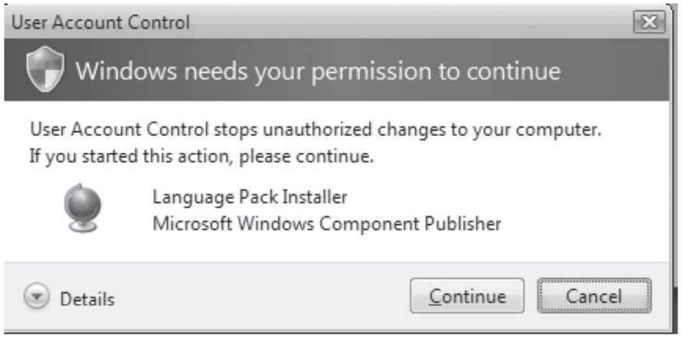
- MAC grants permissions by matching object labels with subject labels
  - Labels indicate level of privilege
- To determine if file may be opened:
  - Compare object and subject labels
  - Subject must have equal or greater level than object to be granted access
- Two major implementations of MAC
  - Lattice model
  - Bell-LaPadula model

Access Control Models (cont’d.)

- Lattice model
  - Subjects and objects are assigned a “rung” on the lattice
  - Multiple lattices can be placed beside each other
- Bell-LaPadula
  - Similar to lattice model
  - Subjects may not create a new object or perform specific functions on lower level objects

Access Control Models (cont’d.)

- Example of MAC implementation
  - Windows 7/Vista has four security levels
  - Specific actions by a subject with lower classification require administrator approval
- Discretionary Access Control (DAC)
  - Least restrictive model
  - Every object has an owner
  - Owners have total control over their objects
  - Owners can give permissions to other subjects over their objects


User Account Control

Windows needs your permission to continue

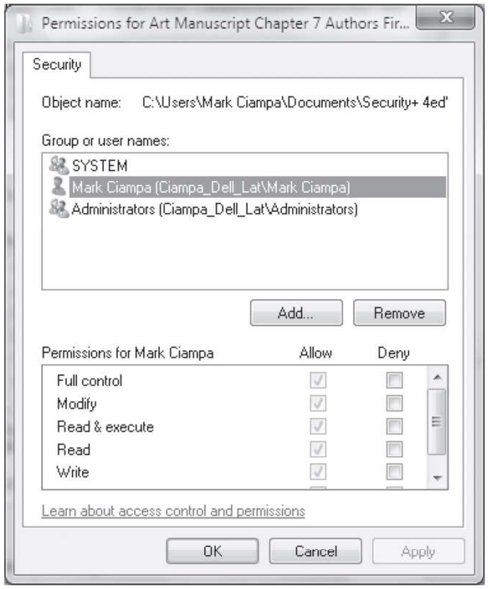
User Account Control stops unauthorized changes to your computer.
If you started this action, please continue.

Language Pack Installer
Microsoft Windows Component Publisher

Windows User Account Control (UAC) dialog box

Access Control Models (cont’d.)

- Discretionary Access Control (cont’d.)
  - Used on operating systems such as most types of UNIX and Microsoft Windows
- DAC weaknesses
  - Relies on decisions by end user to set proper security level
    - Incorrect permissions may be granted
  - Subject’s permissions will be “inherited” by any programs the subject executes
  - Trojans are a particular problem with DAC


Permissions for Art Manuscript Chapter 7 Authors Fir...

Object name: C:\Users\Mark Ciampa\Documents\Security+ 4ed'

Group or user names:

SYSTEM
Mark Ciampa (Ciampa_Dell_Lat\Mark Ciampa)
Administrators (Ciampa_Dell_Lat\Administrators)

Permissions for Mark Ciampa	Allow	Deny
Full control	☑	☐
Modify	☑	☐
Read & execute	☑	☐
Read	☑	☐
Write	☑	☐

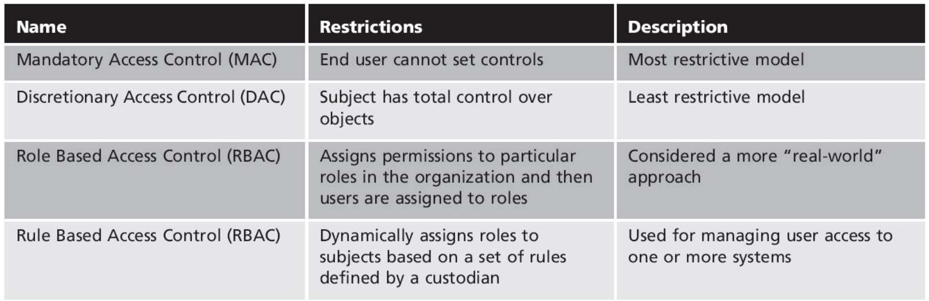
Discretionary Access Control (DAC)

Access Control Models (cont’d.)

- Role Based Access Control (RBAC)
  - Also called Non-discretionary Access Control
  - Access permissions are based on user’s job function
- RBAC assigns permissions to particular roles in an organization
  - Users are assigned to those roles
- Rule Based Access Control (RBAC)
  - Dynamically assigns roles to subjects based on a set of rules defined by a custodian

Access Control Models (cont'd.)

- Rule Based Access Control (cont'd.)
  - Each resource object contains access properties based on the rules
  - When user attempts access, system checks object's rules to determine access permission
  - Often used for managing user access to one or more systems
    - Business changes may trigger application of the rules specifying access changes



Name	Restrictions	Description
Mandatory Access Control (MAC)	End user cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
Role Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real-world" approach
Rule Based Access Control (RBAC)	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems

Access control models

Best Practices for Access Control

- Establishing best practices for limiting access
  - Can help secure systems and data
- Examples of best practices
  - Separation of duties
  - Job rotation
  - Least privilege
  - Implicit deny
  - Mandatory vacations

Best Practices for Access Control (cont'd.)

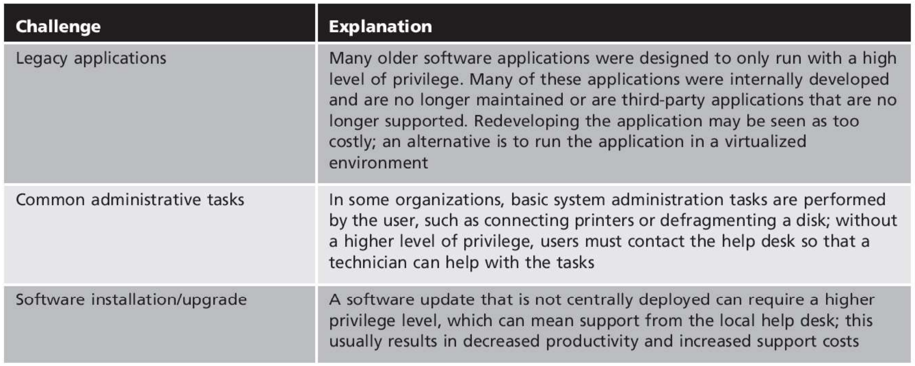
- Separation of duties
  - Fraud can result from single user being trusted with complete control of a process
  - Requiring two or more people responsible for functions related to handling money
  - System is not vulnerable to actions of a single person
- Job rotation
  - Individuals periodically moved between job responsibilities

Best Practices for Access Control (cont'd.)

- Job rotation (cont'd.)
  - Employees can rotate within their department or across departments
- Advantages of job rotation
  - Limits amount of time individuals are in a position to manipulate security configurations
  - Helps expose potential avenues for fraud
    - Individuals have different perspectives and may uncover vulnerabilities
  - Reduces employee burnout

Best Practices for Access Control (cont'd.)

- Least privilege
  - Limiting access to information based on what is needed to perform a job function
  - Helps reduce attack surface by eliminating unnecessary privileges
  - Should apply to users and processes on the system
  - Processes should run at minimum security level needed to correctly function
  - Temptation to assign higher levels of privilege is great



Challenge	Explanation
Legacy applications	Many older software applications were designed to only run with a high level of privilege. Many of these applications were internally developed and are no longer maintained or are third-party applications that are no longer supported. Redeveloping the application may be seen as too costly; an alternative is to run the application in a virtualized environment
Common administrative tasks	In some organizations, basic system administration tasks are performed by the user, such as connecting printers or defragmenting a disk; without a higher level of privilege, users must contact the help desk so that a technician can help with the tasks
Software installation/upgrade	A software update that is not centrally deployed can require a higher privilege level, which can mean support from the local help desk; this usually results in decreased productivity and increased support costs

Challenges of least privilege

Best Practices for Access Control (cont'd.)

- Implicit deny
  - If a condition is not explicitly met, access request is rejected
  - Example: network router rejects access to all except conditions matching the rule restrictions
- Mandatory vacations
  - Limits fraud, because perpetrator must be present daily to hide fraudulent actions
  - Audit of employee's activities usually scheduled during vacation for sensitive positions

Access Control Lists

- Set of permissions attached to an object
- Specifies which subjects may access the object and what operations they can perform
- When subject requests to perform an operation:
  - System checks ACL for an approved entry
- ACLs usually viewed in relation to operating system files

Access Control Lists (cont'd.)

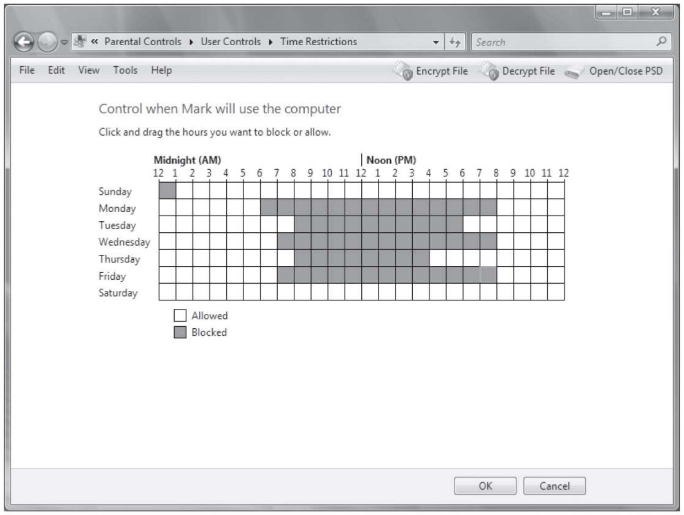
- Each entry in the ACL table is called access control entry (ACE)
- ACE structure (Windows)
  - Security identifier for the user or group account or logon session
  - Access mask that specifies access rights controlled by ACE
  - Flag that indicates type of ACE
  - Set of flags that determine whether objects can inherit permissions

Group Policies

- Microsoft Windows feature
  - Provides centralized management and configuration of computers and remote users using Active Directory (AD)
  - Usually used in enterprise environments
  - Settings stored in Group Policy Objects (GPOs)
- Local Group Policy
  - Fewer options than a Group Policy
  - Used to configure settings for systems not part of AD

Account Restrictions

- Time of day restrictions
  - Limits the time of day a user may log onto a system
  - Time blocks for permitted access are chosen
  - Can be set on individual systems
- Account expiration
  - Orphaned accounts: accounts that remain active after an employee has left the organization
  - Dormant accounts: not accessed for a lengthy period of time
  - Both can be security risks



Control when Mark will use the computer

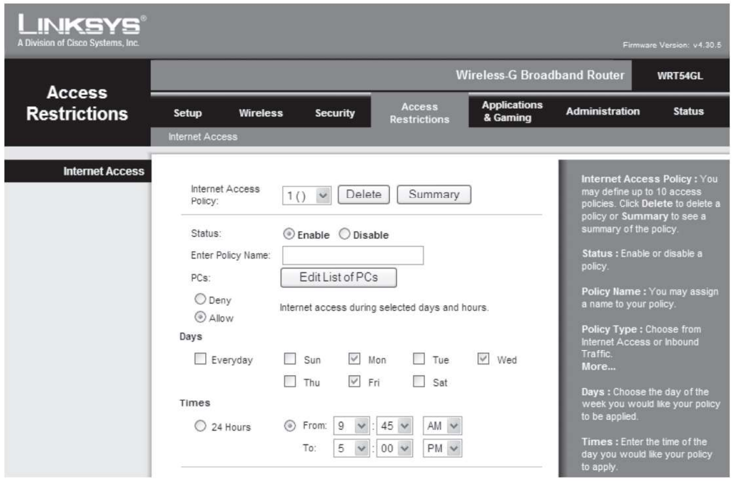
Click and drag the hours you want to block or allow.

	Midnight (AM)												Noon (PM)											
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sunday	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Monday	□	□	□	□	□	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□
Tuesday	□	□	□	□	□	□	□	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	□	□
Wednesday	□	□	□	□	□	□	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□
Thursday	□	□	□	□	□	□	□	□	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□	□	□	□	□
Friday	□	□	□	□	□	□	□	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	□	□	□	□
Saturday	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

□ Allowed

▨ Blocked

Operating system time of day restrictions



Internet Access Policy: 1 ()

Status: ● Enable ○ Disable

Enter Policy Name:

PCs:

○ Deny
● Allow
Internet access during selected days and hours.

Days

□ Everyday ☐ Sun ☑ Mon ☐ Tue ☑ Wed ☐ Thu ☑ Fri ☐ Sat

Times

○ 24 Hours ● From: 9 : 45 AM To: 5 : 00 PM

Internet Access Policy : You may define up to 10 access policies. Click **Delete** to delete a policy or **Summary** to see a summary of the policy.

Status : Enable or disable a policy.

Policy Name : You may assign a name to your policy.

Policy Type : Choose from Internet Access or Inbound Traffic.

Days : Choose the day of the week you would like your policy to be applied.

Times : Enter the time of the day you would like your policy to apply.

Wireless access point restrictions

Account Restrictions (cont'd.)

- Recommendations for dealing with orphaned or dormant accounts
  - Establish a formal process
  - Terminate access immediately
  - Monitor logs
- Orphaned accounts remain a problem in today's organizations
- Account expiration
  - Sets a user's account to expire

Account Restrictions (cont'd.)

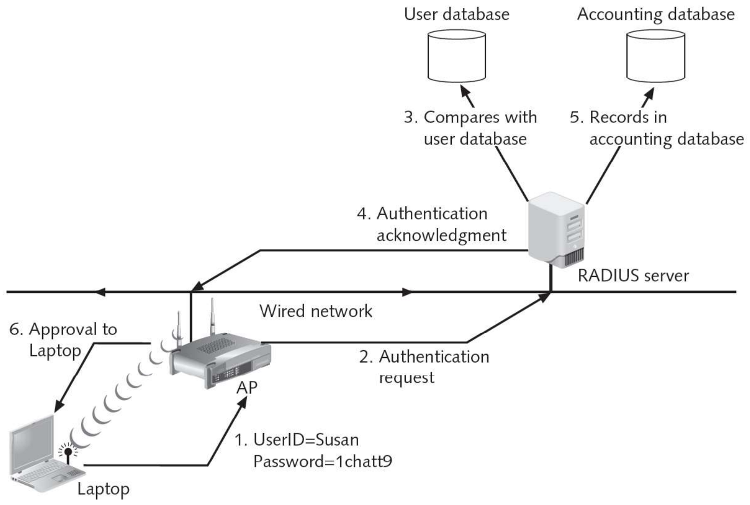
- Password expiration sets a time when user must create a new password
  - Different from account expiration
- Account expiration can be a set date, or a number of days of inactivity

Authentication Services

- Authentication
  - Process of verifying credentials
- Authentication services provided on a network
  - Dedicated authentication server
    - Or AAA server if it also performs authorization and accounting
- Common types of authentication and AAA servers
  - Kerberos, RADIUS, TACACS, LDAP

RADIUS

- Remote Authentication Dial In User Service
  - Developed in 1992
  - Became industry standard
  - Suitable for high volume service control applications
    - Such as dial-in access to corporate network
  - Still in use today
- RADIUS client
  - Typically a device such as a wireless AP
    - Responsible for sending user credentials and connection parameters to the RADIUS server


User database
Accounting database
3. Compares with user database
5. Records in accounting database
4. Authentication acknowledgment
RADIUS server
Wired network
6. Approval to Laptop
AP
2. Authentication request
1. UserID=Susan Password=1chatt9
Laptop

RADIUS authentication

RADIUS (cont’d.)

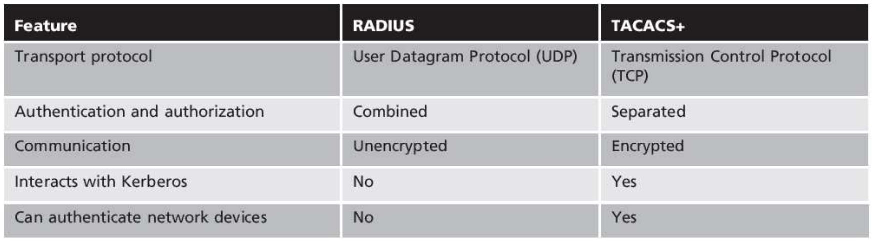
- RADIUS user profiles stored in central database
  - All remote servers can share
- Advantages of a central service
  - Increases security due to a single administered network point
  - Easier to track usage for billing and keeping network statistics

Kerberos

- Authentication system developed at MIT
  - Uses encryption and authentication for security
- Most often used in educational and government settings
- Works like using a driver’s license to cash a check
- Kerberos ticket
  - Contains information linking it to the user
  - User presents ticket to network for a service
  - Difficult to copy
  - Expires after a few hours or a day

Terminal Access Control Access Control System (TACACS)

- Authentication service similar to RADIUS
- Developed by Cisco Systems
- Commonly used on UNIX devices
- Communicates by forwarding user authentication information to a centralized server



Feature	RADIUS	TACACS+
Transport protocol	User Datagram Protocol (UDP)	Transmission Control Protocol (TCP)
Authentication and authorization	Combined	Separated
Communication	Unencrypted	Encrypted
Interacts with Kerberos	No	Yes
Can authenticate network devices	No	Yes

Comparison of RADIUS and TACACS+

Lightweight Directory Access Protocol (LDAP)

- Directory service
  - Database stored on a network
  - Contains information about users and network devices
  - Keeps track of network resources and user’s privileges to those resources
  - Grants or denies access based on its information
- Standard for directory services
  - X.500

Lightweight Directory Access Protocol (cont'd.)

- X.500 standard defines protocol for client application to access the DAP
- LDAP
  - A simpler subset of DAP
  - Designed to run over TCP/IP
  - Has simpler functions
  - Encodes protocol elements in simpler way than X.500
  - An open protocol

Lightweight Directory Access Protocol (cont'd.)

- Weakness of LDAP
  - Can be subject to LDAP injection attacks
    - Similar to SQL injection attacks
    - Occurs when user input is not properly filtered

Summary

- Access control is the process by which resources or services are denied or granted
- Four major access control models exist
- Best practices for implementing access control
  - Separation of duties
  - Job rotation
  - Least privilege
  - Mandatory vacations

Summary (cont'd.)

- Access control lists define which subjects are allowed to access which objects
  - Specify which operations they may perform
- Group Policy is a Windows feature that provides centralized management and configuration
- Authentication services can be provided on a network by a dedicated AAA or authentication server
  - RADIUS is the industry standard

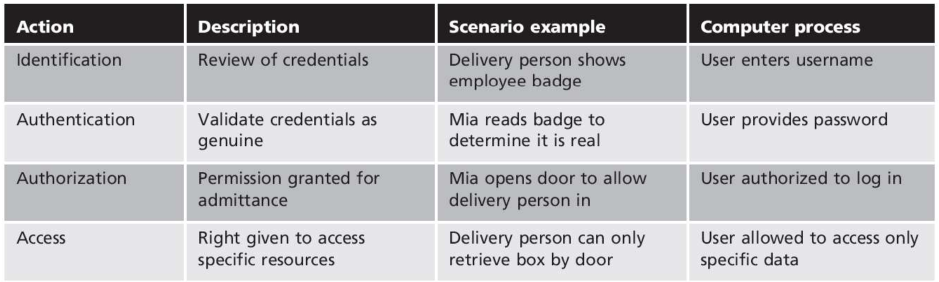
Access Control

What Is Access Control?

- Granting or denying approval to use specific resources
- Information system’s mechanism to allow or restrict access to data or devices
- Four standard models
- Specific practices used to enforce access control

Access Control Terminology

- Identification
  - Presenting credentials
  - Example: delivery driver presenting employee badge
- Authentication
  - Checking the credentials
  - Example: examining the delivery driver’s badge
- Authorization
  - Granting permission to take action
  - Example: allowing delivery driver to pick up package

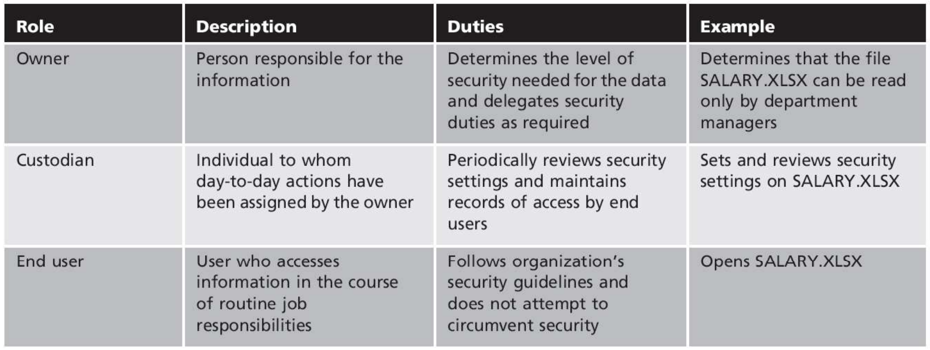


Action	Description	Scenario example	Computer process
Identification	Review of credentials	Delivery person shows employee badge	User enters username
Authentication	Validate credentials as genuine	Mia reads badge to determine it is real	User provides password
Authorization	Permission granted for admittance	Mia opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data

Basic steps in access control

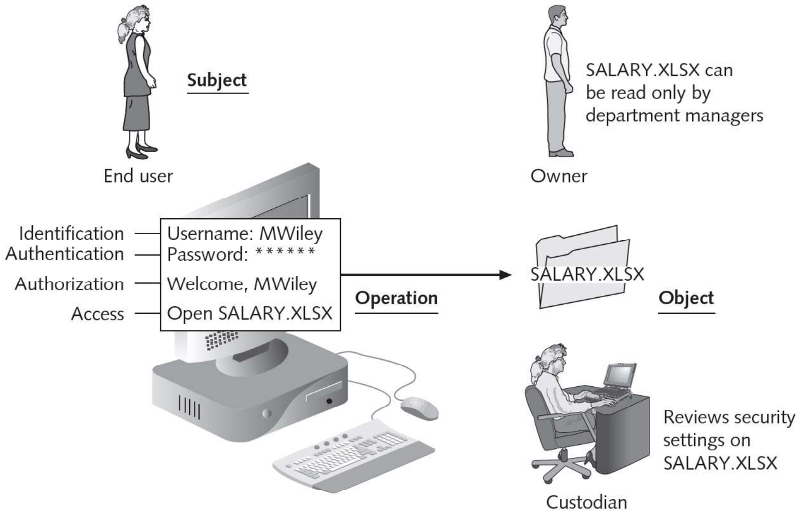
Access Control Terminology (cont'd.)

- Object
  - Specific resource
  - Example: file or hardware device
- Subject
  - User or process functioning on behalf of a user
  - Example: computer user
- Operation
  - Action taken by the subject over an object
  - Example: deleting a file



Role	Description	Duties	Example
Owner	Person responsible for the information	Determines the level of security needed for the data and delegates security duties as required	Determines that the file SALARY.XLSX can be read only by department managers
Custodian	Individual to whom day-to-day actions have been assigned by the owner	Periodically reviews security settings and maintains records of access by end users	Sets and reviews security settings on SALARY.XLSX
End user	User who accesses information in the course of routine job responsibilities	Follows organization's security guidelines and does not attempt to circumvent security	Opens SALARY.XLSX

Roles in access control



Access control process and terminology

Access Control Models

- Standards that provide a predefined framework for hardware or software developers
- Used to implement access control in a device or application
- Custodians can configure security based on owner's requirements
- Four major access control models
  - Mandatory Access Control (MAC)
  - Discretionary Access Control (DAC)

Access Control Models (cont’d.)

- Four major access control models (cont’d.)
  - Role Based Access Control (RBAC)
  - Rule Based Access Control (RBAC)
- Mandatory Access Control
  - Most restrictive access control model
  - Typically found in military settings
  - Two elements
    - Labels
    - Levels

Access Control Models (cont’d.)

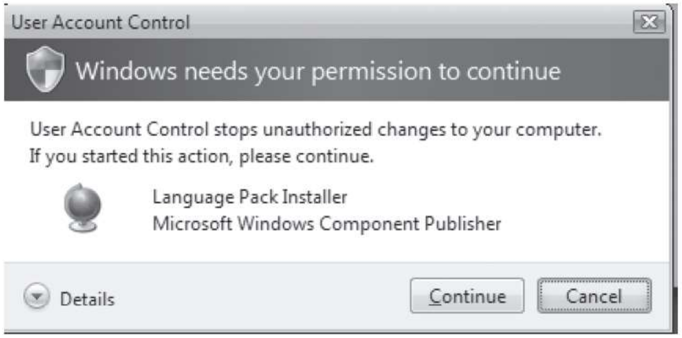
- MAC grants permissions by matching object labels with subject labels
  - Labels indicate level of privilege
- To determine if file may be opened:
  - Compare object and subject labels
  - Subject must have equal or greater level than object to be granted access
- Two major implementations of MAC
  - Lattice model
  - Bell-LaPadula model

Access Control Models (cont’d.)

- Lattice model
  - Subjects and objects are assigned a “rung” on the lattice
  - Multiple lattices can be placed beside each other
- Bell-LaPadula
  - Similar to lattice model
  - Subjects may not create a new object or perform specific functions on lower level objects

Access Control Models (cont’d.)

- Example of MAC implementation
  - Windows 7/Vista has four security levels
  - Specific actions by a subject with lower classification require administrator approval
- Discretionary Access Control (DAC)
  - Least restrictive model
  - Every object has an owner
  - Owners have total control over their objects
  - Owners can give permissions to other subjects over their objects



User Account Control

Windows needs your permission to continue

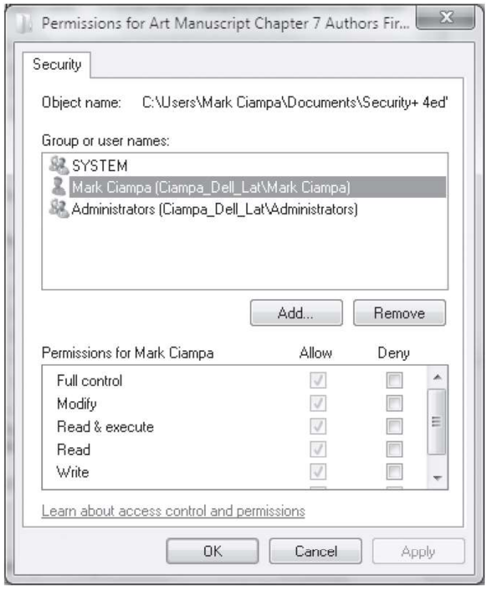
User Account Control stops unauthorized changes to your computer.
If you started this action, please continue.

Language Pack Installer
Microsoft Windows Component Publisher

Windows User Account Control (UAC) dialog box

Access Control Models (cont’d.)

- Discretionary Access Control (cont’d.)
  - Used on operating systems such as most types of UNIX and Microsoft Windows
- DAC weaknesses
  - Relies on decisions by end user to set proper security level
    - Incorrect permissions may be granted
  - Subject’s permissions will be “inherited” by any programs the subject executes
  - Trojans are a particular problem with DAC



Permissions for Art Manuscript Chapter 7 Authors Fir...

Security

Object name: C:\Users\Mark Ciampa\Documents\Security+ 4ed'

Group or user names:

SYSTEM
Mark Ciampa (Ciampa_Dell_Lat\Mark Ciampa)
Administrators (Ciampa_Dell_Lat\Administrators)

Permissions for Mark Ciampa	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
Read	☑	□
Write	☑	□

Learn about access control and permissions

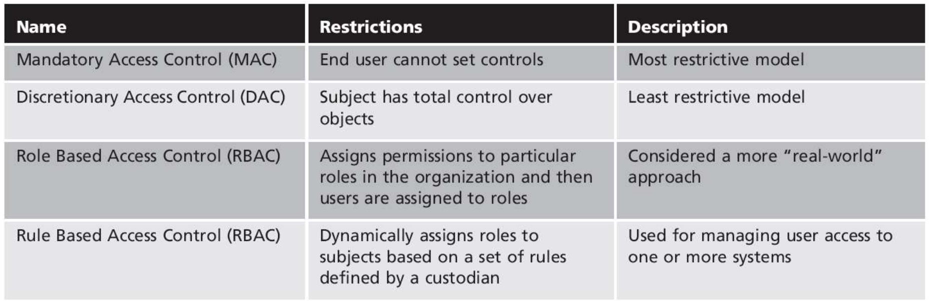
Discretionary Access Control (DAC)

Access Control Models (cont’d.)

- Role Based Access Control (RBAC)
  - Also called Non-discretionary Access Control
  - Access permissions are based on user’s job function
- RBAC assigns permissions to particular roles in an organization
  - Users are assigned to those roles
- Rule Based Access Control (RBAC)
  - Dynamically assigns roles to subjects based on a set of rules defined by a custodian

Access Control Models (cont'd.)

- Rule Based Access Control (cont'd.)
  - Each resource object contains access properties based on the rules
  - When user attempts access, system checks object's rules to determine access permission
  - Often used for managing user access to one or more systems
    - Business changes may trigger application of the rules specifying access changes



Name	Restrictions	Description
Mandatory Access Control (MAC)	End user cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
Role Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real-world" approach
Rule Based Access Control (RBAC)	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems

Access control models

Best Practices for Access Control

- Establishing best practices for limiting access
  - Can help secure systems and data
- Examples of best practices
  - Separation of duties
  - Job rotation
  - Least privilege
  - Implicit deny
  - Mandatory vacations

Best Practices for Access Control (cont'd.)

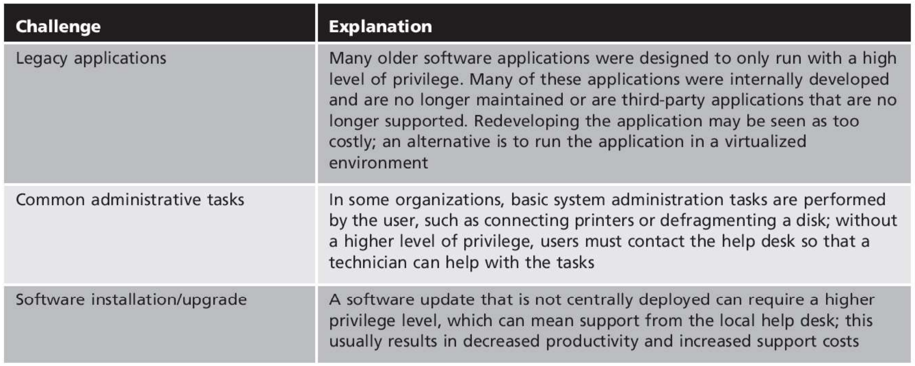
- Separation of duties
  - Fraud can result from single user being trusted with complete control of a process
  - Requiring two or more people responsible for functions related to handling money
  - System is not vulnerable to actions of a single person
- Job rotation
  - Individuals periodically moved between job responsibilities

Best Practices for Access Control (cont'd.)

- Job rotation (cont'd.)
  - Employees can rotate within their department or across departments
- Advantages of job rotation
  - Limits amount of time individuals are in a position to manipulate security configurations
  - Helps expose potential avenues for fraud
    - Individuals have different perspectives and may uncover vulnerabilities
  - Reduces employee burnout

Best Practices for Access Control (cont'd.)

- Least privilege
  - Limiting access to information based on what is needed to perform a job function
  - Helps reduce attack surface by eliminating unnecessary privileges
  - Should apply to users and processes on the system
  - Processes should run at minimum security level needed to correctly function
  - Temptation to assign higher levels of privilege is great



Challenge	Explanation
Legacy applications	Many older software applications were designed to only run with a high level of privilege. Many of these applications were internally developed and are no longer maintained or are third-party applications that are no longer supported. Redeveloping the application may be seen as too costly; an alternative is to run the application in a virtualized environment
Common administrative tasks	In some organizations, basic system administration tasks are performed by the user, such as connecting printers or defragmenting a disk; without a higher level of privilege, users must contact the help desk so that a technician can help with the tasks
Software installation/upgrade	A software update that is not centrally deployed can require a higher privilege level, which can mean support from the local help desk; this usually results in decreased productivity and increased support costs

Challenges of least privilege

Best Practices for Access Control (cont'd.)

- Implicit deny
  - If a condition is not explicitly met, access request is rejected
  - Example: network router rejects access to all except conditions matching the rule restrictions
- Mandatory vacations
  - Limits fraud, because perpetrator must be present daily to hide fraudulent actions
  - Audit of employee's activities usually scheduled during vacation for sensitive positions

Access Control Lists

- Set of permissions attached to an object
- Specifies which subjects may access the object and what operations they can perform
- When subject requests to perform an operation:
  - System checks ACL for an approved entry
- ACLs usually viewed in relation to operating system files

Access Control Lists (cont'd.)

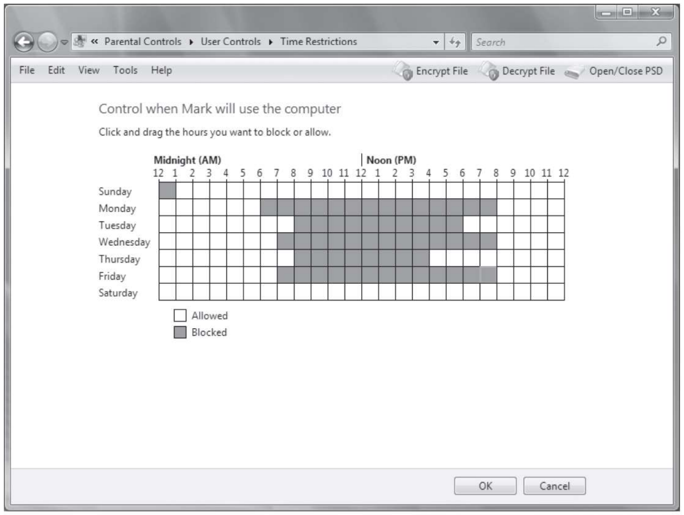
- Each entry in the ACL table is called access control entry (ACE)
- ACE structure (Windows)
  - Security identifier for the user or group account or logon session
  - Access mask that specifies access rights controlled by ACE
  - Flag that indicates type of ACE
  - Set of flags that determine whether objects can inherit permissions

Group Policies

- Microsoft Windows feature
  - Provides centralized management and configuration of computers and remote users using Active Directory (AD)
  - Usually used in enterprise environments
  - Settings stored in Group Policy Objects (GPOs)
- Local Group Policy
  - Fewer options than a Group Policy
  - Used to configure settings for systems not part of AD

Account Restrictions

- Time of day restrictions
  - Limits the time of day a user may log onto a system
  - Time blocks for permitted access are chosen
  - Can be set on individual systems
- Account expiration
  - Orphaned accounts: accounts that remain active after an employee has left the organization
  - Dormant accounts: not accessed for a lengthy period of time
  - Both can be security risks


« Parental Controls ▸ User Controls ▸ Time Restrictions
Search
File Edit View Tools Help
Encrypt File
Decrypt File
Open/Close PSD
OK
Cancel

Control when Mark will use the computer

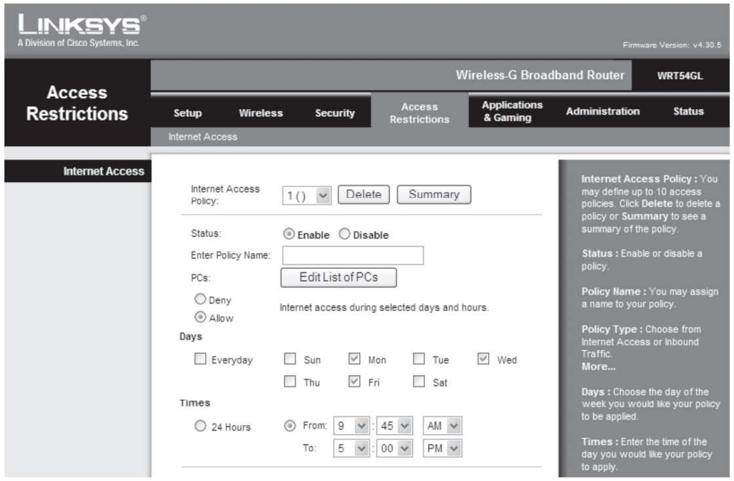
Click and drag the hours you want to block or allow.

Midnight (AM) | Noon (PM)

	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sunday	▨																							
Monday							▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨				
Tuesday									▨	▨	▨	▨	▨	▨	▨	▨	▨	▨						
Wednesday								▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨				
Thursday									▨	▨	▨	▨	▨	▨	▨	▨								
Friday								▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨				
Saturday																								

□ Allowed
▨ Blocked

Operating system time of day restrictions



Internet Access Policy: 1 () Delete Summary

Status: ● Enable ○ Disable

Enter Policy Name:

PCs: Edit List of PCs

○ Deny
● Allow
Internet access during selected days and hours.

Days

□ Everyday □ Sun ☑ Mon □ Tue ☑ Wed
□ Thu ☑ Fri □ Sat

Times

○ 24 Hours ● From: 9 : 45 AM
To: 5 : 00 PM

Internet Access Policy : You may define up to 10 access policies. Click **Delete** to delete a policy or **Summary** to see a summary of the policy.

Status : Enable or disable a policy.

Policy Name : You may assign a name to your policy.

Policy Type : Choose from Internet Access or Inbound Traffic.
More...

Days : Choose the day of the week you would like your policy to be applied.

Times : Enter the time of the day you would like your policy to apply.

Wireless access point restrictions

Account Restrictions (cont'd.)

- Recommendations for dealing with orphaned or dormant accounts
  - Establish a formal process
  - Terminate access immediately
  - Monitor logs
- Orphaned accounts remain a problem in today's organizations
- Account expiration
  - Sets a user's account to expire

Account Restrictions (cont'd.)

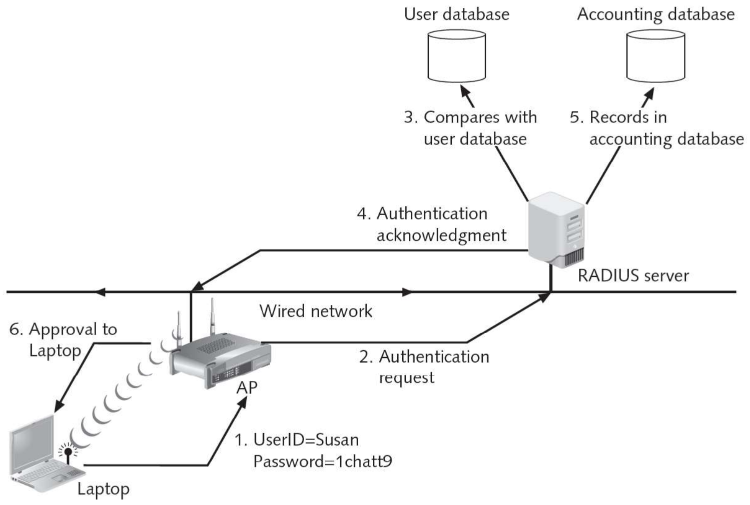
- Password expiration sets a time when user must create a new password
  - Different from account expiration
- Account expiration can be a set date, or a number of days of inactivity

Authentication Services

- Authentication
  - Process of verifying credentials
- Authentication services provided on a network
  - Dedicated authentication server
    - Or AAA server if it also performs authorization and accounting
- Common types of authentication and AAA servers
  - Kerberos, RADIUS, TACACS, LDAP

RADIUS

- Remote Authentication Dial In User Service
  - Developed in 1992
  - Became industry standard
  - Suitable for high volume service control applications
    - Such as dial-in access to corporate network
  - Still in use today
- RADIUS client
  - Typically a device such as a wireless AP
    - Responsible for sending user credentials and connection parameters to the RADIUS server


User database
Accounting database
3. Compares with user database
5. Records in accounting database
4. Authentication acknowledgment
RADIUS server
Wired network
6. Approval to Laptop
AP
2. Authentication request
1. UserID=Susan Password=1chatt9
Laptop

RADIUS authentication

RADIUS (cont’d.)

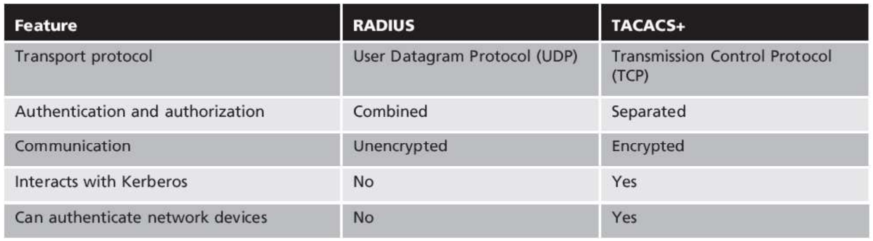
- RADIUS user profiles stored in central database
  - All remote servers can share
- Advantages of a central service
  - Increases security due to a single administered network point
  - Easier to track usage for billing and keeping network statistics

Kerberos

- Authentication system developed at MIT
  - Uses encryption and authentication for security
- Most often used in educational and government settings
- Works like using a driver's license to cash a check
- Kerberos ticket
  - Contains information linking it to the user
  - User presents ticket to network for a service
  - Difficult to copy
  - Expires after a few hours or a day

Terminal Access Control Access Control System (TACACS)

- Authentication service similar to RADIUS
- Developed by Cisco Systems
- Commonly used on UNIX devices
- Communicates by forwarding user authentication information to a centralized server



Feature	RADIUS	TACACS+
Transport protocol	User Datagram Protocol (UDP)	Transmission Control Protocol (TCP)
Authentication and authorization	Combined	Separated
Communication	Unencrypted	Encrypted
Interacts with Kerberos	No	Yes
Can authenticate network devices	No	Yes

Comparison of RADIUS and TACACS+

Lightweight Directory Access Protocol (LDAP)

- Directory service
  - Database stored on a network
  - Contains information about users and network devices
  - Keeps track of network resources and user's privileges to those resources
  - Grants or denies access based on its information
- Standard for directory services
  - X.500

Lightweight Directory Access Protocol (cont'd.)

- X.500 standard defines protocol for client application to access the DAP
- LDAP
  - A simpler subset of DAP
  - Designed to run over TCP/IP
  - Has simpler functions
  - Encodes protocol elements in simpler way than X.500
  - An open protocol

Lightweight Directory Access Protocol (cont'd.)

- Weakness of LDAP
  - Can be subject to LDAP injection attacks
    - Similar to SQL injection attacks
    - Occurs when user input is not properly filtered

Summary

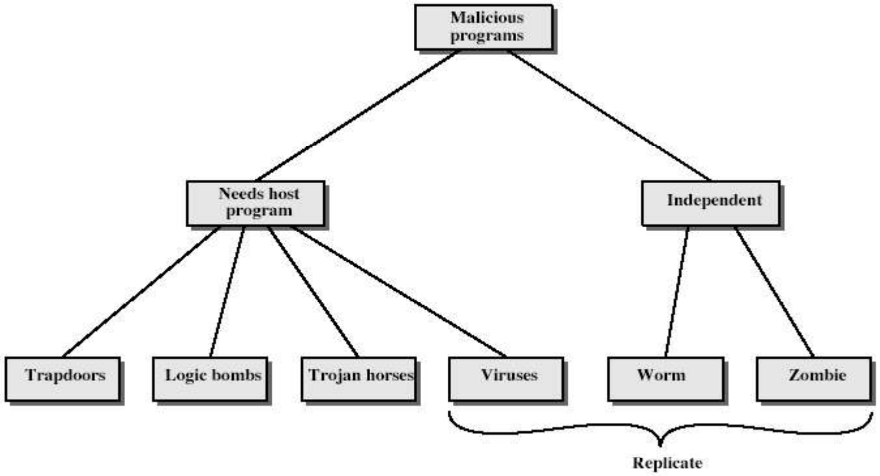
- Access control is the process by which resources or services are denied or granted
- Four major access control models exist
- Best practices for implementing access control
  - Separation of duties
  - Job rotation
  - Least privilege
  - Mandatory vacations

Summary (cont'd.)

- Access control lists define which subjects are allowed to access which objects
  - Specify which operations they may perform
- Group Policy is a Windows feature that provides centralized management and configuration
- Authentication services can be provided on a network by a dedicated AAA or authentication server
  - RADIUS is the industry standard

Malicious Software

Malicious Software



Viruses and Other Malicious Content

- computer viruses have got a lot of publicity
- one of a family of **malicious software**
- effects usually obvious
- have figured in news reports, fiction, movies (often exaggerated)
- getting more attention than deserve
- are a concern though

Trapdoors

- secret entry point into a program
- allows those who know access bypassing usual security procedures
- have been commonly used by developers
- a threat when left in production programs allowing exploited by attackers
- very hard to block in O/S
- requires good s/w development & update

Logic Bomb

- one of oldest types of malicious software
- code embedded in legitimate program
- activated when specified conditions met
  - eg presence/absence of some file
  - particular date/time
  - particular user
- when triggered typically damage system
  - modify/delete files/disks

Zombie

- program which secretly takes over another networked computer
- then uses it to indirectly launch attacks
- often used to launch distributed denial of service (DDoS) attacks
- exploits known flaws in network systems

Trojan Horse

- program with hidden side-effects
- which is usually superficially attractive
  - eg game, s/w upgrade etc
- when run performs some additional tasks
  - allows attacker to indirectly gain access they do not have directly
- often used to propagate a virus/worm or install a backdoor
- or simply to destroy data

Viruses

- a piece of self-replicating code attached to some other code
  - cf biological virus
- both propagates itself & carries a payload
  - carries code to make copies of itself
  - as well as code to perform some covert task

Virus Operation

- virus phases:
  - – dormant – waiting on trigger event
  - – propagation – replicating to programs/disks
  - – triggering – by event to execute payload
  - – execution – of payload
- details usually machine/OS specific
  - – exploiting features/weaknesses

Types of Viruses

- can classify on basis of how they attack
- parasitic virus-A Parasitic Virus (also referred to as a file virus) is a type of virus that spreads by attaching itself to another program
- memory-resident virus-A Memory-Resident Virus is a virus that is located in the memory of a computer, even after the ‘host’ application or program has stopped running (been terminated).

Virus Structure

```
program V :=
    {goto main;
    1234567;
    subroutine infect-executable :=         {loop:
                    file := get-random-executable-file;
                    if (first-line-of-file = 1234567) then goto loop
                    else prepend V to file; }
    subroutine do-damage :=        {whatever damage is to be done}
    subroutine trigger-pulled :=   {return true if some condition holds}
    main: main-program :=          {infect-executable;
                                   if trigger-pulled then do-damage;
                                   goto next;}
    next:
}
```

- boot sector virus- A boot sector virus is a type of virus that infects the boot sector of floppy disks or the primary boot record of hard disks (some infect the boot sector of the hard disk instead of the primary boot record).
- stealth-A stealth virus is a computer virus that uses various mechanisms to avoid detection by antivirus software.

- polymorphic virus-A polymorphic virus, sometimes referred to as a metamorphic virus, is a type of malware that is programmed to repeatedly mutate its appearance or signature files through new decryption routines.

Email Virus

- spread using email with attachment containing a macro virus
  - cf Melissa
- triggered when user opens attachment
- or worse even when mail viewed by using scripting features in mail agent
- usually targeted at Microsoft Outlook mail agent & Word/Excel documents

Macro Virus

- **macro code** attached to some **data file**
- interpreted by program using file
  - eg Word/Excel macros
  - esp. using auto command & command macros
- code is now platform independent
- is a major source of new viral infections
- blurs distinction between data and program files making task of detection much harder
- classic trade-off: "ease of use" vs "security"

Worms

- replicating but not infecting program
- typically spreads over a network
  - cf Morris Internet Worm in 1988
  - led to creation of CERTs
- using users distributed privileges or by exploiting system vulnerabilities
- widely used by hackers to create **zombie PC's**, subsequently used for further attacks, esp DoS
- major issue is lack of security of permanently connected systems, esp PC's

Worm Operation

- worm phases like those of viruses:
  - dormant
  - propagation
    - search for other systems to infect
    - establish connection to target remote system
    - replicate self onto remote system
  - triggering
  - execution

Recent Worm Attacks

- new spate of attacks from mid-2001
- **Code Red**
  - exploited bug in MS IIS to penetrate & spread
  - probes random IPs for systems running IIS
  - had trigger time for denial-of-service attack
  - 2nd wave infected 360000 servers in 14 hours
- **Code Red 2**
  - had backdoor installed to allow remote control
- **Nimda**
  - used multiple infection mechanisms
    - email, shares, web client, IIS, Code Red 2 backdoor

Morris Worm

- best known classic worm
- released by Robert Morris in 1988
- targeted Unix systems
- using several propagation techniques
  - simple password cracking of local pw file
  - exploit bug in finger daemon
  - exploit debug trapdoor in sendmail daemon
- if any attack succeeds then replicated self

Virus Countermeasures

- viral attacks exploit lack of integrity control on systems
- to defend need to add such controls
- typically by one or more of:
  - **prevention** - block virus infection mechanism
  - **detection** - of viruses in infected system
  - **reaction** - restoring system to clean state

Anti-Virus Software

- **first-generation**
  - scanner uses virus signature to identify virus
  - or change in length of programs
- **second-generation**
  - uses heuristic rules to spot viral infection
  - or uses program checksums to spot changes
- **third-generation**
  - memory-resident programs identify virus by actions
- **fourth-generation**
  - packages with a variety of antivirus techniques
  - eg scanning & activity traps, access-controls

Behavior-Blocking Software

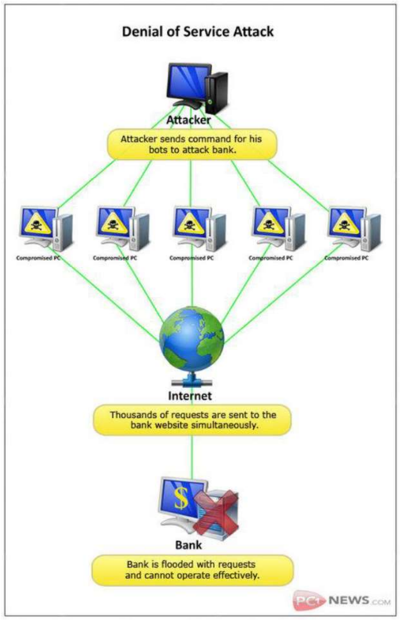
- integrated with host O/S
- monitors program behavior in real-time
  - eg file access, disk format, executable mods, system settings changes, network access
- for possibly malicious actions
  - if detected can block, terminate, or seek ok
- has advantage over scanners
- but malicious code runs before detection

Advanced Anti-Virus Techniques

- generic decryption
  - use CPU simulator to check program signature & behavior before actually running it
- digital immune system (IBM)
  - general purpose emulation & virus detection
  - any virus entering org is captured, analyzed, detection/shielding created for it, removed

Network Security

TYPES OF DOS ATTACKS


Denial of Service Attack
Attacker
Attacker sends command for his bots to attack bank.
Compromised PC
Compromised PC
Compromised PC
Compromised PC
Compromised PC
Internet
Thousands of requests are sent to the bank website simultaneously.
Bank
Bank is flooded with requests and cannot operate effectively.
PCT NEWS.COM

WHAT IS “DOS ATTACK”

Denial-Of-Service Attack = DOS Attack is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to it customers.

- DoS = when a single host attacks
- DDoS = when multiple hosts attack simultaneously

TYPES OF DOS ATTACKS

- Penetration
- Eavesdropping
- Man-In-The-Middle
- Flooding

TYPES OF DOS ATTACKS

Penetration

- Attacker gets inside your machine
- Can take over machine and do whatever he wants
- Achieves entry via software flaw(s), stolen passwords or insider access

TYPES OF DOS ATTACKS

Man-in-the-Middle

- Attacker listens to output and controls output
- Can substitute messages in both directions

TYPES OF DOS ATTACKS

Eavesdropping

- Attacker gains access to same network
- Listens to traffic going in and out of your machine

TYPES OF DOS ATTACKS

Flooding

- Attacker sends an overwhelming number of messages at your machine; great congestion
- The congestion may occur in the path before your machine
- Messages from legitimate users are crowded out
- Usually called a Denial of Service (DoS) attack, because that’s the effect.
- Usually involves a large number of machines, hence Distributed Denial of Service (DDoS) attack

HOW TO DEFEND

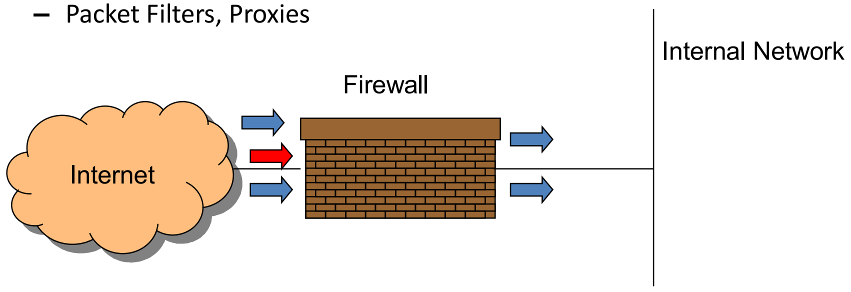
- Firewalls - can effectively prevent users from launching simple flooding type attacks from machines behind the firewall.
- Switches - Some switches provide automatic and/or system-wide rate limiting, traffic shaping, delayed binding to detect and remediate denial of service attacks
- Routers - If you add rules to take flow statistics out of the router during the DoS attacks, they further slow down and complicate the matter

Firewalls

- Lots of vulnerabilities on hosts in network
- Users don’t keep systems up to date
  - Lots of patches
  - Lots of exploits in wild (no patch for them)
- Solution?
  - Limit access to the network
  - Put firewalls across the perimeter of the network

Firewalls (contd…)

- Firewall inspects traffic through it
- Allows traffic specified in the policy
- Drops everything else
- Two Types
  - Packet Filters, Proxies



Packet Filters

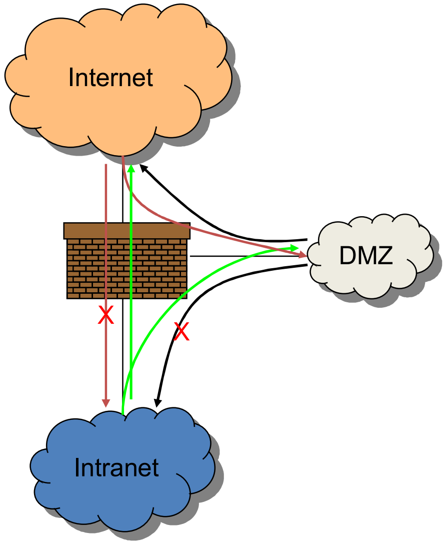
- Packet filter selectively passes packets from one network interface to another
- Usually done within a router between external and internal networks
  - screening router
- Can be done by a dedicated network element
  - packet filtering bridge
  - harder to detect and attack than screening routers

Packet Filters Contd.

- **Data Available**
  - IP source and destination addresses
  - Transport protocol (TCP, UDP, or ICMP)
  - TCP/UDP source and destination ports
  - ICMP message type
  - Packet options (Fragment Size etc.)
- **Actions Available**
  - Allow the packet to go through
  - Drop the packet (Notify Sender/Drop Silently)
  - Alter the packet (NAT?)
  - Log information about the packet

Typical Firewall Configuration

- Internal hosts can access DMZ and Internet
- External hosts can access DMZ only, not Intranet
- DMZ hosts can access Internet only
- Advantages?
  - If a service gets compromised in DMZ it cannot affect internal hosts



Packet Filters Contd.

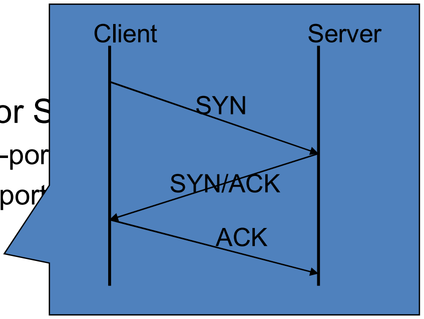
- Example filters
  - Block all packets from outside except for SMTP servers
  - Block all traffic to a list of domains
  - Block all connections from a specified domain

Example Firewall Rules

- Stateless packet filtering firewall
- Rule → (Condition, Action)
- Rules are processed in top-down order
  - If a condition satisfied – action is taken

Sample Firewall Rule

- Allow SSH from external hosts to internal hosts
  - Two rules
    - Inbound and outbound
  - How to know a packet is for S
    - Inbound: src-port>1023, dst-por
    - Outbound: src-port=22, dst-port
    - Protocol=TCP
  - Ack Set?
  - Problems?



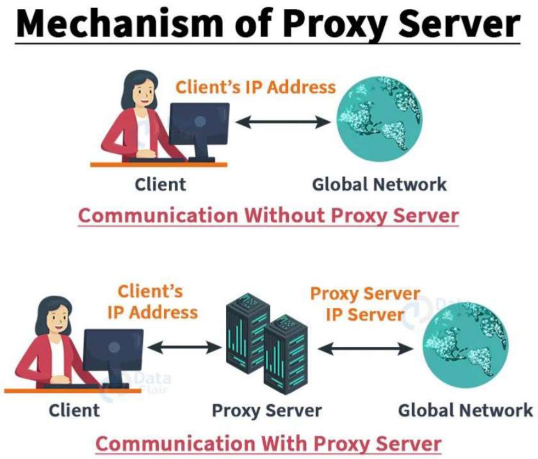
Rule	Dir	Src Addr	Src Port	Dst Addr	Dst Port	Proto	Ack Set?	Action
SSH-1	In	Ext	> 1023	Int	22	TCP	Any	Allow
SSH-2	Out	Int	22	Ext	> 1023	TCP	Yes	Alow

proxy server

- A proxy server is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network. It is a server, referred to as an “intermediary” because it goes between end-users and the web pages they visit online.

Alternatives

- Proxy Firewalls
  - Two connections instead of one
  - Either at transport level
    - SOCKS proxy
  - Or at application level
    - HTTP proxy
- Requires applications (or dynamically linked libraries) to be modified to use the proxy



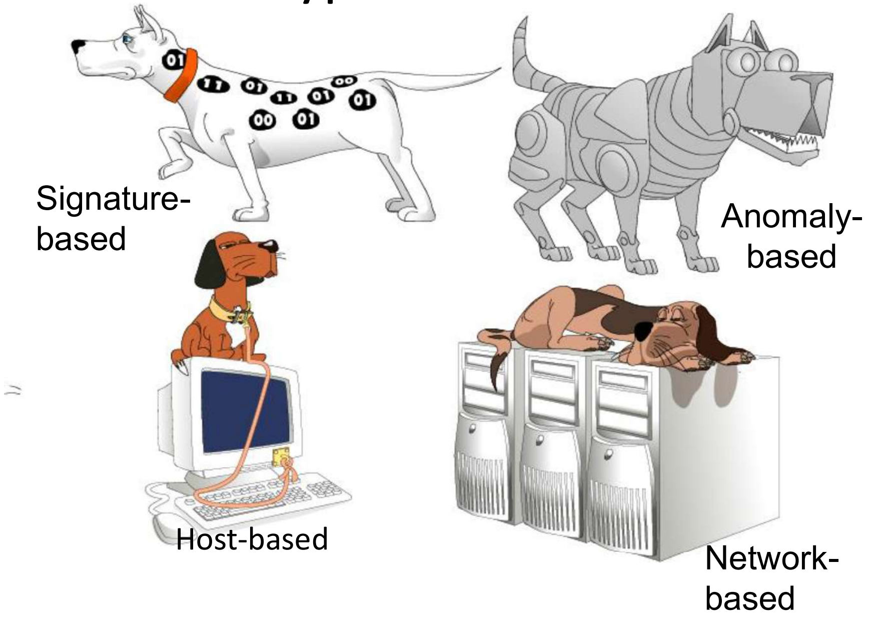
Proxy Firewall

- Data Available
  - Application level information
  - User information
- Advantages?
  - Better policy enforcement
  - Better logging
  - Fail closed
- Disadvantages?
  - Doesn’t perform as well
  - One proxy for each application
  - Client modification

Intrusion Detection Systems

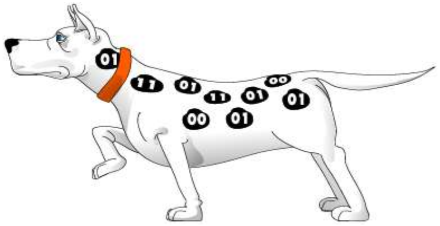
- Firewalls allow traffic only to legitimate hosts and services
- Traffic to the legitimate hosts/services can have attacks
  - CodeReds on IIS
- Solution?
  - Intrusion Detection Systems
  - Monitor data and behavior
  - Report when identify attacks

Types of IDS



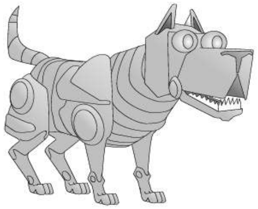
Signature-based IDS

- Characteristics
  - Uses known pattern matching to signify attack
- Advantages?
  - Widely available
  - Fairly fast
  - Easy to implement
  - Easy to update
- Disadvantages?
  - Cannot detect attacks for which it has no signature



Anomaly-based IDS

- Characteristics
  - Uses statistical model or machine learning engine to characterize normal usage behaviors
  - Recognizes departures from normal as potential intrusions
- Advantages?
  - Can detect attempts to exploit new and unforeseen vulnerabilities
  - Can recognize authorized usage that falls outside the normal pattern
- Disadvantages?
  - Generally slower, more resource intensive compared to signature-based IDS
  - Greater complexity, difficult to configure
  - Higher percentages of false alerts



IP Fragmentation Attack

- IP fragmentation attacks is a type of cyber attack that exploits how IP packets are fragmented and reassembled to evade security controls and launch attacks.
- Attackers manipulate fragmented packet parameters like offsets and sizes to trigger vulnerabilities or bypass firewall rules.

Network-based IDS

- Characteristics
  - NIDS examine raw packets in the network passively and triggers alerts
- Advantages?
  - Easy deployment
  - Unobtrusive
  - Difficult to evade if done at low level of network operation
- Disadvantages?
  - Fail Open
  - Different hosts process packets differently
  - NIDS needs to create traffic seen at the end host
  - Need to have the complete network topology and complete host behavior

How IP Fragmentation Works

- IP fragmentation occurs when an IP packet exceeds the Maximum Transmission Unit (MTU) size for a network path. Routers must split the large packet into smaller fragments to be transmitted.
- The router divides the IP packet into fragments starting with offset 0. A header is added to each fragment containing:
- Identification – Unique ID matching all fragments

- Flags – Indicates first, middle, or last fragment
- Offset – The fragment position within the original packet
- The destination host reassembles the fragments using the identification and offset fields. Fragments arrive out-of-order, so buffering allows reordering before reassembly.

Types of Fragmentation Attacks

- **Teardrop Attack**
- Sends offset and size fields designed to overwrite the header during reassembly. This has the ability to crash many older systems.
- **Bonk Attack**
- Uses a large fragment designed to crash systems attempting to allocate huge buffers during reassembly.

- **Fragrouter Tool**
- Performs automated attacks by generating malicious traffic patterns and packet values.
- **Jolt2 Attack**
- Sends invalid fragmentation flags triggering crashes in some Windows TCP/IP implementations.
- **SMS of Death**
- Sends specially crafted ping packets that get fragmented, aiming to disable iPhone devices.

TCP/IP ATTACKS

- **TCP "SYN" attacks**: This attack is caused by the three-way handshake mechanism used between host and the server to setup connection. A server has limited resources. Once it responds to a SYN request using SYN ACK it sets aside resources for this connection and listens for ACK from client. If the attacker sends multiple SYN within very short interval then the server will exhaust its resources. The attacker does not respond to SYN ACK sent by the server and the connections are left half opened. This ways server is unable to respond to further connection request because of exhaustion of resources and denial of service takes place

IP Spoofing

- IP address spoofing involves maliciously creating TCP/IP packets using other IP address as source address with the aim to either conceal own identity or impersonate the identity of the owner of the IP address used [10]. Routers use the IP address of the destination and forward the packet to it. The recipient uses the IP address of the source to reply to the packet. If the source address is spoofed, the recipient will reply to the spoofed address.

Connection Hijacking

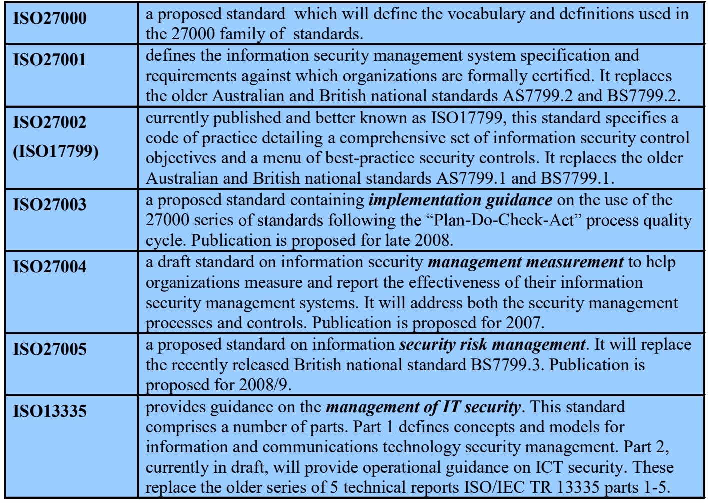
- Authentication between two hosts takes place during the initial stages of the connection setup. Attacker can take advantage of this by sending a reset to the client and destroing the connection for the client and then the attacker spoofs the client and continues session with server using spoofed source address The other way of session hijacking is exploiting authenticated machine by stealing the cookies stored on that machine or stealing cookies by sniffing the unencrypted network traffic.

Routing Information Protocol (RIP) Attacks

- The attacker can forge RIP routing updates to advertise the least cost path to the target node. This will cause RIP to route all packets to the target node through attacker as he is considered the nearest to target node [15]. The attacker can use this to launch any attack on the target node.

IT Security Management and Risk Assessment

ISO 27000 Security Standards

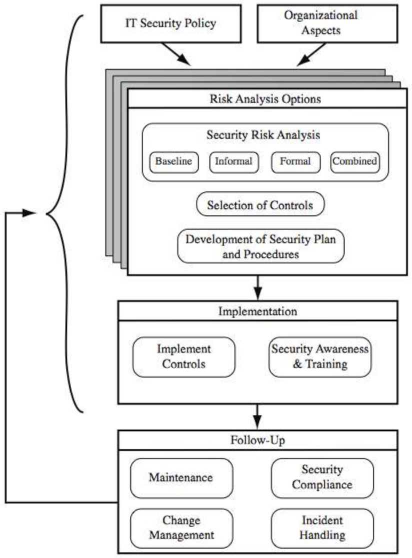


ISO27000	a proposed standard which will define the vocabulary and definitions used in the 27000 family of standards.
ISO27001	defines the information security management system specification and requirements against which organizations are formally certified. It replaces the older Australian and British national standards AS7799.2 and BS7799.2.
ISO27002 **(ISO17799)**	currently published and better known as ISO17799, this standard specifies a code of practice detailing a comprehensive set of information security control objectives and a menu of best-practice security controls. It replaces the older Australian and British national standards AS7799.1 and BS7799.1.
ISO27003	a proposed standard containing ***implementation guidance*** on the use of the 27000 series of standards following the "Plan-Do-Check-Act" process quality cycle. Publication is proposed for late 2008.
ISO27004	a draft standard on information security ***management measurement*** to help organizations measure and report the effectiveness of their information security management systems. It will address both the security management processes and controls. Publication is proposed for 2007.
ISO27005	a proposed standard on information ***security risk management***. It will replace the recently released British national standard BS7799.3. Publication is proposed for 2008/9.
ISO13335	provides guidance on the ***management of IT security***. This standard comprises a number of parts. Part 1 defines concepts and models for information and communications technology security management. Part 2, currently in draft, will provide operational guidance on ICT security. These replace the older series of 5 technical reports ISO/IEC TR 13335 parts 1-5.

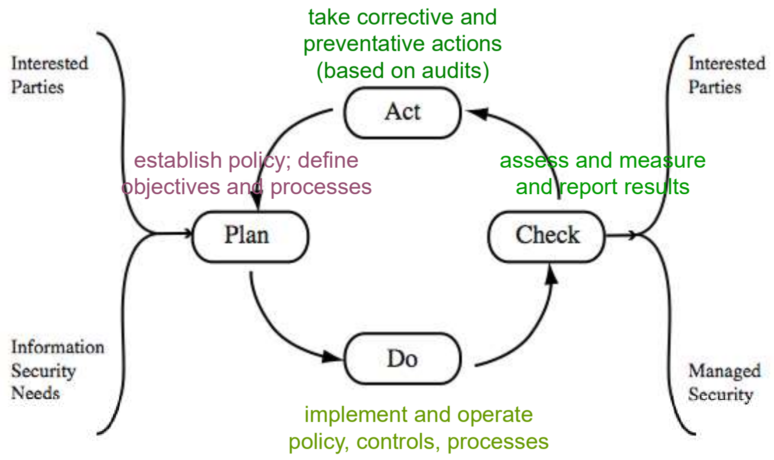
IT Security Management

- **IT Security Management:** a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability. IT security management functions include:
  - organizational IT security objectives, strategies and policies
  - determining organizational IT security requirements
  - identifying and analyzing security threats to IT assets
  - identifying and analyzing risks
  - specifying appropriate safeguards
  - monitoring the implementation and operation of safeguards
  - developing and implement a security awareness program
  - detecting and reacting to incidents

IT Security Management Process



Plan - Do - Check – Act (Deming Cycle)



Security Policy: Topics to Cover

- needs to address:
  - scope and purpose including relation of objectives to business, legal, regulatory requirements
  - IT security requirements
  - assignment of responsibilities
  - risk management approach
  - security awareness and training
  - general personnel issues and any legal sanctions
  - integration of security into systems development
  - information classification scheme
  - contingency and business continuity planning
  - incident detection and handling processes
  - how when policy reviewed, and change control to it

Organizational Context and Security Policy

- first examine organization’s IT security:
  - objectives - wanted IT security outcomes
  - strategies - how to meet objectives
  - policies - identify what needs to be done
- maintained and updated regularly
  - using periodic security reviews
  - reflect changing technical/risk environments

Management Support

- IT security policy must be supported by senior management
- need IT security officer
  - to provide consistent overall supervision
  - manage process
  - handle incidents
- large organizations needs IT security officers on major projects/teams
  - manage process within their areas

Security Risk Assessment

- critical component of process
  - else may have vulnerabilities or waste money
- ideally examine every asset vs risk
  - not feasible in practice
- choose one of possible alternatives based on organization’s resources and risk profile
  - baseline
  - informal
  - formal
  - combined

Informal Approach

- conduct informal, pragmatic risk analysis on organization’s IT systems
- exploits knowledge and expertise of analyst
- fairly quick and cheap
- does address some org specific issues
- some risks may be incorrectly assessed
- skewed by analysts views, varies over time
- suitable for small to medium sized orgs

Baseline Approach

- use “industry best practice”
  - easy, cheap, can be replicated
  - but gives no special consideration to org
  - may give too much or too little security
- implement safeguards against most common threats
- baseline recommendations and checklist documents available from various bodies
- alone only suitable for small organizations

Detailed Risk Analysis

- most comprehensive alternative
- assess using formal structured process
  - with a number of stages
  - identify likelihood of risk and consequences
  - hence have confidence controls appropriate
- costly and slow, requires expert analysts
- may be a legal requirement to use
- suitable for large organizations with IT systems critical to their business objectives

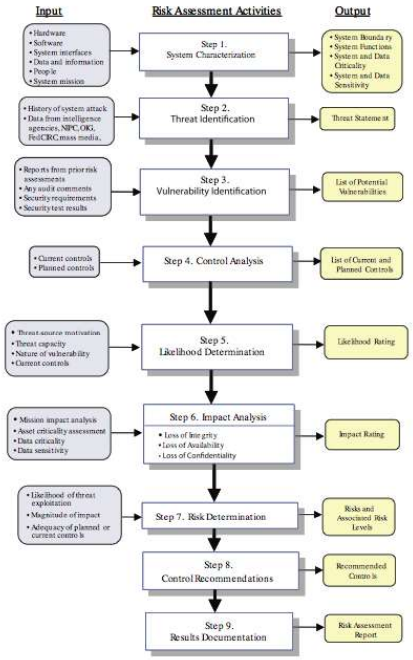
Combined Approach

- combines elements of other approaches
  - initial baseline on all systems
  - informal analysis to identify critical risks
  - formal assessment on these systems
  - iterated and extended over time
- better use of time and money resources
- better security earlier that evolves
- may miss some risks early
- recommended alternative for most orgs

Establish Context

- determine broad risk exposure of org
  - related to wider political/social environment
  - legal and regulatory constraints
- specify organization’s risk *appetite*
- set boundaries of risk assessment
  - partly on risk assessment approach used
- decide on risk assessment criteria used

Detailed Risk Analysis Process



Asset Identification

- identify assets
  - “anything which needs to be protected”
  - of value to organization to meet its objectives
  - tangible or intangible
  - in practice try to identify significant assets
- draw on expertise of people in relevant areas of organization to identify key assets
  - identify and interview such personnel
  - see checklists in various standards

Terminology

asset: anything that has value to the organization

threat: a potential cause of an unwanted incident which may result in harm to a system or organization

vulnerability: a weakness in an asset or group of assets which can be exploited by a threat

risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

Threat Sources

- threats may be
  - natural “acts of god”
  - man-made and either accidental or deliberate
- should consider human attackers
  - motivation
  - capability
  - resources
  - probability of attack
  - deterrence
- any previous history of attack on org

Threat Identification

- to identify threats or risks to assets asK
  - who or what could cause it harm?
  - how could this occur?
- threats are anything that hinders or prevents an asset providing appropriate levels of the key security services:
  - confidentiality, integrity, availability, accountability, authenticity and reliability
- assets may have multiple threats

Threat Identification

- depends on risk assessors experience
- uses variety of sources
  - natural threat chance from insurance stats
  - lists of potential threats in standards, IT security surveys, info from governments
  - tailored to organization’s environment
  - and any vulnerabilities in its IT systems

Vulnerability Identification

- identify exploitable flaws or weaknesses in organization’s IT systems or processes
- hence determine applicability and significance of threat to organization
- need combination of threat and vulnerability to create a risk to an asset
- again can use lists of potential vulnerabilities in standards etc

Analyze Risks

- specify likelihood of occurrence of each identified threat to asset given existing controls
  - management, operational, technical processes and procedures to reduce exposure of org to some risks
- specify consequence should threat occur
- hence derive overall risk rating for each threat

  risk = probability threat occurs x cost to organization
- in practice very hard to determine exactly
- use qualitative not quantitative, ratings for each
- aim to order resulting risks in order to treat them

Determine Likelihood

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may deemed as “unlucky” or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

Determine Consequence

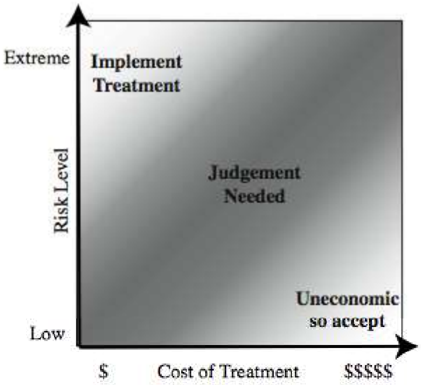
Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week, but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last ***up to 2 weeks*** and generally requires management intervention. Will have ongoing compliance costs to overcome.
4	**Major**	Ongoing systemic security breach. Impact will likely last ***4-8 weeks*** and require significant management intervention and resources to overcome, and compliance costs are expected to be substantial. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for ***3 months or more*** and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable.

Determine Resultant Risk

	Consequences					
Likelihood	Doomsday	Catastrophic	Major	Moderate	Minor	Insignificant
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed r esearch and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Risk Treatment



Document in Risk Register and Evaluate Risks

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet Router	Outside Hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of Data Center	Accidental Fire or Flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Risk Treatment Alternatives

- **risk acceptance**: *accept risk (perhaps because of excessive cost of risk treatment)*
- **risk avoidance**: *do not proceed with the activity that causes the risk (loss of convenience)*
- **risk transfer**: buy insurance; outsource
- **reduce consequence**: *modify the uses of an asset to reduce risk impact (e.g., offsite backup)*
- **reduce likelihood**: *implement suitable controls*

Assets

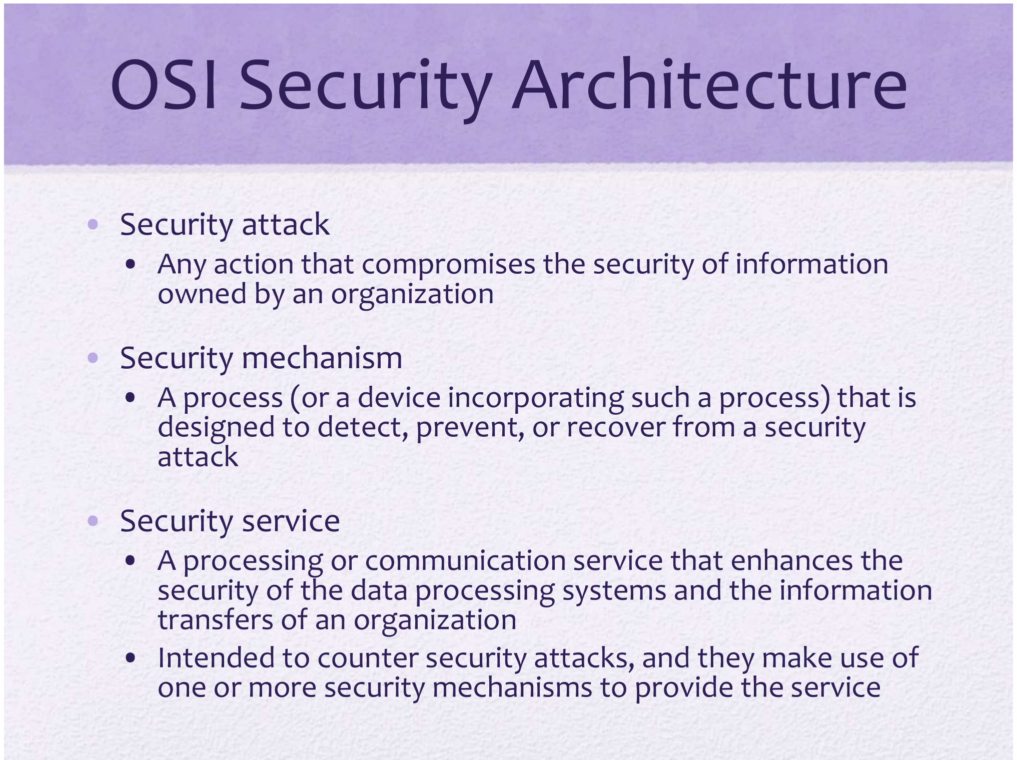
- reliability and integrity of SCADA nodes and net
- integrity of stored file and database information
- availability, integrity of financial system
- availability, integrity of procurement system
- availability, integrity of maintenance/production system
- availability, integrity and confidentiality of mail services

Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	layered firewalls & servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	firewall, policies	Possible	Major	Extreme	2
Availability and integrity of Financial System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	3
Availability and integrity of Procurement System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	4
Availability and integrity of Maintenance/ Production System	Attacks/errors affecting system	firewall, policies	Possible	Minor	Medium	5
Availability, integrity and confidentiality of mail services	Attacks/errors affecting system	firewall, ext mail gateway	Almost Certain	Minor	High	6

Threats & Vulnerabilities

- unauthorized modification of control system
- corruption, theft, loss of info
- attacks/errors affecting procurement system
- attacks/errors affecting financial system
- attacks/errors affecting mail system
- attacks/errors maintenance/production affecting system



OSI Security Architecture

- Security attack
  - Any action that compromises the security of information owned by an organization
- Security mechanism
  - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack
- Security service
  - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization
  - Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

Table 1.1
Threats and Attacks (RFC 4949)

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted

- Two types of passive attacks are:
  - The release of message contents
  - Traffic analysis

Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*
- A *passive attack* attempts to learn or make use of information from the system but does not affect system resources
- An *active attack* attempts to alter system resources or affect their operation

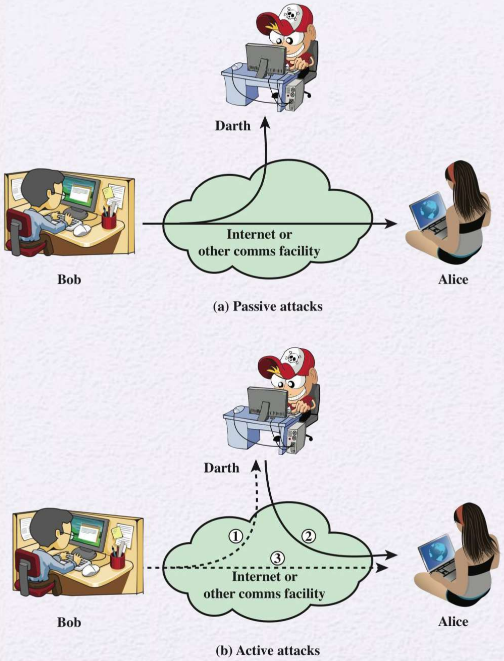


Figure 1.1 Security Attacks

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

Masquerade	• Takes place when one entity pretends to be a different entity • Usually includes one of the other forms of active attack
Replay	• Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
Modification of messages	• Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect
Denial of service	• Prevents or inhibits the normal use or management of communications facilities

Security Services

- Defined by X.800 as:
  - A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers
- Defined by RFC 4949 as:
  - A processing or communication service provided by a system to give a specific kind of protection to system resources

Authentication

- Concerned with assuring that a communication is authentic
  - In the case of a single message, assures the recipient that the message is from the source that it claims to be from
  - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:

- Peer entity authentication
- Data origin authentication

X.800 Service Categories

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation

Access Control

- The ability to limit and control the access to host systems and applications via communications links
- To achieve this, each entity trying to gain access must first be indentified, or authenticated, so that access rights can be tailored to the individual

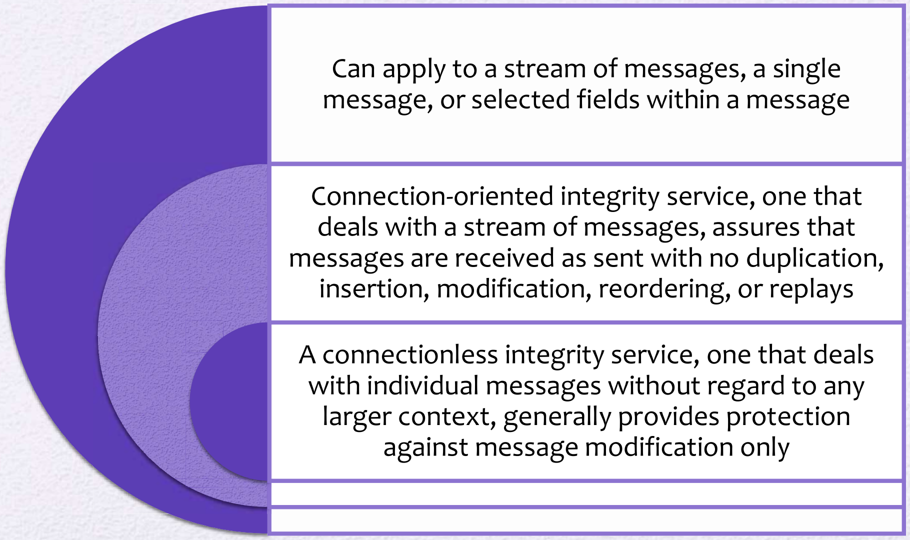
Data Confidentiality

- The protection of transmitted data from passive attacks
  - Broadest service protects all user data transmitted between two users over a period of time
  - Narrower forms of service includes the protection of a single message or even specific fields within a message
- The protection of traffic flow from analysis
  - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

Nonrepudiation

- Prevents either sender or receiver from denying a transmitted message
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message

Data Integrity

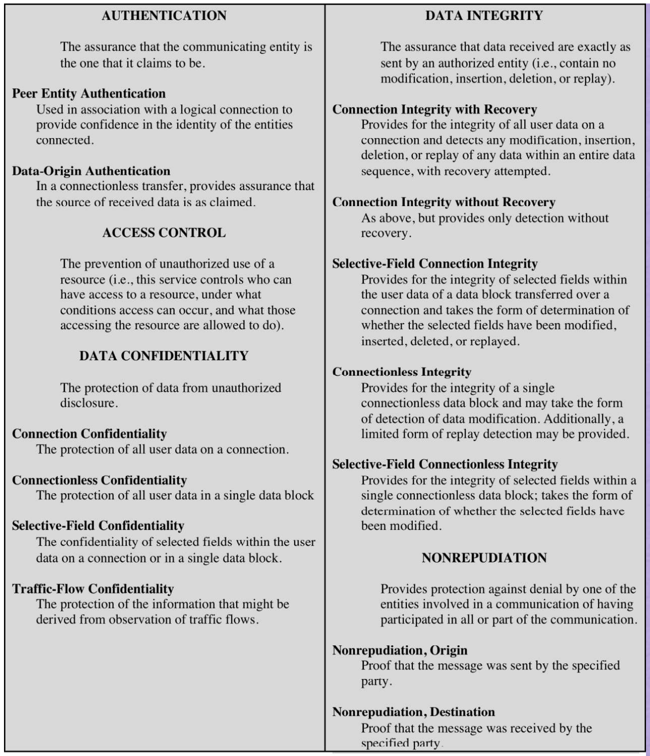


Can apply to a stream of messages, a single message, or selected fields within a message

Connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays

A connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only

Security Services (X.800)



AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

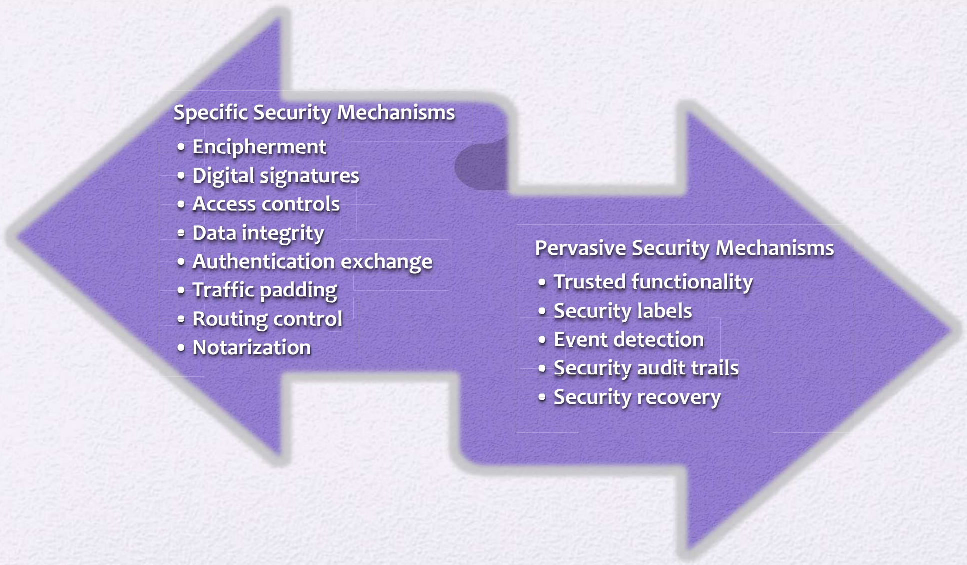
NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Security Mechanisms (X.800)

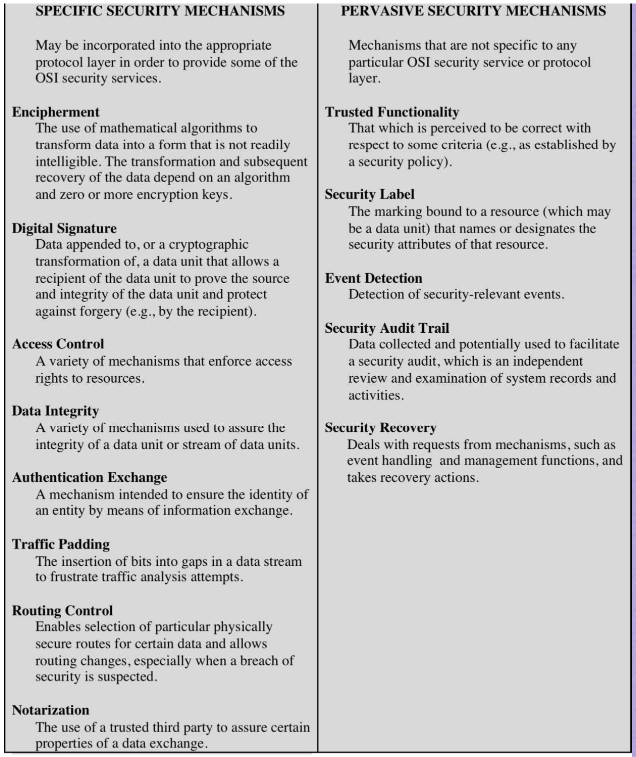


Specific Security Mechanisms

- Encipherment
- Digital signatures
- Access controls
- Data integrity
- Authentication exchange
- Traffic padding
- Routing control
- Notarization

Pervasive Security Mechanisms

- Trusted functionality
- Security labels
- Event detection
- Security audit trails
- Security recovery



SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment
The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature
Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

Access Control
A variety of mechanisms that enforce access rights to resources.

Data Integrity
A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange
A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding
The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control
Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization
The use of a trusted third party to assure certain properties of a data exchange.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality
That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label
The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection
Detection of security-relevant events.

Security Audit Trail
Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

Security Recovery
Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Table 1.3

Security Mechanisms (X.800)

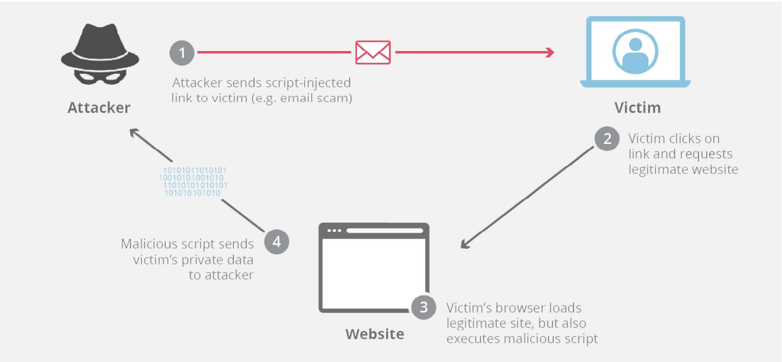
Web Security

Cross-site scripting

- Cross-site scripting (XSS) is an exploit where the attacker attaches code onto a legitimate website that will execute when the victim loads the website. That malicious code can be inserted in several ways. Most popularly, it is either added to the end of a url or posted directly onto a page that displays user-generated content. In more technical terms, cross-site scripting is a client-side code injection attack.

Web Application Security

- Web application security is the practice of protecting websites, applications, and APIs from attacks.
- It is a broad discipline, but its ultimate aims are keeping web applications functioning smoothly and protecting business from cyber vandalism, data theft, unethical competition, and other negative consequences.


Attacker
1
Attacker sends script-injected link to victim (e.g. email scam)
Victim
2
Victim clicks on link and requests legitimate website
3
Victim's browser loads legitimate site, but also executes malicious script
Website
4
Malicious script sends victim's private data to attacker

How to prevent cross-site scripting

- If possible, avoiding HTML in inputs - One very effective way to avoid persistent cross-site scripting attacks is to prevent users from posting HTML into form inputs. There are other options which let users create rich content without the use of HTML, such as markdown and WYSIWYG editors.
- Validating inputs - Validation means implementing rules that prevent a user from posting data into a form that doesn't meet certain criteria. For example, an input that asks for the user's "Last Name" should have validation rules that only let the user submit data consisting of alphanumeric characters. Validation rules can also be set to reject any tags or characters commonly used in cross-site scripting, such as "<script>" tags.
- Sanitizing data - Sanitizing data is similar to validation, but it happens after the data has already been posted to the web server, yet still before it is displayed to another user. There are several online tools that can sanitize HTML and filter out any malicious code injections.
- Taking cookie security measures - Web applications can also set special rules for their cookie handling that can mitigate cookie-theft via cross-site scripting attacks. Cookies can be tied to particular IP addresses so that cross-site scripting attackers cannot access them. Additionally, rules can be created to block JavaScript from accessing cookies altogether.

Normal SQL query:

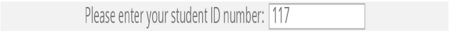
In this normal SQL query, the studentId string is passed into a SQL statement. The goal is to look through the list of students for a student that matches the studentId entered. Once found, that student's record will be returned. Put simply, the command says "go find this user and give me their data".

The code might look something like this:

```
studentId = getRequestString("studentId");

lookupStudent  = "SELECT * FROM students WHERE studentId = " + studentId
```

If a student enters a student ID of 117 inside a webpage form labelled 'Please enter your student ID number'



Please enter your student ID number: 117

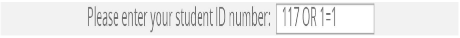
the resulting SQL query will look like:

```
SELECT * FROM students WHERE studentId = 117;
```

This command will return the record for the particular student with a studentId, which is what the developer who wrote the API expects to have happen.

SQL Injection query:

In this example, an attacker instead enters a SQL command or conditional logic into the input field, he enters a student ID number of:



Please enter your student ID number: 117 OR 1=1

Where normally the query would search the database table for the matching ID, it now looks for an ID or tests to see if 1 is equal to 1. As you might expect, the statement is always true for every student in the column, and as a result, the database will return all data from the students table back to the attacker making the query.

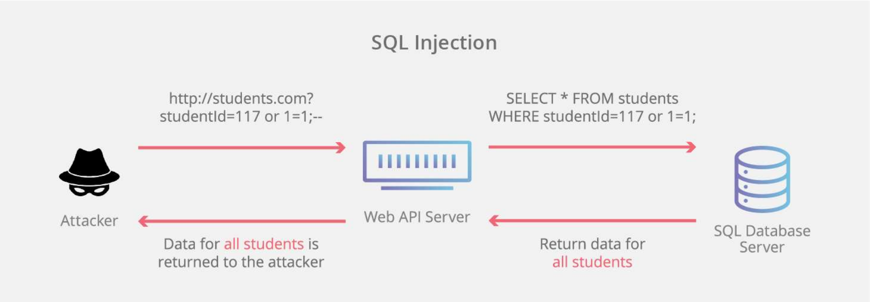
```
SELECT * FROM students WHERE studentId = 117 OR 1=1;
```

SQL injection

- Structured Query Language (SQL*) Injection is a code injection technique used to modify or retrieve data from SQL databases. By inserting specialized SQL statements into an entry field, an attacker is able to execute commands that allow for the retrieval of data from the database, the destruction of sensitive data, or other manipulative behaviors.

Denial-of-service attack

- A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.



Important web application security strategies

- DDoS mitigation**:** DDoS mitigation services sit between a server and the public Internet, using specialized filtration and extremely high bandwidth capacity to prevent surges of malicious traffic from overwhelming the server. These services are important because many modern DDoS attacks deliver enough malicious traffic to overwhelm even the most resilient servers.
- Web Application Firewall **(WAF):** Which filter out traffic known or suspected to be taking advantage of web application vulnerabilities. WAFs are important because new vulnerabilities emerge too quickly and quietly for nearly all organizations to catch on their own.
- **API gateways:** Which help identify overlooked 'shadow APIs,' and block traffic known or suspected to target API vulnerabilities. They also help manage and monitor API traffic. (Learn more about API security.)
- DNSSEC**:** A protocol which guarantees a web application's DNS traffic is safely routed to the correct servers, so users are are not intercepted by an on-path attacker.
- Encryption certificate **management:** In which a third party manages key elements of the SSL/TLS encryption process, such as generating private keys, renewing certificates, and revoking certificates due to vulnerabilities. This removes the risk of those elements going overlooked and exposing private traffic.

Buffer overflow

- Buffer overflow is an anomaly that occurs when software writing data to a defined space in memory known as a buffer. Overflowing the buffer's capacity results in adjacent memory locations being overwritten with data. This behavior can be exploited to inject malicious code into memory, potentially creating a vulnerability in the targeted machine.

TCP/IP Security

- TCP is used for organizing data in a way that ensures the secure transmission between the server and client. It guarantees the integrity of data sent over the network, regardless of the amount. For this reason, it is used to transmit data from other higher-level protocols that require all transmitted data to arrive.

IP Security (IPSec)

- Support for IPsec, as the architecture is called, is optional in IPv4 but mandatory in IPv6.
- IPsec is really a framework (as opposed to a single protocol or system) for providing all the security services discussed throughout this chapter.
- IPsec provides three degrees of freedom.
  - First, it is highly modular, allowing users (or more likely, system administrators) to select from a variety of cryptographic algorithms and specialized security protocols.
  - Second, IPsec allows users to select from a large menu of security properties, including access control, integrity, authentication, originality, and confidentiality.
  - Third, IPsec can be used to protect “narrow” streams (e.g., packets belonging to a particular TCP connection being sent between a pair of hosts) or “wide” streams (e.g., all packets flowing between a pair of routers).

- The abstraction that binds these two pieces together is the security association (SA).
- An SA is a simplex (one-way) connection with one or more of the available security properties.
- Securing a bidirectional communication between a pair of hosts—corresponding to a TCP connection, for example—requires two SAs, one in each direction.
- Although IP is a connectionless protocol, security depends on connection state information such as keys and sequence numbers.
- When created, an SA is assigned an ID number called a security parameters index (SPI) by the receiving machine

- When viewed from a high level, IPsec consists of two parts.
- The first part is a pair of protocols that implement the available security services.
- They are the Authentication Header (AH), which provides access control, connectionless message integrity, authentication, and antireplay protection, and the Encapsulating Security Payload (ESP), which supports these same services, plus confidentiality.
- AH is rarely used so we focus on ESP here.
- The second part is support for key management, which fits under an umbrella protocol known as ISAKMP:
- Internet Security Association and Key Management Protocol.

- IPsec supports a tunnel mode as well as the more straightforward transport mode.
- Each SA operates in one or the other mode.
- In a transport mode SA, ESP’s payload data is simply a message for a higher layer such as UDP or TCP.
- In this mode, IPsec acts as an intermediate protocol layer, much like SSL/TLS does between TCP and a higher layer.
- When an ESP message is received, its payload is passed to the higher level protocol.
- In a tunnel mode SA, however, ESP’s payload data is itself an IP packet

Virtual Private Network (VPN)

- VPNs are private data networks over public network – usually the Internet.
- VPNs extend corporate networks to remote offices, mobile users, telecommuters and other extranet partners.
- VPNs use advanced encryption and ‘tunneling’ technology to establish secure, end-to-end private network connections over Internet.

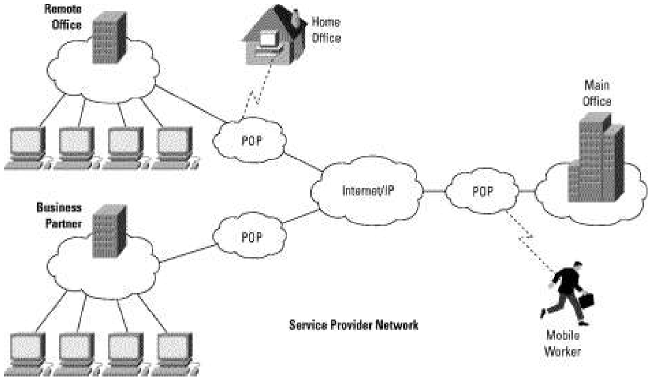
VPN Solutions

Remote access VPNs establish secure, encrypted connections between mobile or remote users and their corporate networks via a third-party network, such as a Internet Service Provider(ISP)

- VPN client – software, hardware as well as router, or firewall based solutions available.

- Reduced cost of long distance access calls and internal equipment inventory

A typical VPN



VPN Solutions

Site-to-Site VPNs are an alternative WAN infrastructure that used to connect branch offices, home offices, or business partners' sites to all or portions of a company's network.

- Intranet VPNs provide full access to company’s network

- Extranet VPNS provide business partners with limited access to a company’s network

VPN Technology

- *Trusted VPNs* – companies lease circuits from communication providers and use them in the same manner they use physical cables in a private LAN

- Communication provider is ‘t*rusted*’ for data integrity and security.

- Used before Internet became universal

VPN Technology

- *Hybrid VPNs* – A secure VPN is created as part of the trusted VPN thus creating a ‘hybrid’ VPN. Secure part of the VPN is usually administered by customer (using VPN equipments).
- Secure VPNs that are administered by ISPs are called *provider-provisioned VPNs*.

VPN Technology

- *Secure VPNs* use Internet as a corporate communication medium. Data is encrypted before sending, moved over to Internet, and then decrypted at the receiving end.

- Encryption creates a security ‘tunnel’ that can’t be attacked

- More desirable than Trusted VPNs

Web Service Security

- What is web service security?

WS- Security is flexible and is designed to be used as the basis for the construction of a wide variety of security models including PKI, Kerberos, and SSL.

- What are the goals of web service security?

The goal of WS-Security is to enable applications to construct secure SOAP message exchange.

- What are the requirements of web service security?
  - Multiple security tokens for authentication or authorization
  - Multiple trust domains
  - Multiple encryption technologies
  - End-to-end message-level security and not just transport-level security

Web Services Security Model Terminology

➢Web service

Broadly applicable to a wide variety of network based application topologies.

➢Security Token

Define a security token as a representation of security-related information (e.g.X.509 certificate, Kerberos tickes and authenticators, mobile device security from SIM cards, username, etc.)

➢Signed Security Token

It contains a set of related claims cryptographically endorsed by an issuer.

Web Service Security Model Terminology

➢Web Service Endpoint Policy

Web services have complete flexibility in specifying the claims they require in order to process messages.

➢Claim Requirements

Whole messages or elements of messages,to all actions of a given type or to actions only under certain circumstances.

➢Intermediaries

It perform actions such as routing the message or even modifying the message.

➢Actor

An intermediary or endpoint which is identified by a URI and which processes a SOAP message. SOAP stands for Simple Object Access Protocol. It is a XML-based protocol for accessing web services. SOAP is a W3C recommendation for communication between two applications. SOAP is XML based protocol. It is platform independent and language independent.

Web Services Security Model Terminology

➢Claims

A statement about a subject either by the subject or by an relying party that associates the subject with the claim.

➢Subject

The subject of the security token is a principal about which the claims expressed in the security token apply.

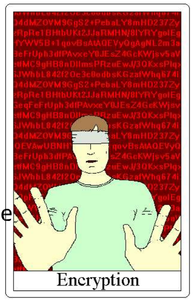
➢Proof-of-Possession

To be information used in the process of proving ownership of a security tiken or set of claims.

XML Encryption

- **Purpose**:
  - Allow users to encrypt and decrypt data
  - Provide confidentiality in transport *and* in storage
- **Features**:
  - Defined vocabulary for ciphers and encryption information
  - Both XML and non-XML content can be encrypted
  - Encryption granularity – element content
  - Encrypted infromation stays in XML form.
  - Compatible with signatures
  - Supports for many encryption algorithms

XML Encryption



Key Concepts:

- Encrypted elements are replaced by an <Encrypte element
- <EncryptedData> element contains:
  - A Type attribute – indicates the type of the information encrypted
  - Information about the algorithm used for encryption
  - An <EncryptedKey> element
  - <CipherData> A Reference to the cipher, or the cipher itself
- <EncryptedKey> - used for encrypting secret keys in symmetric key encryption

```
<?xml version='1.0'?>
<PaymentInfo xmlns='http://example.org/paymentv2'>
  <Name>John Smith</Name>
  <CreditCard Limit='5,000' Currency='USD'>
    <Number>
      <EncryptedData
xmlns='http://www.w3.org/2001/04/xmlenc#‘

Type='http://www.w3.org/2001/04/xmlenc#Content'>
        <CipherData>
          <CipherValue>A23B45C56</CipherValue>
        </CipherData>
      </EncryptedData>
    </Number>
    <Issuer>Example Bank</Issuer>
    <Expiration>04/02</Expiration>
  </CreditCard>
</PaymentInfo>
```

Electronic Mail Security

Email Security

- email is one of the most widely used and regarded network services
- currently message contents are not secure
  - may be inspected either in transit
  - or by suitably privileged users on destination system

Email Security Enhancements

- confidentiality
  - protection from disclosure
- authentication
  - of sender of message
- message integrity
  - protection from modification
- non-repudiation of origin
  - protection from denial by sender

Pretty Good Privacy (PGP)

- widely used de facto secure email
- developed by Phil Zimmermann
- selected best available crypto algs to use
- integrated into a single program
- available on Unix, PC, Macintosh and Amiga systems
- originally free, now have commercial versions available also

PGP Operation – Authentication

1. sender creates a message
2. SHA-1 used to generate 160-bit hash code of message
3. hash code is encrypted with RSA using the sender's private key, and result is attached to message
4. receiver uses RSA or DSS with sender's public key to decrypt and recover hash code
5. receiver generates new hash code for message and compares with decrypted hash code, if match, message is accepted as authentic

PGP Operation – Confidentiality

1. sender generates message and random 128-bit number to be used as session key for this message only
2. message is encrypted, using CAST-128 / IDEA/3DES with session key
3. session key is encrypted using RSA with recipient's public key, then attached to message
4. receiver uses RSA with its private key to decrypt and recover session key
5. session key is used to decrypt message

PGP Operation – Confidentiality & Authentication

- uses both services on same message
  - create signature & attach to message
  - encrypt both message & signature
  - attach RSA encrypted session key

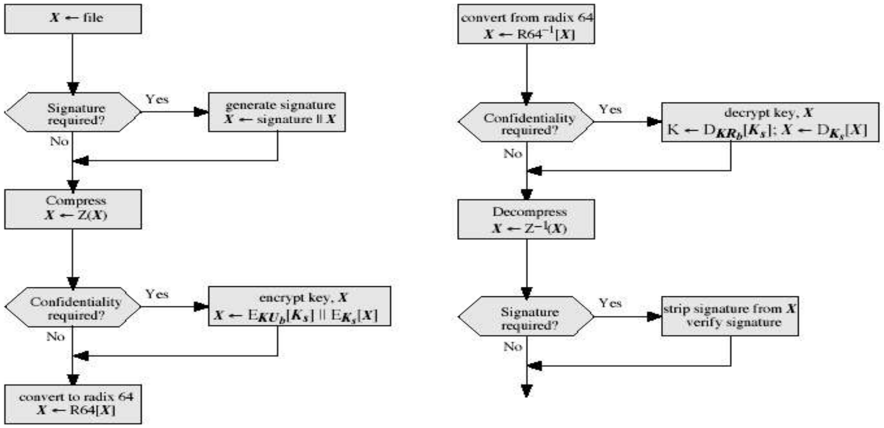
PGP Operation – Compression

- by default PGP compresses message after signing but before encrypting
  - so can store uncompressed message & signature for later verification
  - & because compression is non deterministic
- uses ZIP compression algorithm

PGP Operation – Email Compatibility

- when using PGP will have binary data to send (encrypted message etc)
- however email was designed only for text
- hence PGP must encode raw binary data into printable ASCII characters
- uses radix-64 algorithm
  - maps 3 bytes to 4 printable chars
  - also appends a CRC
- PGP also segments messages if too big

PGP Operation – Summary



$X \leftarrow$ file
Signature required?
Yes
generate signature $X \leftarrow$ signature $\|$ X
No
Compress $X \leftarrow Z(X)$
Confidentiality required?
Yes
encrypt key, X $X \leftarrow E_{KU_b}[K_s] \| E_{K_s}[X]$
No
convert to radix 64 $X \leftarrow R64[X]$
convert from radix 64 $X \leftarrow R64^{-1}[X]$
Confidentiality required?
Yes
decrypt key, X $K \leftarrow D_{KR_b}[K_s]$; $X \leftarrow D_{K_s}[X]$
No
Decompress $X \leftarrow Z^{-1}(X)$
Signature required?
Yes
strip signature from X verify signature
No

(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

PGP Session Keys

- need a session key for each message
  - of varying sizes: 56-bit DES, 128-bit CAST or IDEA, 168-bit Triple-DES
- generated using ANSI X12.17 mode
- uses random inputs taken from previous uses and from keystroke timing of user

PGP Public & Private Keys

- since many public/private keys may be in use, need to identify which is actually used to encrypt session key in a message
  - could send full public-key with every message
  - but this is inefficient
- rather use a key identifier based on key
  - is least significant 64-bits of the key
  - will very likely be unique
- also use key ID in signatures

PGP Key Rings

- each PGP user has a pair of keyrings:
  - public-key ring contains all the public-keys of other PGP users known to this user, indexed by key ID
  - private-key ring contains the public/private key pair(s) for this user, indexed by key ID & encrypted keyed from a hashed passphrase

PGP Key Management

- rather than relying on certificate authorities
- in PGP every user is own CA
  - can sign keys for users they know directly
- forms a “web of trust”
  - trust keys have signed
  - can trust keys others have signed if have a chain of signatures to them
- key ring includes trust indicators
- users can also revoke their keys

S/MIME (Secure/Multipurpose Internet Mail Extensions)

- security enhancement to MIME email
  - original Internet RFC822 email was text only
  - MIME provided support for varying content types and multi-part messages
  - with encoding of binary data to textual form
  - S/MIME added security enhancements
- have S/MIME support in various modern mail agents: MS Outlook, Netscape etc

S/MIME Functions

- enveloped data
  - encrypted content and associated keys
- signed data
  - encoded message + signed digest
- clear-signed data
  - cleartext message + encoded signed digest
- signed & enveloped data
  - nesting of signed & encrypted entities

S/MIME Cryptographic Algorithms

- hash functions: SHA-1 & MD5
- digital signatures: DSS & RSA
- session key encryption: ElGamal & RSA
- message encryption: Triple-DES, RC2/40 and others
- have a procedure to decide which algorithms to use

Certificate Authorities

- have several well-known CA's
- Verisign one of most widely used
- Verisign issues several types of Digital IDs
- with increasing levels of checks & hence trust

Class	Identity Checks	Usage
1	name/email check	web browsing/email
2+	enroll/addr check	email, subs, s/w validate
3+	ID documents	e-banking/service access

S/MIME Certificate Processing

- S/MIME uses X.509 v3 certificates
- managed using a hybrid of a strict X.509 CA hierarchy & PGP's web of trust
- each client has a list of trusted CA's certs
- and own public/private key pairs & certs
- certificates must be signed by trusted CA's