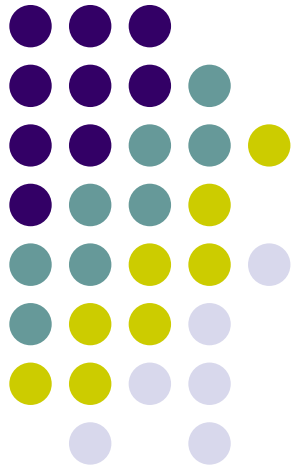
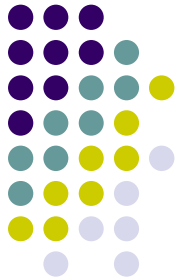
Information System Security

2110213 Information System Organization

Natawut Nupairoj, Ph.D.
Department of Computer Engineering
Chulalongkorn University

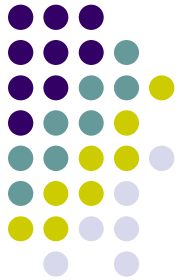


What is IS Security?



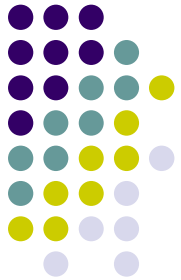
- Protecting and safeguarding systems from accidental, intentional or natural disasters
- Venerable points
  - Hardware, software, networks, physical facilities, data, and personnel

Common Types of Security Violations



- Company data theft by employees
- Gaining access to information stored on computer networks by cracking passwords
- Eavesdropping on wireless communications or on LANs and Internet connections
- Unauthorized modification of software

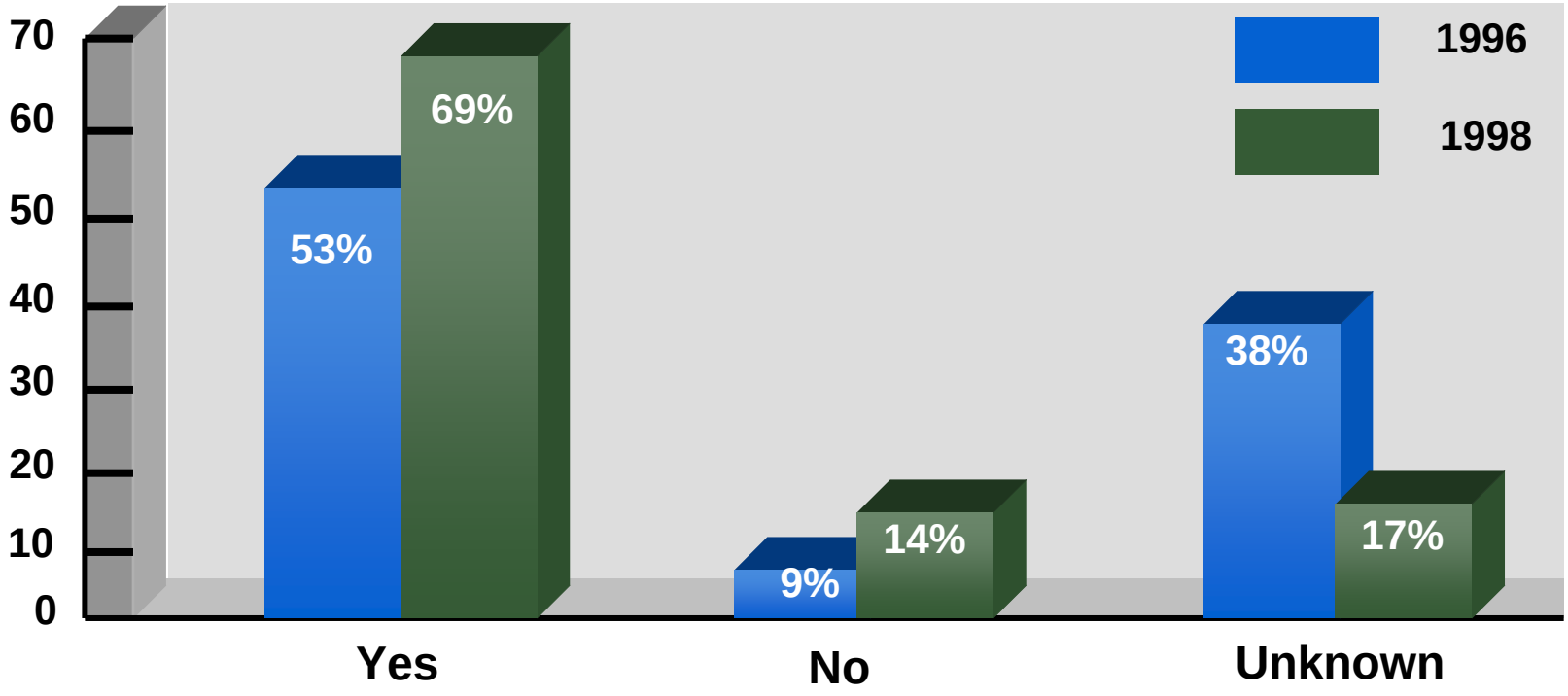
Common Types of Security Violations



- Theft of employees' identities to make illegal statements on the Internet
- Starting or fueling rumors on the Internet that are designed to harm the company
- Denial of service attacks in which people send lots of requests to a server such that no one can access that server

Awareness of Security Violations

Has your organization been the target of information espionage?

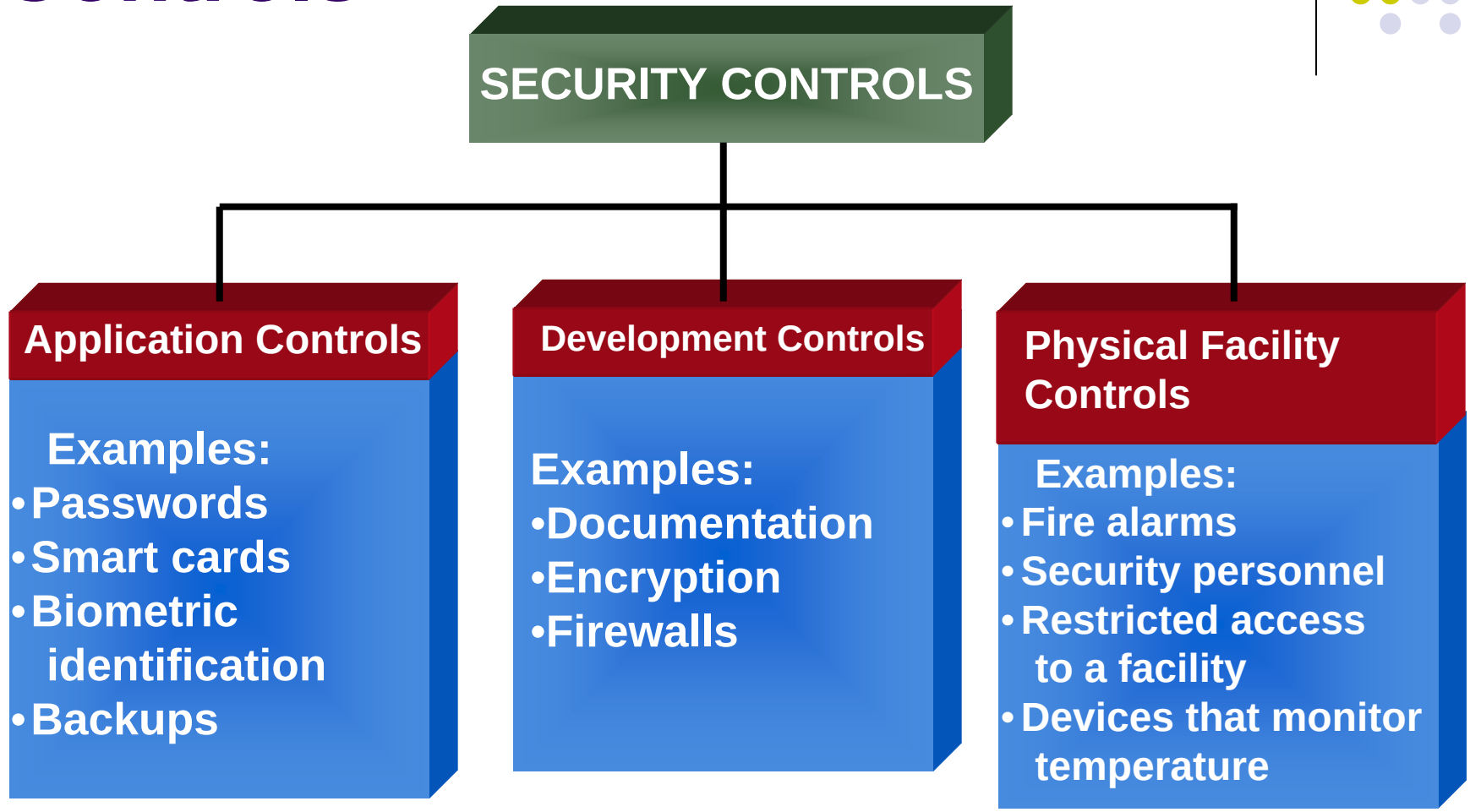


Source: Warroom Research, Inc., Annapolis, Md.

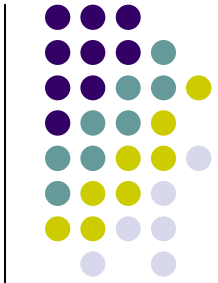
The Three Categories of Security Breaches

Types of Security Breaches	Description
Accidental or unintentional errors	Accidents relating to hardware and software. Employees can also cause unintentional security breaches.
Intentional errors	
Cracking passwords	Most common type of security violation, in which individuals intentionally decode passwords.
Breaking into computer hardware	Breaking into computer hardware such as modems, faxes, and cellular phones.
Software virus	Infected software that behaves in unexpected and undesirable ways.
Natural disasters	Tornadoes, earthquakes, and other disasters that cause computer systems to fail.

Classifications of Security Controls

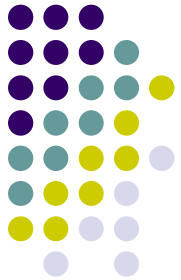


Application Controls



- Passwords
  - Many companies require employees to change their passwords frequently
  - Employees should use hard-to-guess or randomly generated passwords
- Smart cards
  - A plastic card with an embedded chip that provides users with digital signature capabilities

Application Controls *(cont.)*

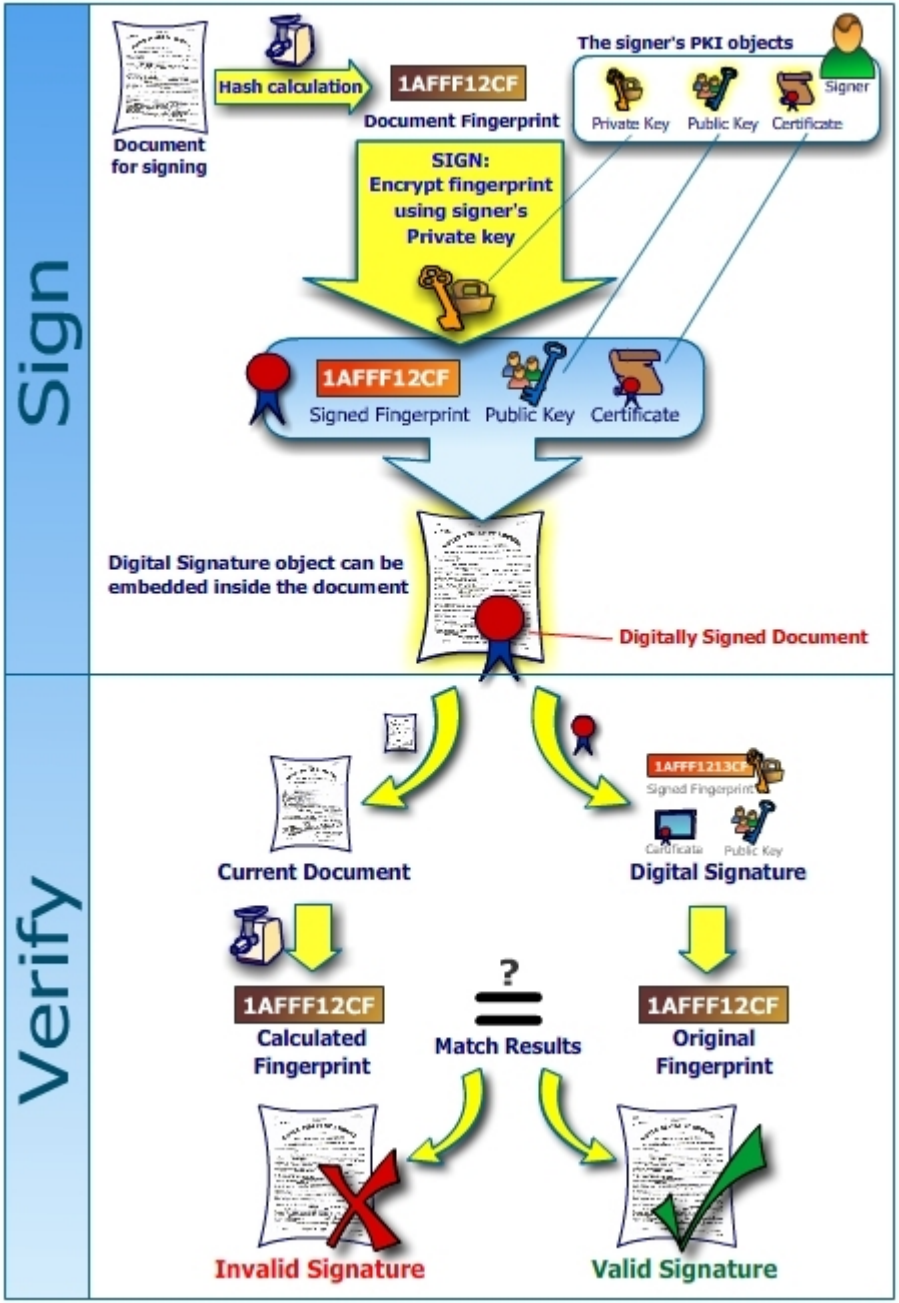


- Biometric identification techniques
  - Rely on body parts to validate that the user can access the system
    - finger prints
    - retinal scans
    - voice recognition
- Backup
  - Treat information like gold
  - Establish a backup routine
  - Keep your backups in a safe place

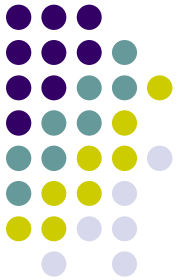
Security Token

Smart Card

- Pocket-size card with circuit to process information
  - Retrieve / store information
  - Digital signing


Sign
Document for signing
Hash calculation
1AFFF12CF
Document Fingerprint
The signer's PKI objects
Signer
Private Key
Public Key
Certificate
SIGN:
Encrypt fingerprint using signer's Private key
1AFFF12CF
Signed Fingerprint
Public Key
Certificate
Digital Signature object can be embedded inside the document
Digitally Signed Document
Verify
Current Document
Digital Signature
1AFFF12CF
Calculated Fingerprint
?
Match Results
1AFFF12CF
Original Fingerprint
Invalid Signature
Valid Signature

Two-Factor Authentication

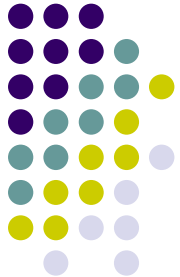


- Something you know
  - Password
- Something you have
  - ID Card, Credit Card, Mobile Phone
- Something you are
  - Biometric: retina, voice, fingerprint, etc.

Development Controls

- Documentation
  - Written set of documents that explain in detail the reasoning behind processes, procedures, and other details
    - The more detailed the documentation, the better off the company will be in the future
- Encryption
  - Converts data into a secret code before they are transmitted over the network

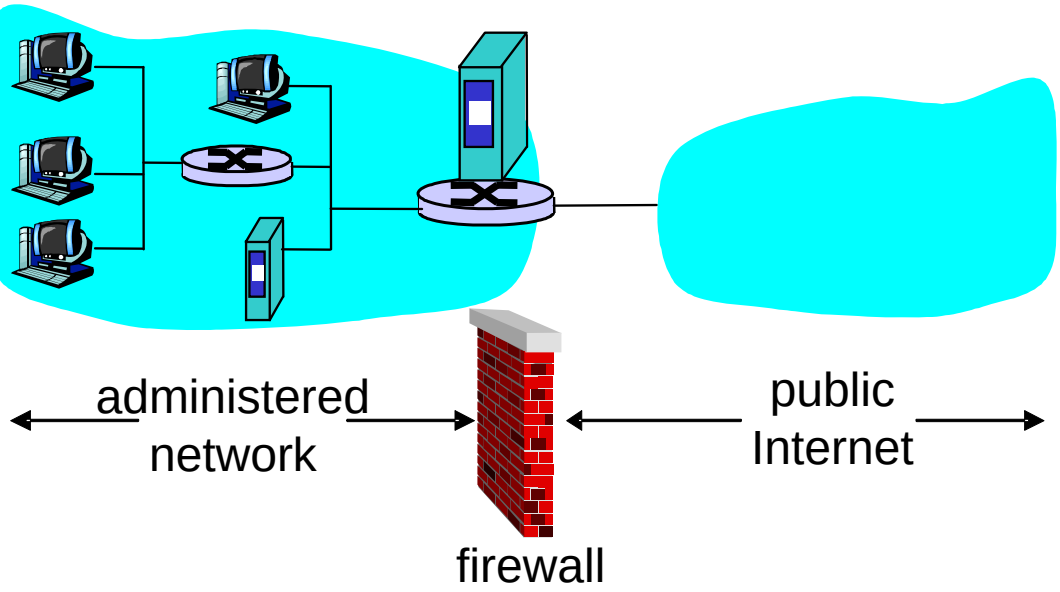
Physical Facility Controls



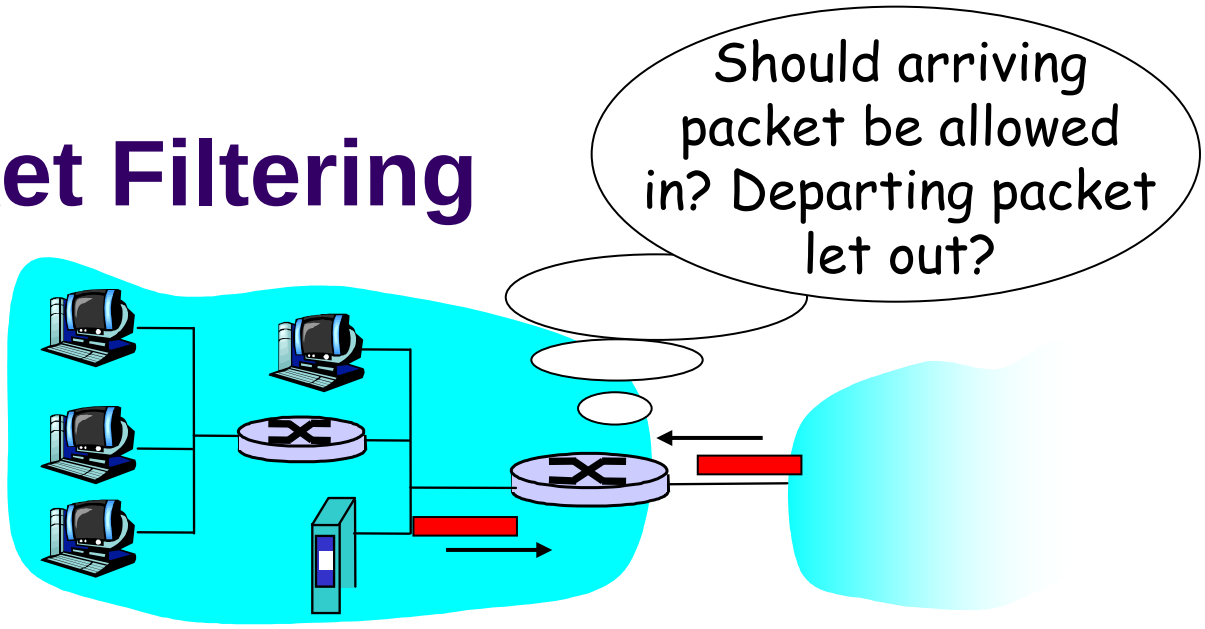
- Physical Facility Controls are the policies and procedures that control the physical environment in which systems reside
  - Posting security personnel
  - Installing fire alarms
  - Security alarms
  - Hidden cameras
  - Requiring users to wear badges or use smart cards to gain access to a building

Firewalls

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.



Packet Filtering



- internal network connected to Internet via router firewall
- router filters packet-by-packet, decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits