Introduction to Management Information Systems

Information Assurance & Security: Attacks, Risk and Protection

Network Systems

What is Information Assurance & Security?

Information Assurance

"Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

National Information Assurance (IA) Glossary

What is …?

- What are Information Systems?
  - Systems that store, transmit, and process information.

- What is Information Security?
  - The protection of information.

- What is Information Systems Security?
  - The protection of systems that store, transmit, and process information.

Information Systems Security

- Information Systems (IS) consists of:
  - hardware
  - operating system
  - application software
- IS Security – a collection of activities that protect the IS and stored data

Information Systems Security

- What is Information Assurance?
  - Emphasis on Information Sharing
  - Establishing and controlling trust
  - Authorization and Authentication (A&A)

- What is Cyber Security?
  - Protection of information and systems within networks that are connected to the Internet.

Information Systems Security

Terms

- Risk
  - something bad might happen to an asset
  - losing data, losing business
- Threat
  - an action that could damage an asset
  - natural (earthquake, flood)
  - human-induced
- businesses need to plan to deal with threats

Information Systems Security

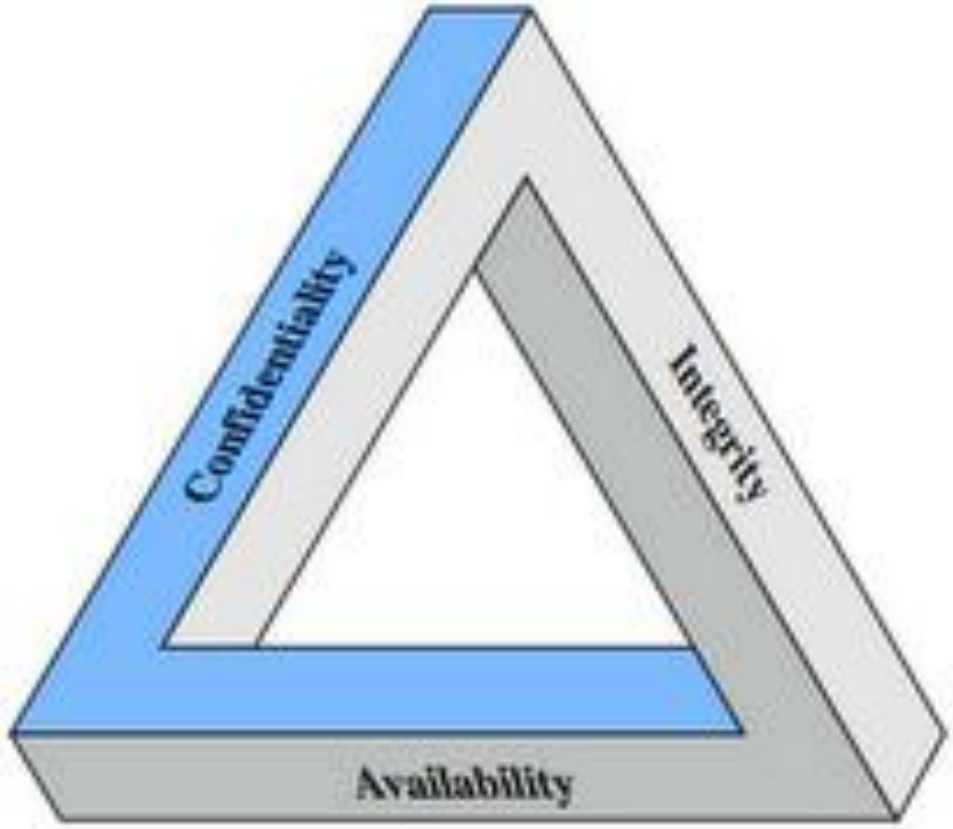
Threats

- Human-caused threats include:
  - viruses
    - a program written to cause damage
  - malicious code
    - a program to cause a specific action to occur
  - unauthorized access

Vulnerability

- A weakness that allows a threat to have access to an asset

CIA Triad



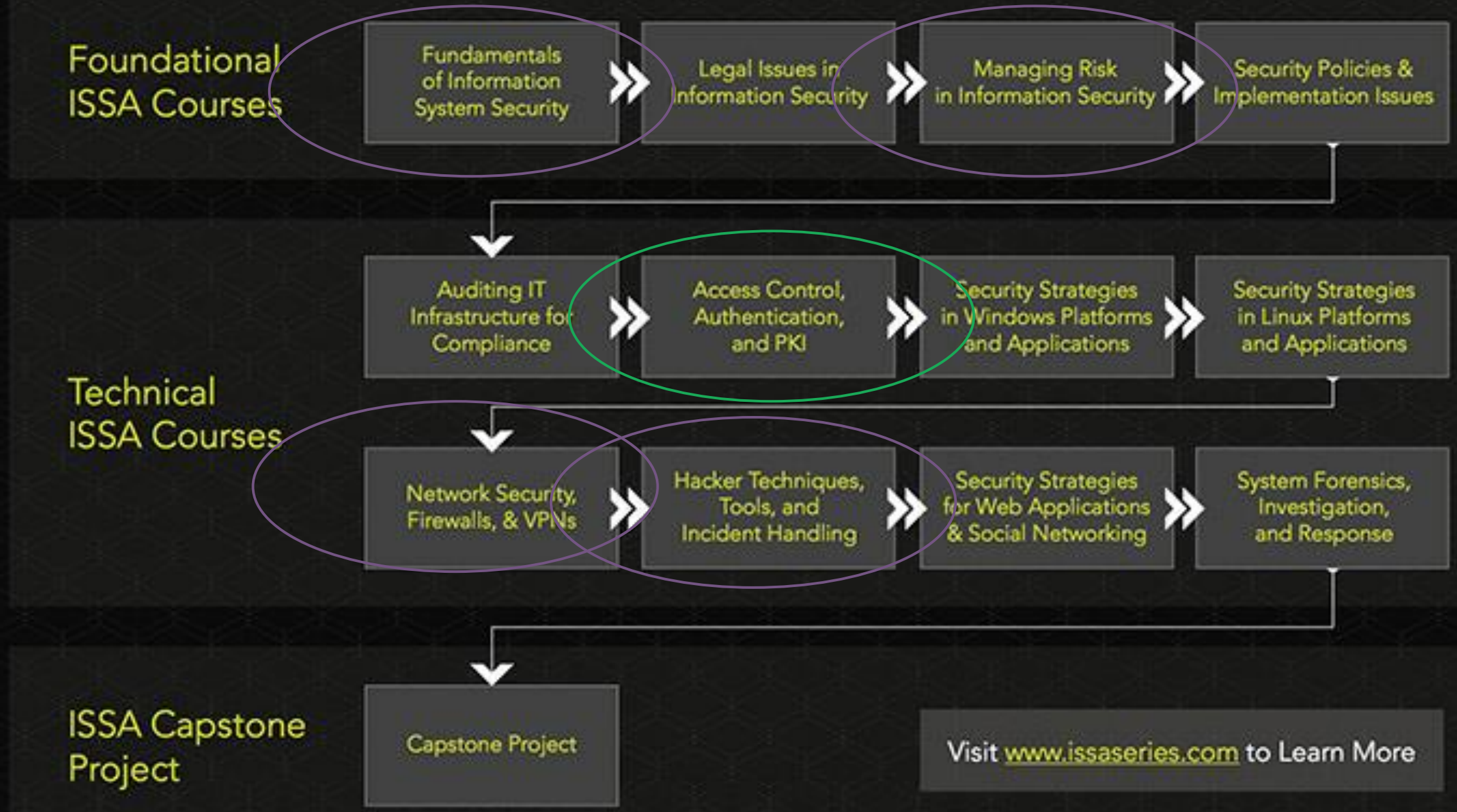
Tenets of Security: The CIA Triad

- Confidentiality
- Integrity
- Availability

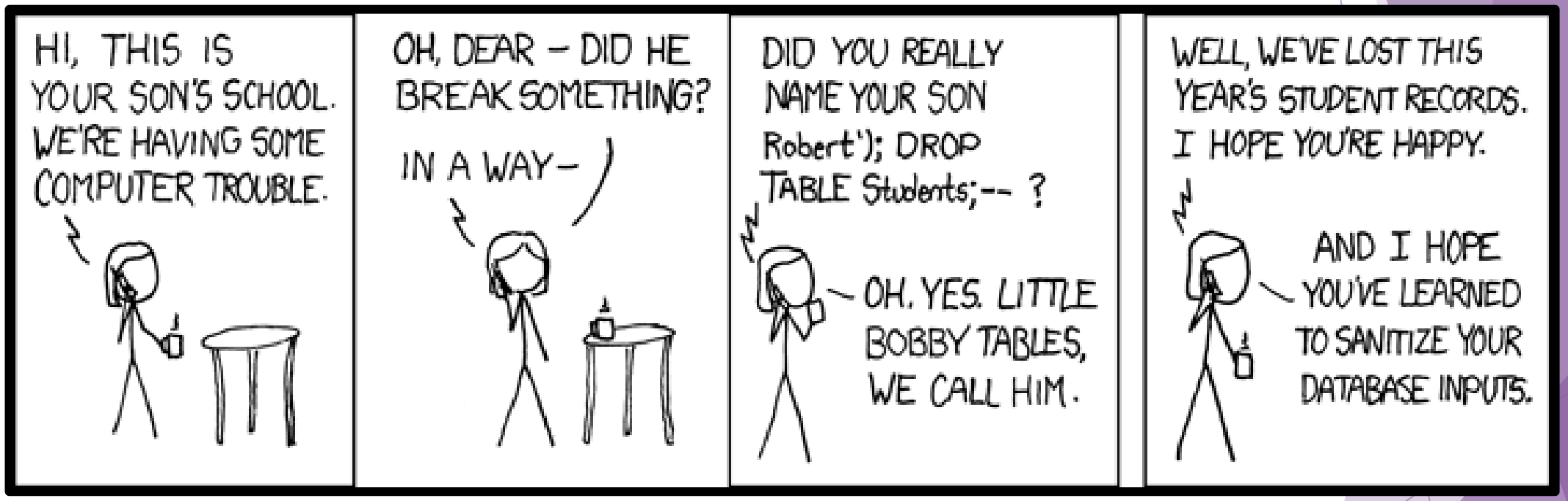
Information Assurance & Security

- Threats: Malware
- Threats: Hacking Tools & Techniques
- Network Security
- Software Security
- Operational Security
- Cryptography
- Access Controls
- Risk, Response & Recovery

International Social Security Association (ISSA)



	Security+ Exam	SSCP Exam	CISSP Exam	EC-Council Certified Ethical Hacker
Access Controls	General security concepts Operational / Organizational security	Access Controls	Access Controls	
Threats	General security concepts	Malicious Code	Application Security	Introduction to Ethical Hacking Footprinting and Reconnaissance System Hacking Trojans and Backdoors Viruses and Worms Sniffers Hacking Mobile Platforms Penetration Testing
Operational security	Infrastructure security Operational / Organizational security	Administration Audit and monitoring	Operational security Physical Security Security Architecture and Design	Social Engineering
Risk, response & recovery	Operational / Organizational security	Risk, response & recovery	Business Continuity and Disaster Recovery Planning Information Security and Risk Management Legal, Regulations, Compliance, and Investigations	
Cryptography	Basics of Cryptography	Cryptography	Cryptography	Cryptography
Network security	Communication Security Infrastructure security	Data Communications	Telecommunications and Network Security	Scanning Networks Enumeration Denial of Service Session Hijacking Hacking Webservers Hacking Wireless Networks Evading IDS, Firewalls and Honeypots
Software security	Infrastructure security	Malicious Code	Application Security	Buffer Overflows SQL Injection


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

attacks

Vulnerabilities

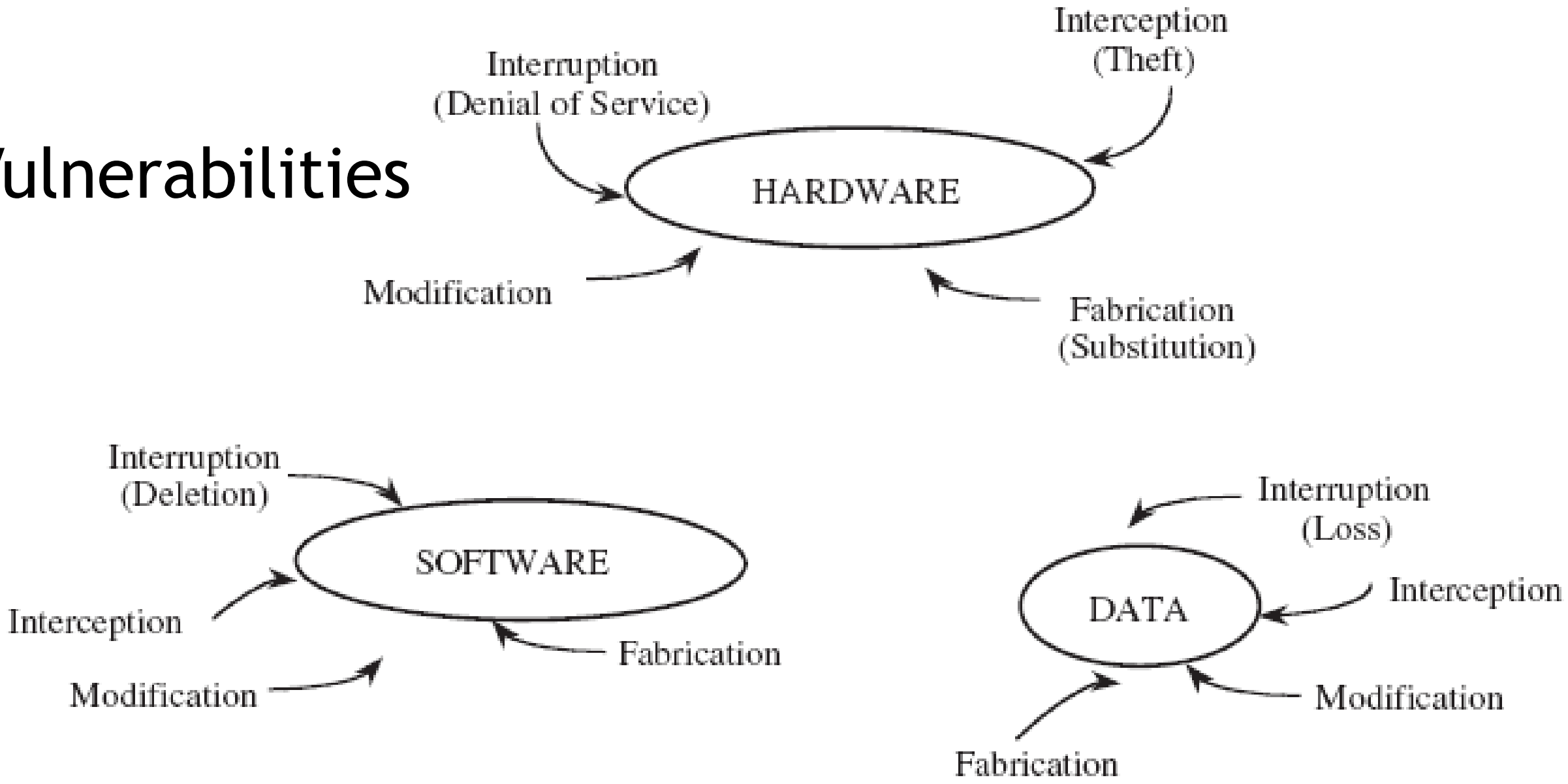


FIGURE 1-4 Vulnerabilities of Computing Systems.

Classifying Communication Attacks

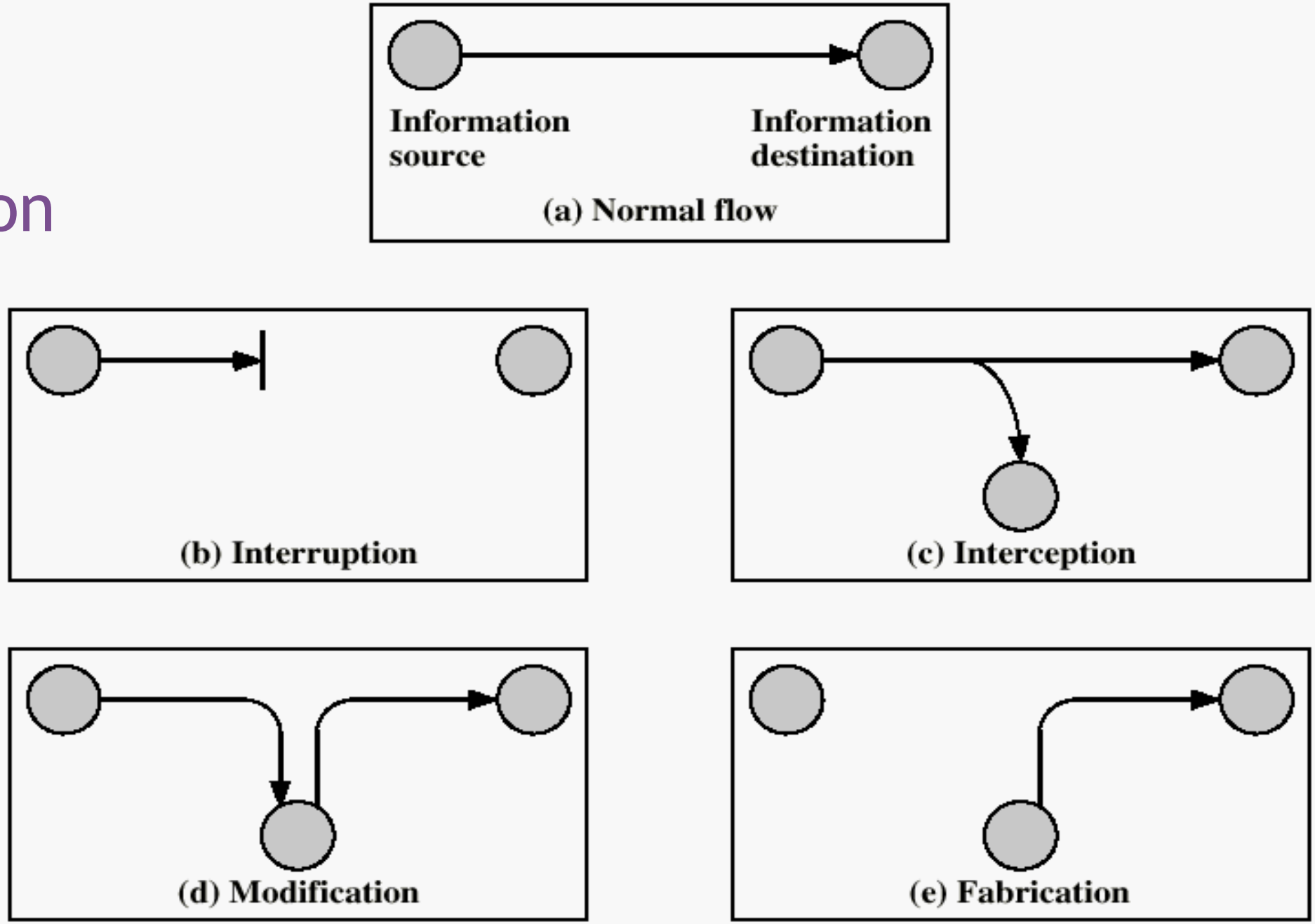


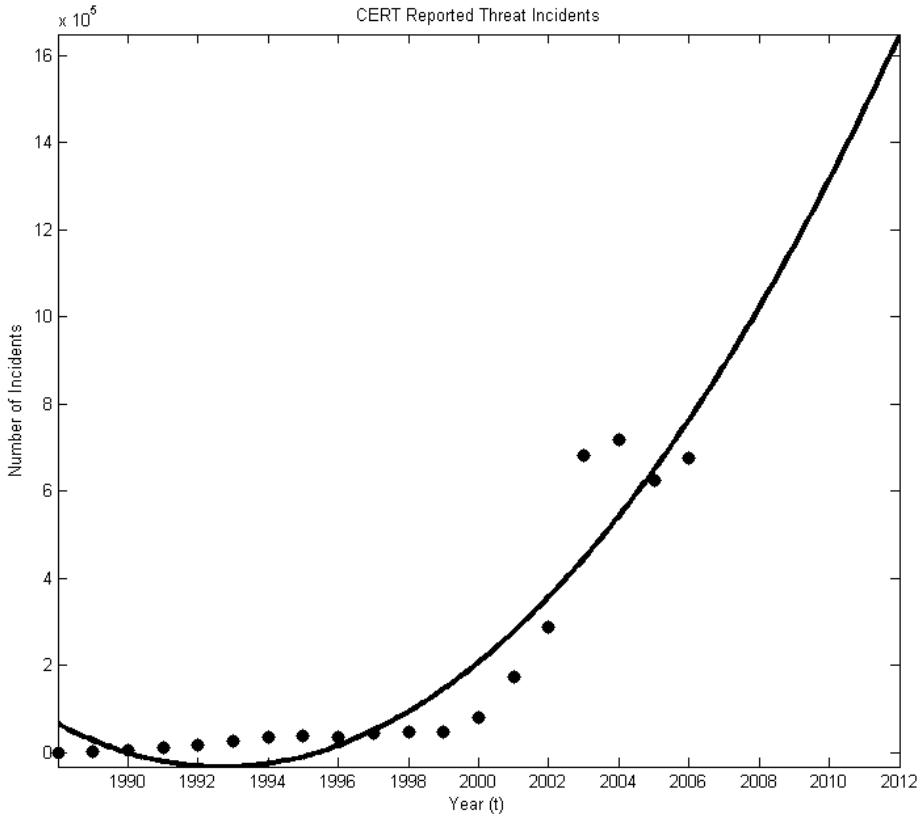
Figure 1.1 Security Threats

Challenges

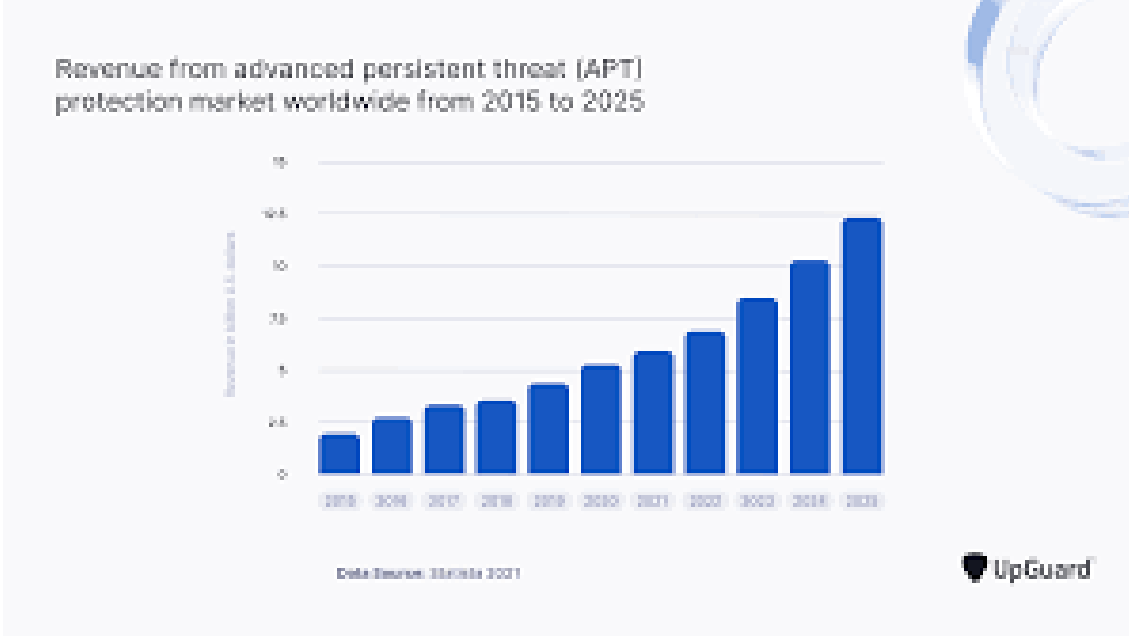
Rapid growth of Advanced Persistent Threats (APTs)

Half million cases of cyber related incidents in 2012.

How many now?

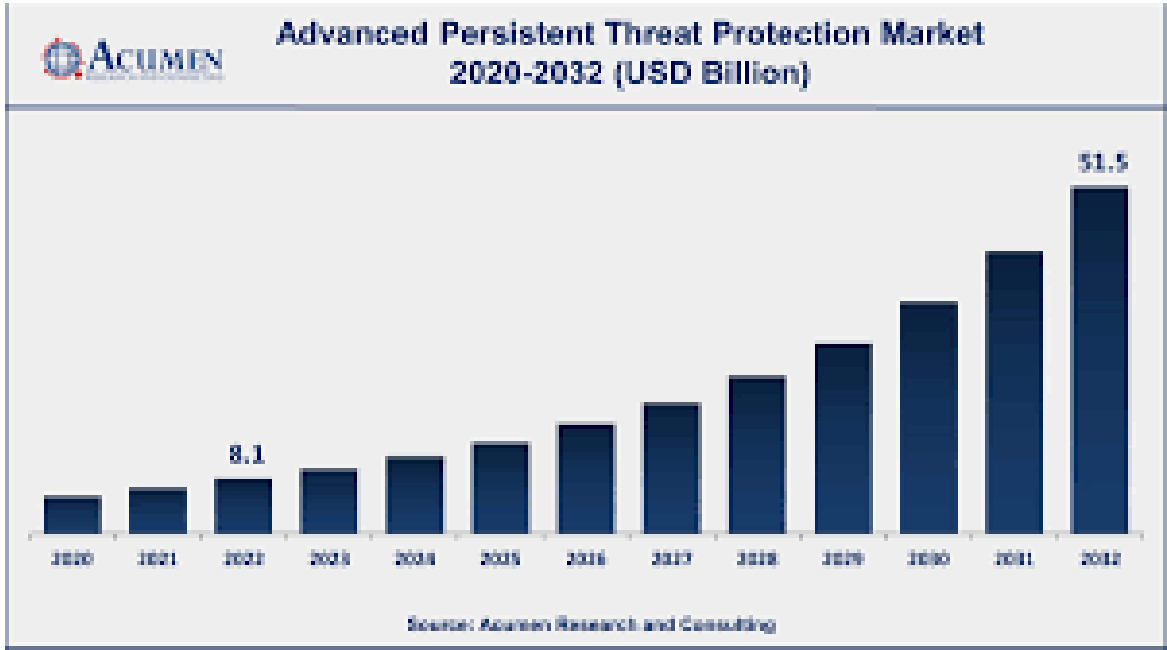


Source: US-CERT



Source: https://www.upguard.com/blog/what-is-an-advanced-persistent-threat

Source: https://www.acumenresearchandconsulting.com/advanced-persistent-threat-protection-aptp-market



attacks

more detail next week

report writing

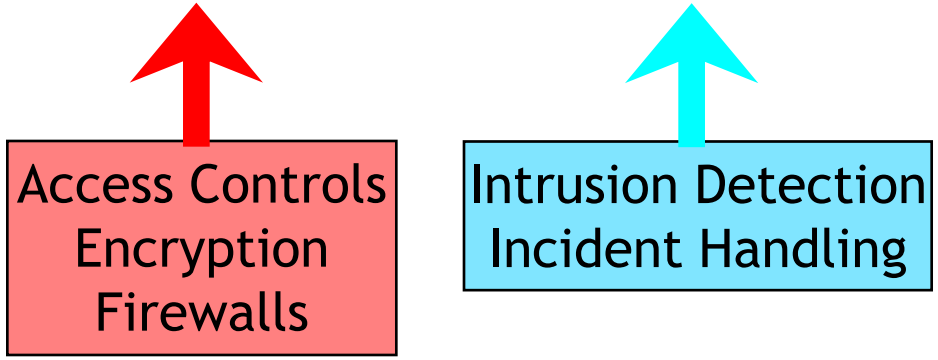
protection

Security Mechanisms

- Prevention, Detection, Recovery
- Prevention:
  - Encryption
  - Software Controls (DB access limitations, operating system process protection)
  - Enforce policies (frequent password change)
  - Physical Controls
- Detection: Intrusion detection systems (IDS)

Computer Security Operational Model

Protection = Prevention + (Detection + Response)



Prevention Mechanisms

- Adequate prevention means that an attack will fail.
- unauthorized access e.g. passwords
- user cannot override
  - but, if the password becomes public they will fail
- Prevention mechanisms are often cumbersome and do not always work perfectly or fail because they are circumvented.

Detection Mechanisms

- Detection is used when an attack cannot be prevented and
- it also indicates the effectiveness of prevention measures.
- The goal is to determine that an attack is underway or has occurred and report it.
- Audit logs are detection mechanisms.
- When you log into the design center's UNIX servers, it gives you the IP address of the last successful login.

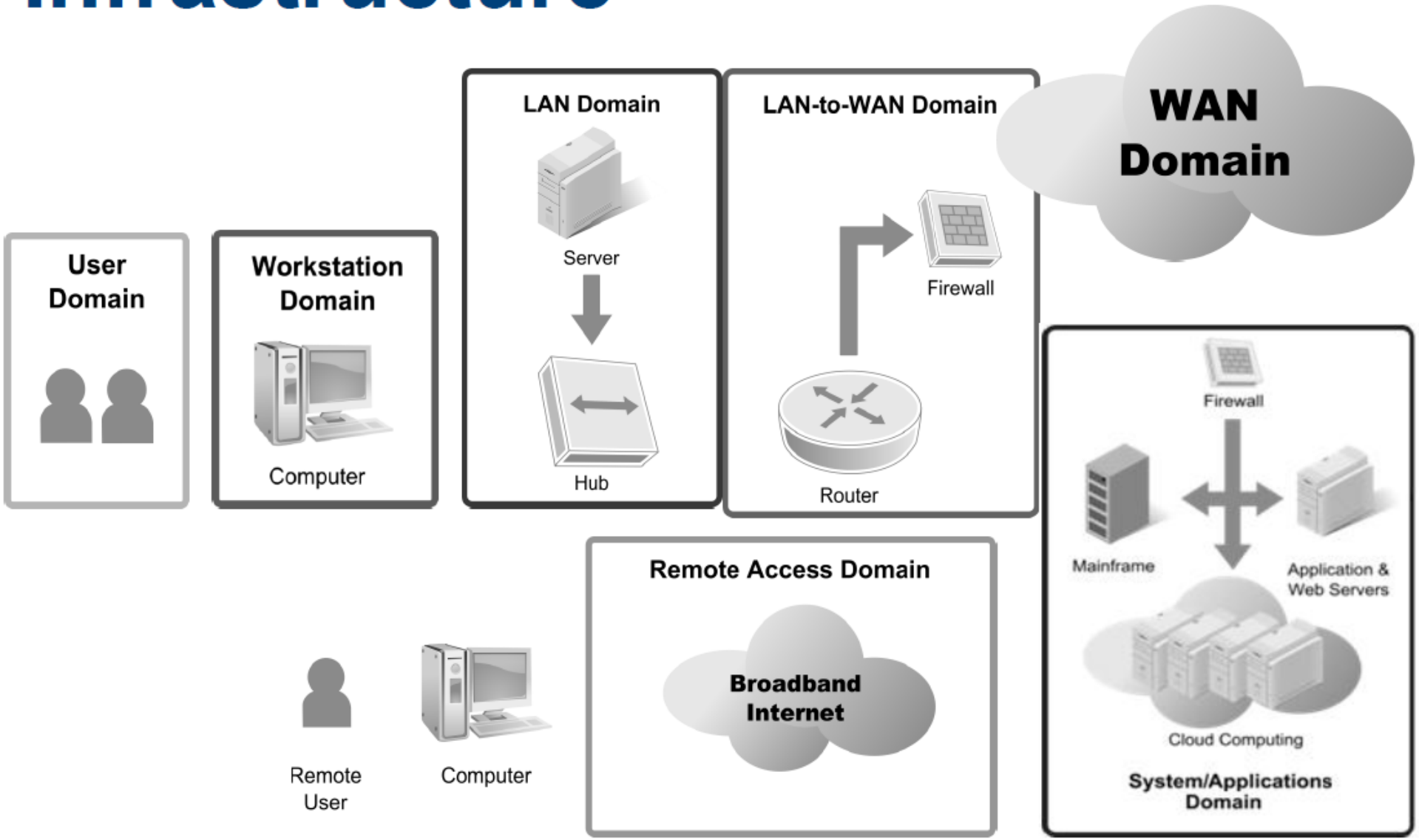
Recovery

- Recovery has several aspects.
  1. stop an attack and repair the damage.
  2. trace the evidence back to the attacker and discover the identity of the attacker (this could result in legal retaliation).
  3. to determine the vulnerability that was exploited and fix it or devise a way of preventing a future attack.

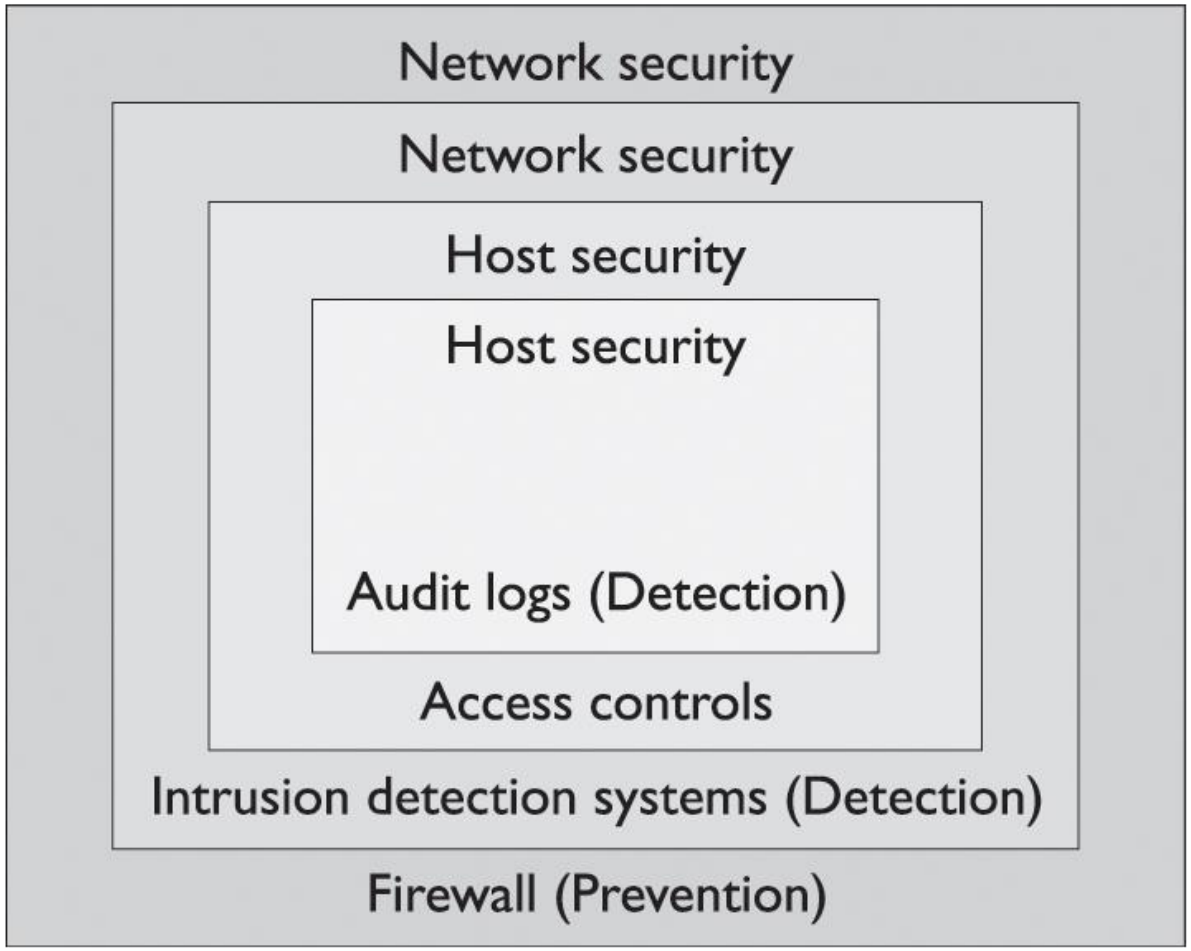
Example: Private Property

- **Prevention:** locks at doors, window bars, walls round the property
- **Detection:** stolen items are missing, burglar alarms, closed circuit TV
- **Recovery:** call the police, replace stolen items, make an insurance claim …

Seven Domains of a Typical IT Infrastructure



The Layered Model



Various layers of security

Defense in Depth

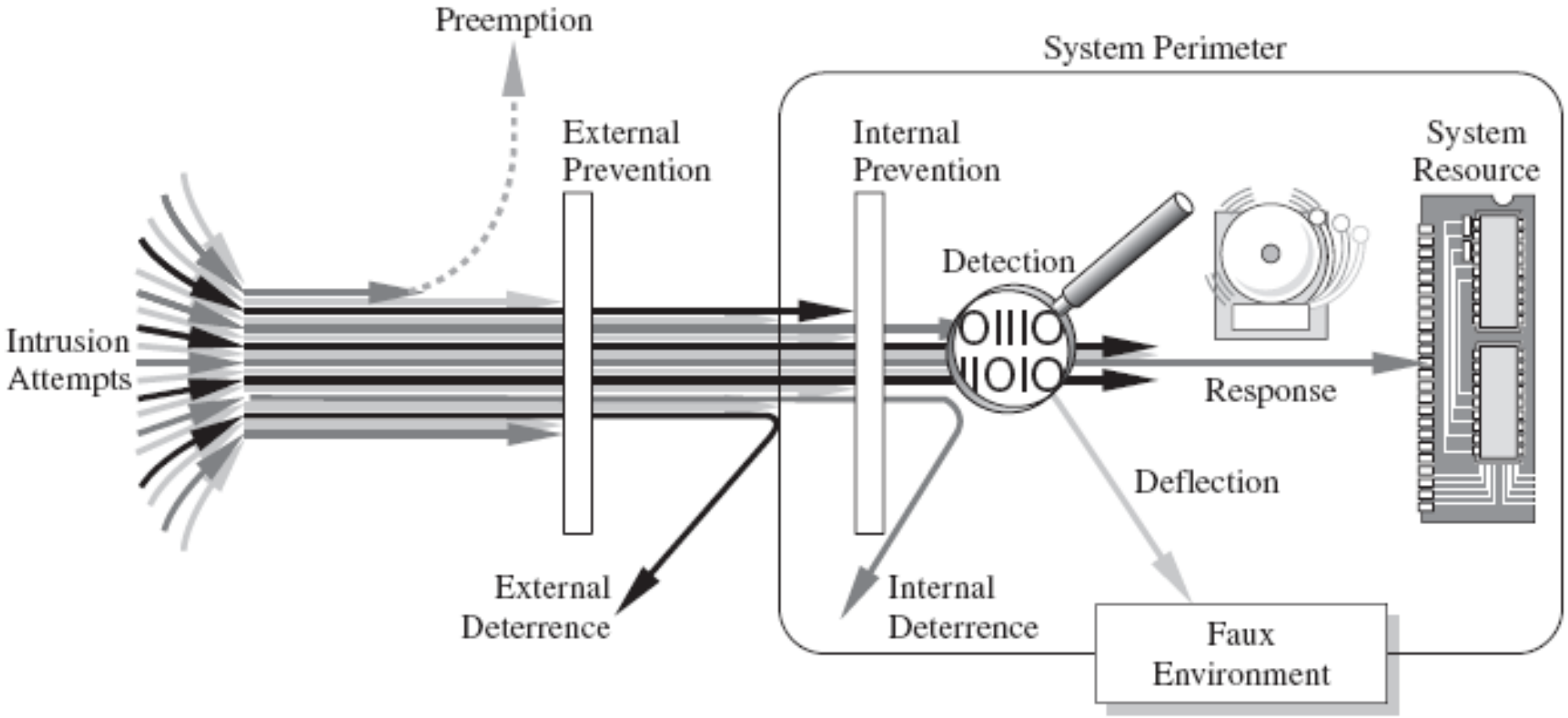


FIGURE 1-6 Multiple Controls.

The Castle Approach

Fail Open / Fail Closed

Security mechanism failure, two outcomes:

- Fail Open the mechanism permits all activity
- Fail Closed the mechanism blocks all activity
- Principles:
  - Different types of failures will have different results
  - Both fail open and fail closed are undesirable, but sometimes one or the other is catastrophic!

Fail Soft

Fail soft:

- Fail soft is the process of shutting down non-essential system components therefore
- resources are freed-up to allow essential services to continue operating

Two Factor Authentication

- First factor: what user knows
- Second factor: what user *has*
  - Password token
    - Passcode creator (*every n minutes*)
  - USB key
  - Digital certificate
  - Smart card

RSA SecurID SD600

RSA SecurID SID700

RSA SecurID SD200

RSA SecurID SID800

RSA SecurID SD520


BlackBerry with
RSA SecurID software token

How a User Should Treat Userids and Passwords

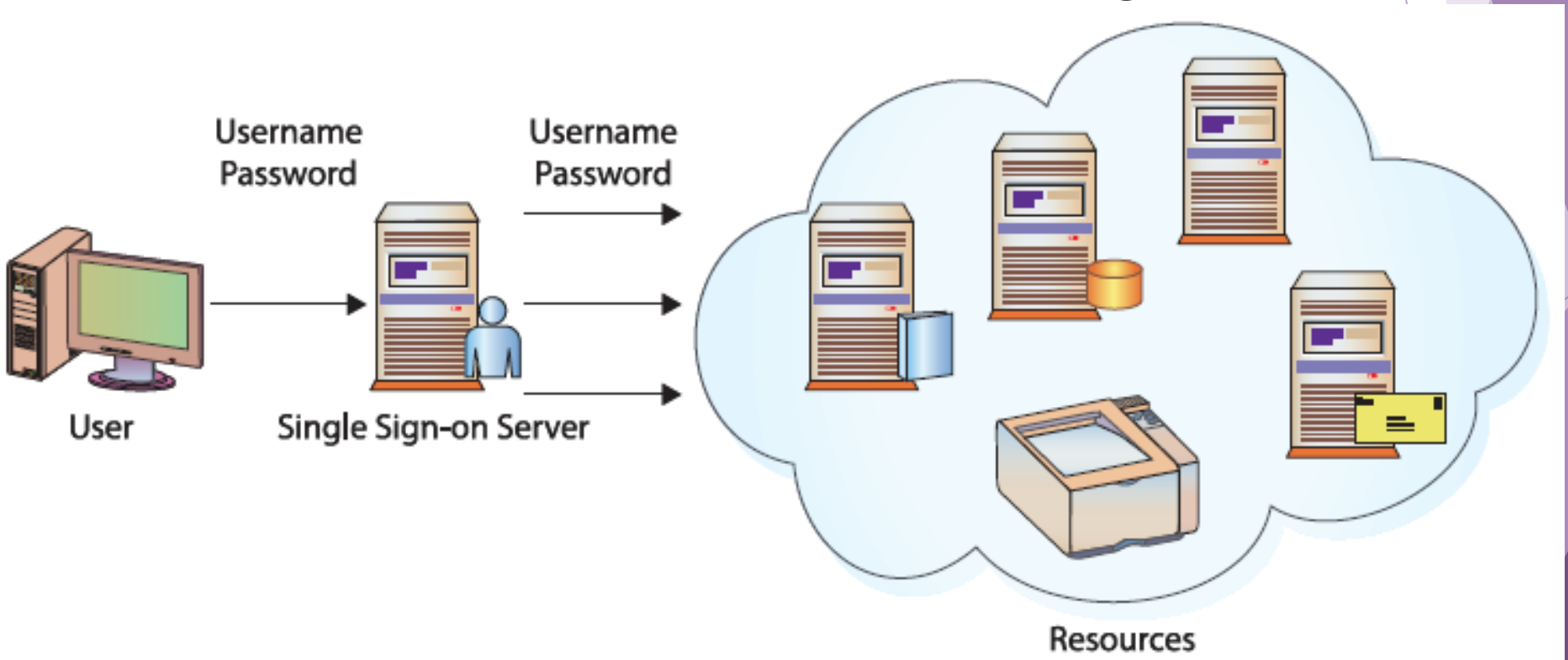
- Like a toothbrush –
  - don’t let anyone else use it, change it every month or so
- Keep it secret
- Do not share with others
- Do not leave written down where someone else can find it
- Store in an encrypted file or vault

Biometric Authentication

- Stronger than userid + password
- Stronger than two-factor

Single Sign-On (SSO)

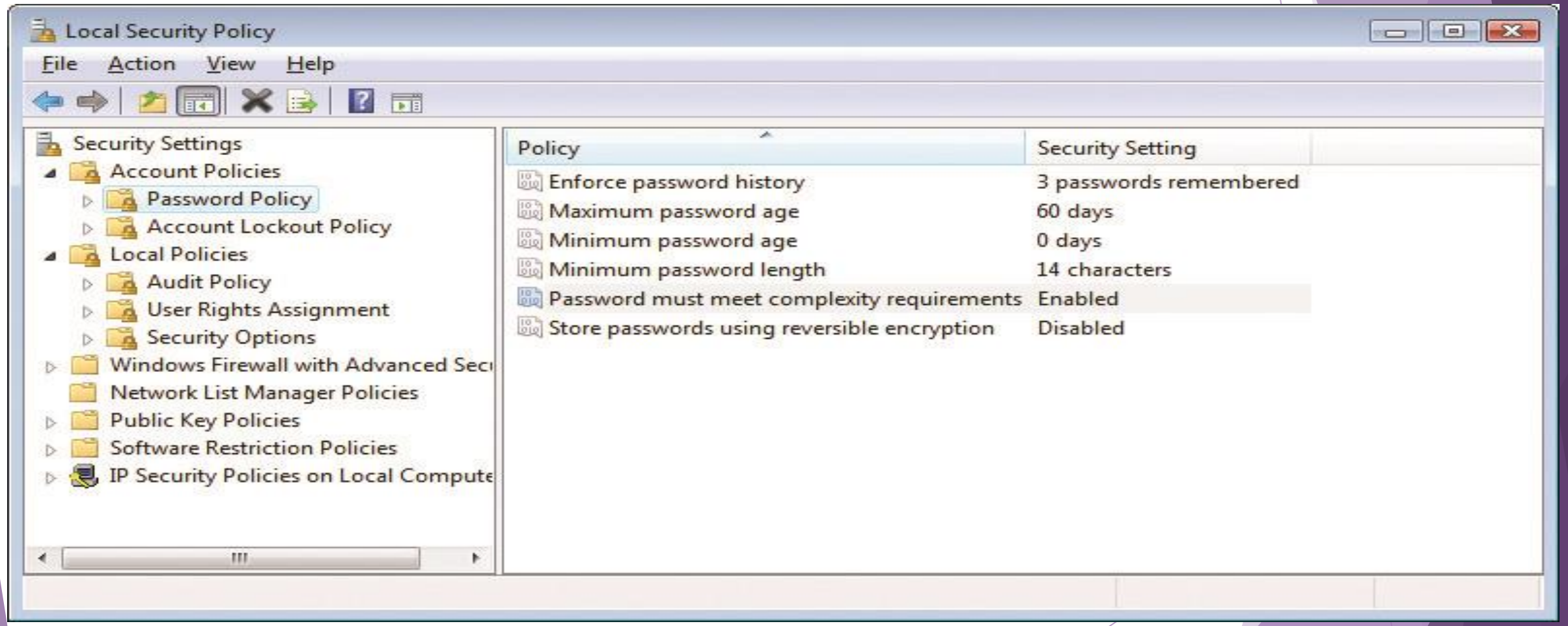
- Weakness: intruder can access all participating systems if password compromised
- Best to combine with two-factor / strong



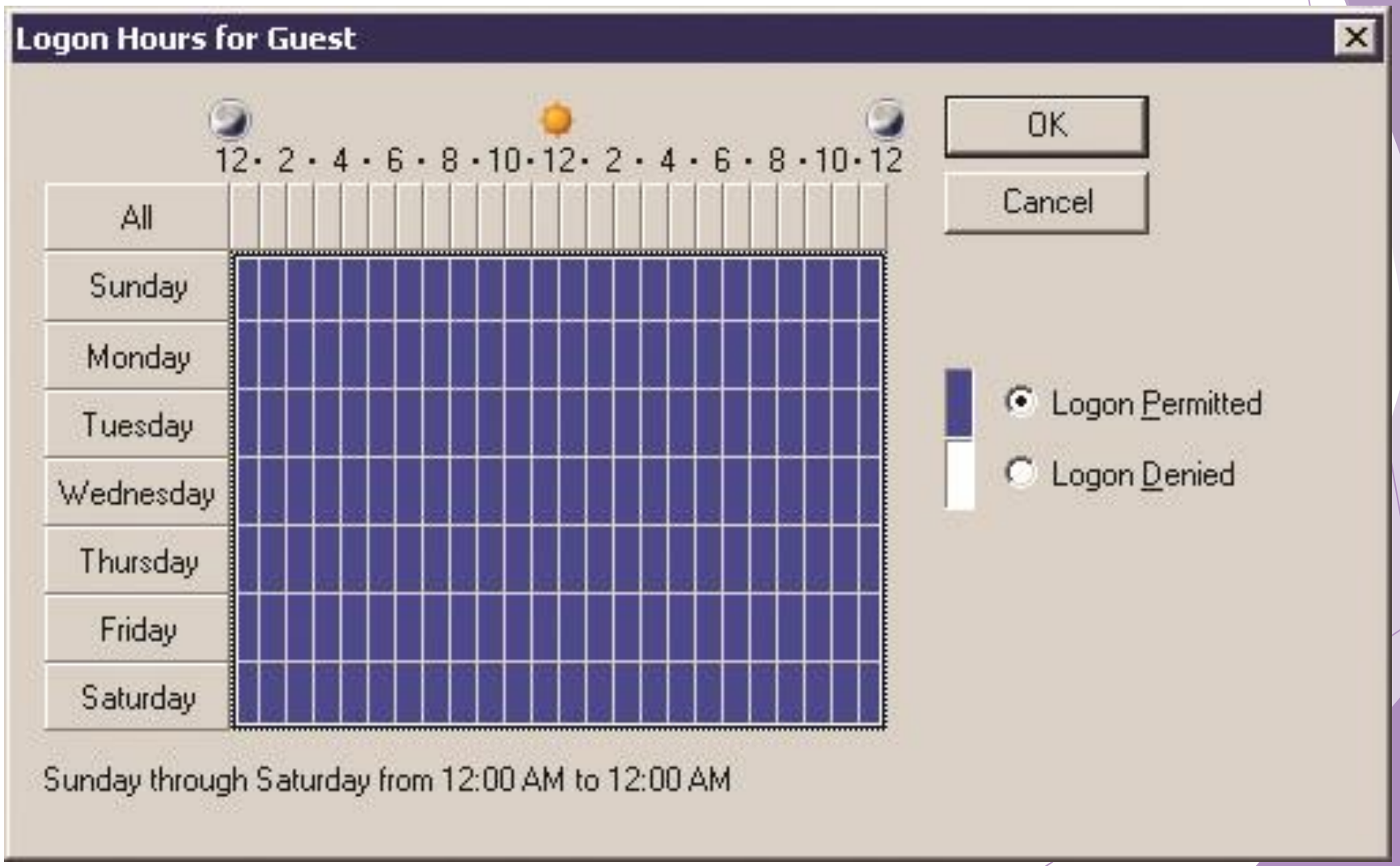
Categories of Controls

- Detective controls
- Deterrent controls
- Preventive controls
- Corrective controls
- Recovery controls
- Compensating controls

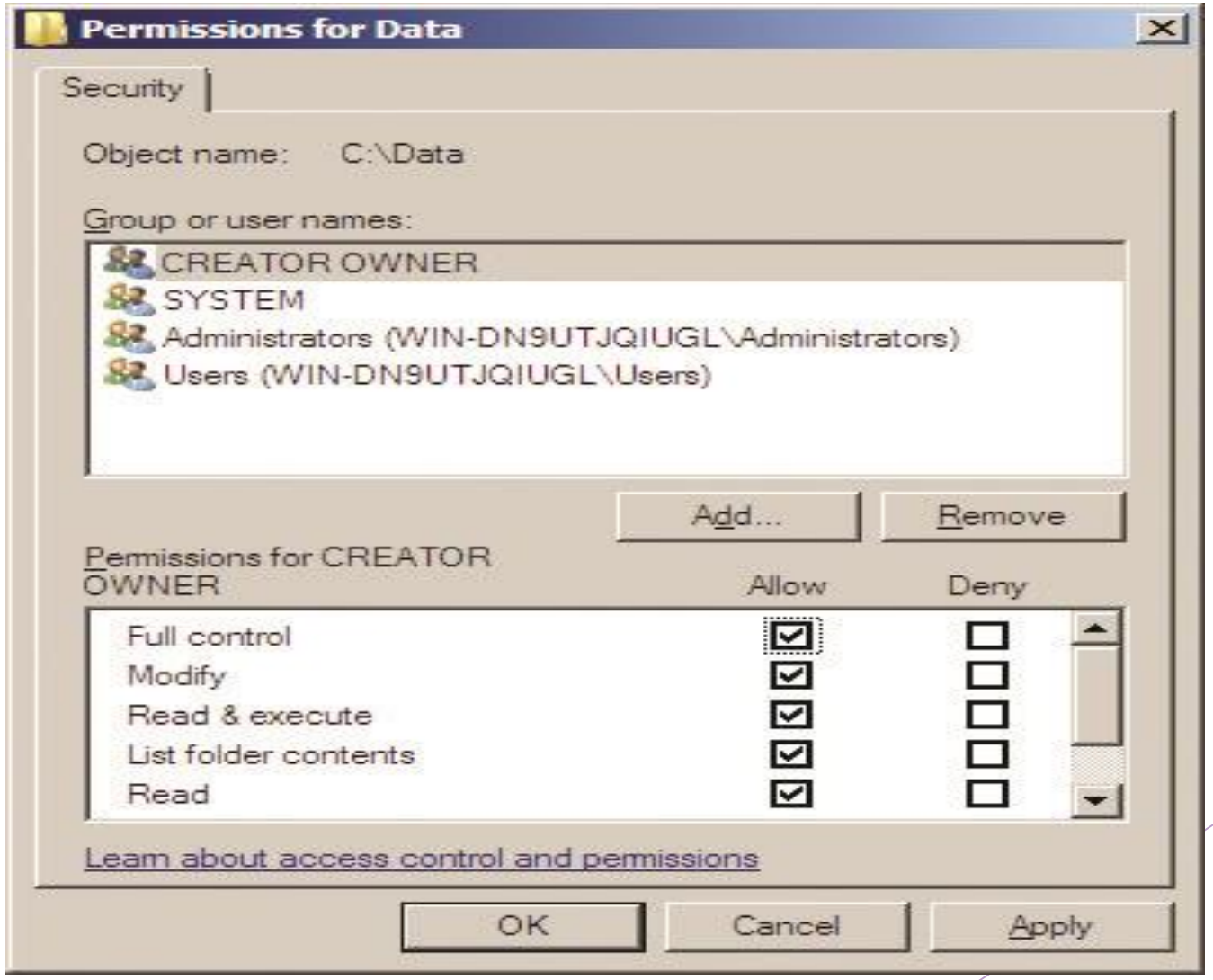
Password Policy Options



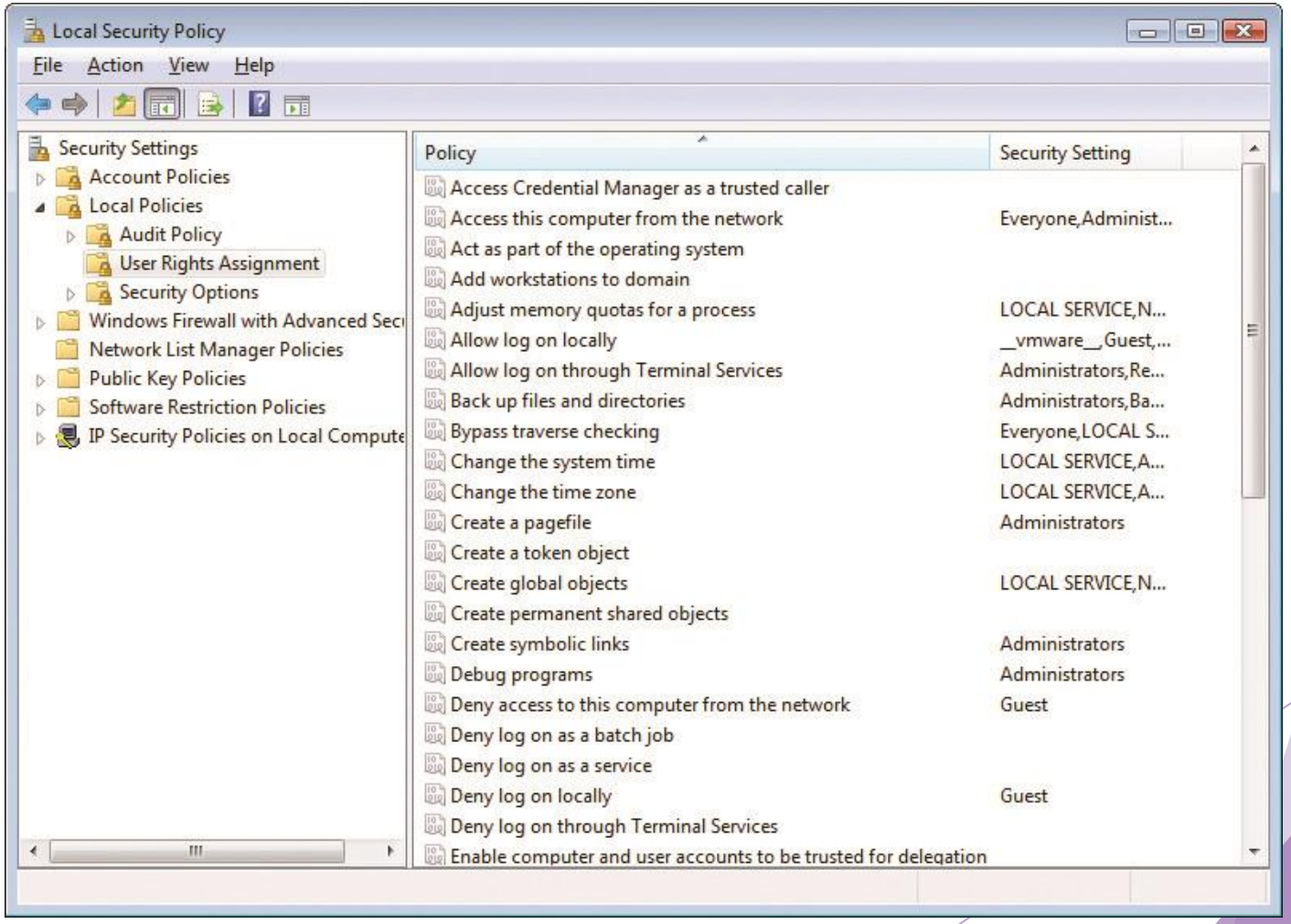
Setting Logon Hours



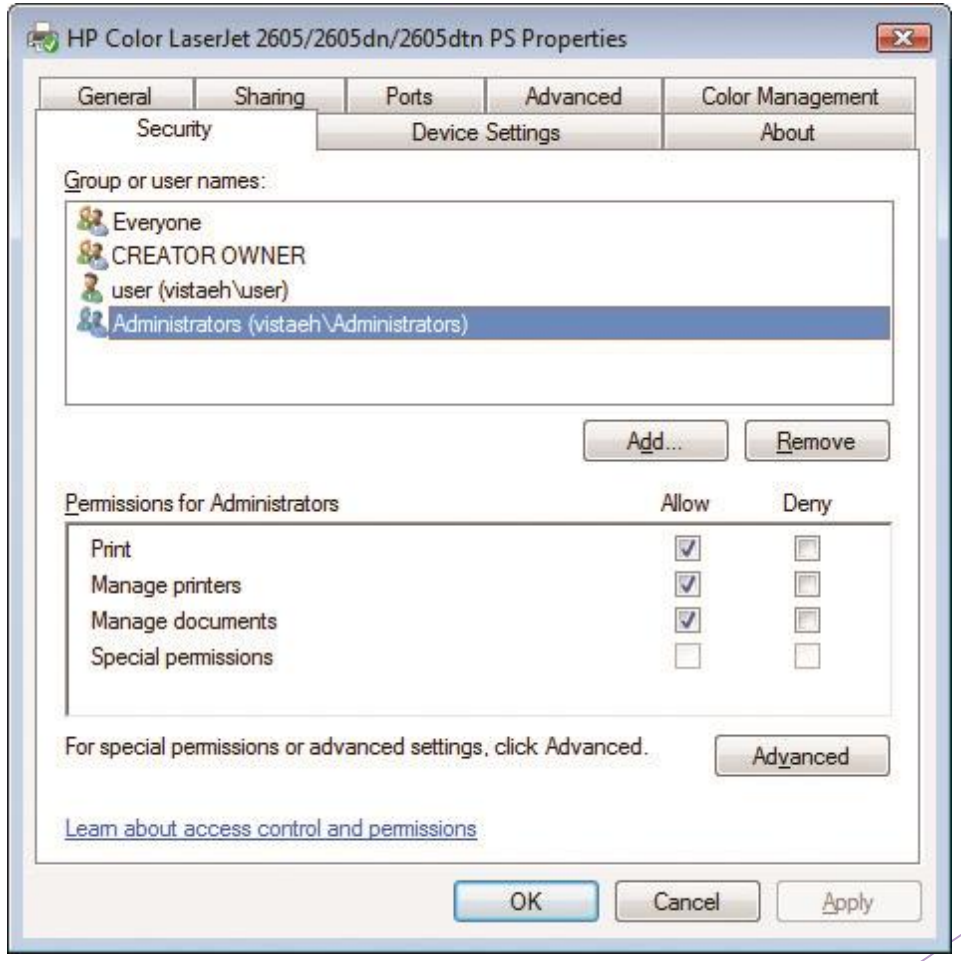
Permissions for the Data Folder



User Rights Assignment Options from Windows Local Security Settings



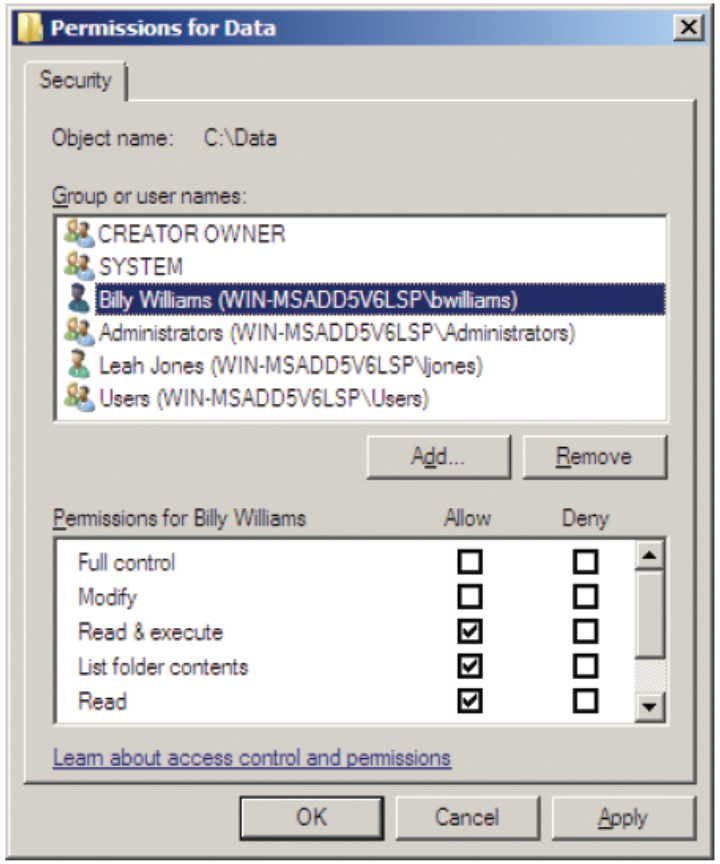
Security Tab Showing Printer Permissions Under Windows Vista

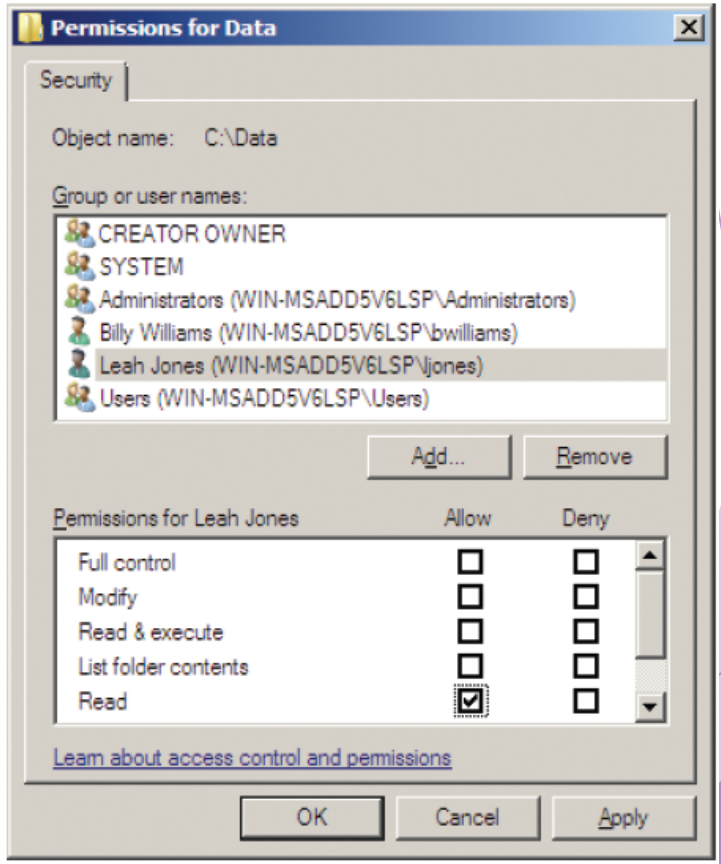


Access Control Lists

- Routers and firewalls – An ACL is a set of rules used to control traffic flow into or out of an interface or network.
- System resources –files and folders
- ACL lists permissions attached to an object
  - who is allowed to view, modify, move, or delete that object

Access Control Lists





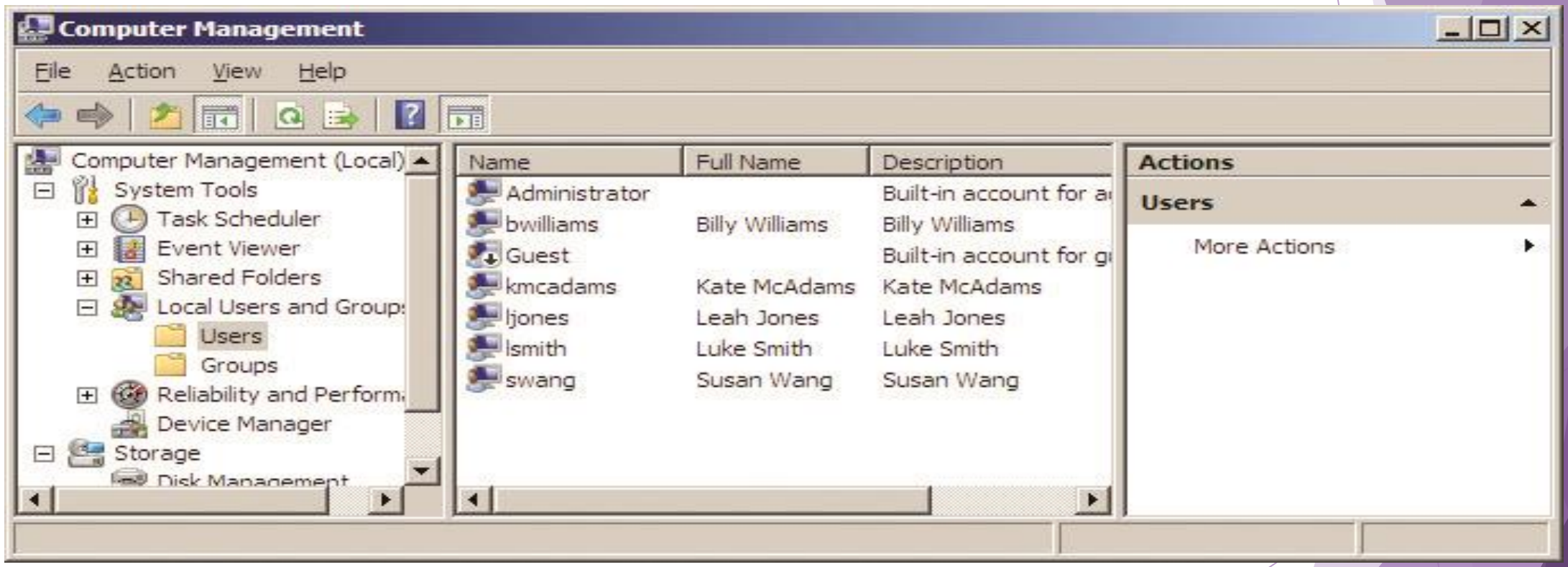
User, Group, and Role Management

- User – Any person accessing a computer system
- Group – Multiple users that are granted access to a resource at the same time
- Role – Access is granted or denied based on a person's job or function within the organization

Users

- Username – A unique alphanumeric identifier given to every user that is used to identify them when logging into or accessing the system.
- First Step in Privilege Management – No user should be allowed to create their own account.
- Permissions – Control what the user is allowed to do with objects on the system.
- Rights – Define the actions a user can perform on the system itself.
- Administrator, Root, Superuser – User accounts with extensive access to a system.

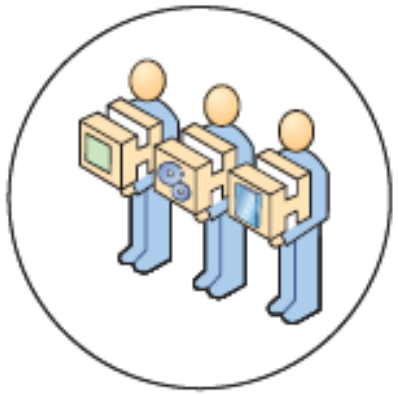
Windows 2008 Server Users



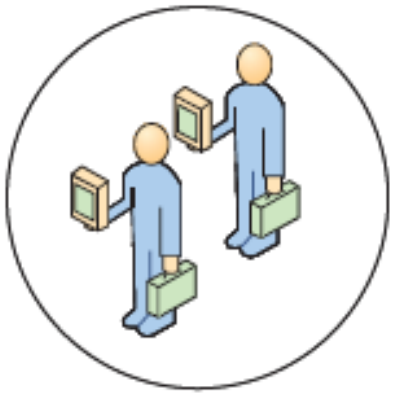
Group

- Group – A collection of users with some common criteria

Management

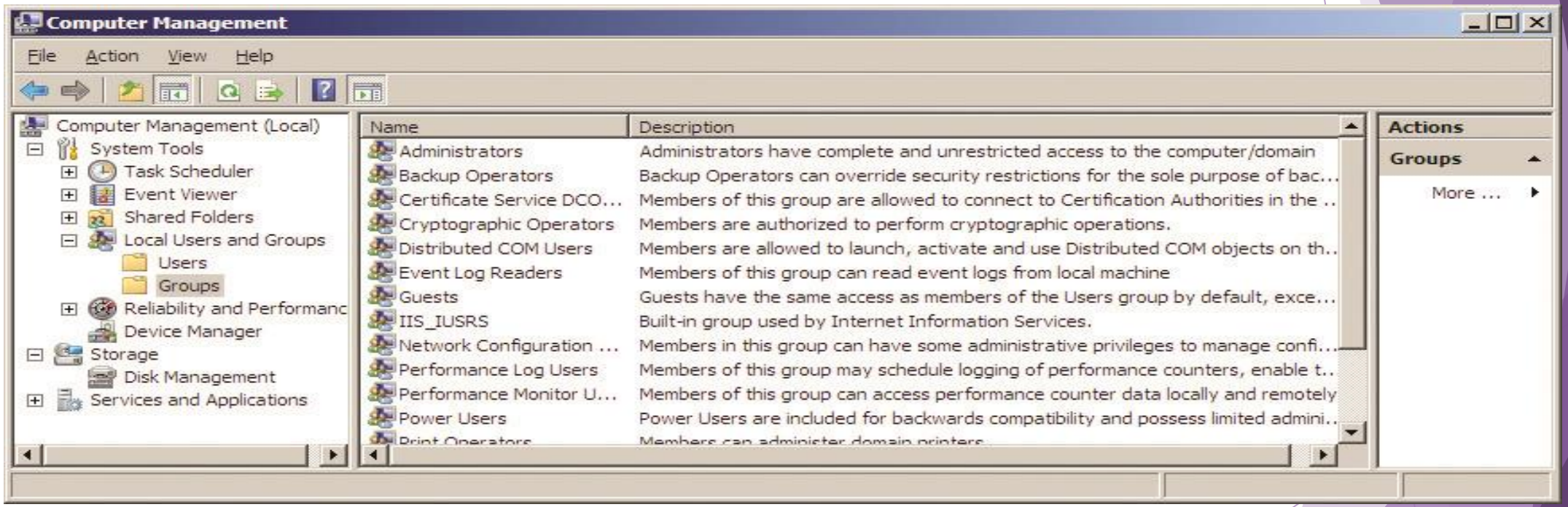


Engineering



Sales

Windows Server 2008 Group Management



Formal Models

Access Control Models

- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Non-discretionary access control (NDAC)
- Rule-based access control (RBAC)
- other models (Biba, Clark-Wilson, Bell-La Padula, etc.)

risk mitigation

Plans

- Business Continuity Plan (BCP)
  - what needs to keep going
- Disaster Recovery Plan (DRP)
  - what to do after a disaster

Thank you!

any questions?