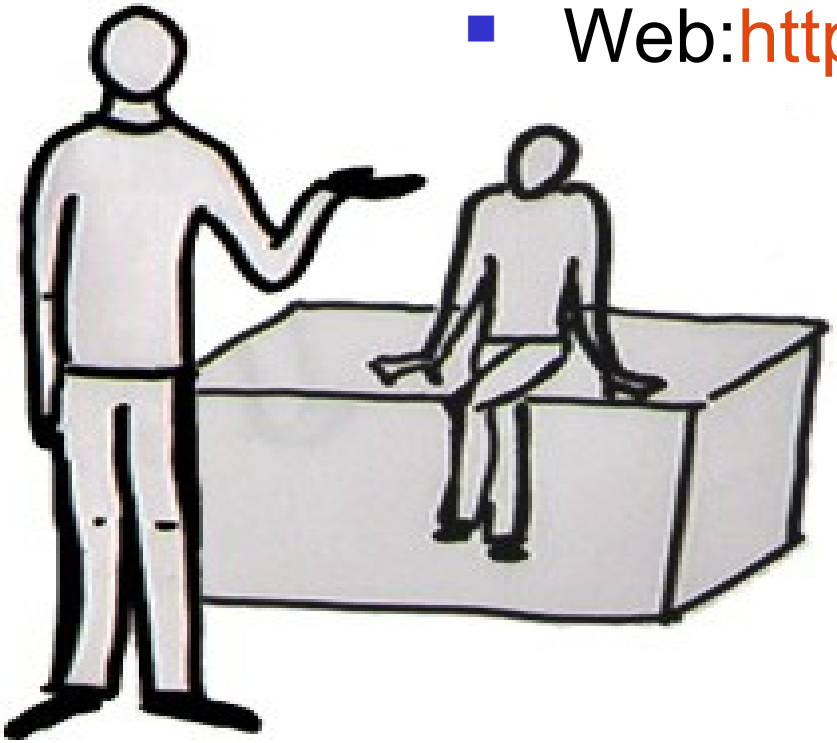
Information System Security

Nguyen Ho Minh Duc, M.Sc

Contact

- **Nguyen Ho Minh Duc**
- Phone: 0935 662211
- E-mail: duc.nhm@gmail.com
- Web:http://nhmduc.wordpress.com



Lecture 01

INTRODUCTION

Topics

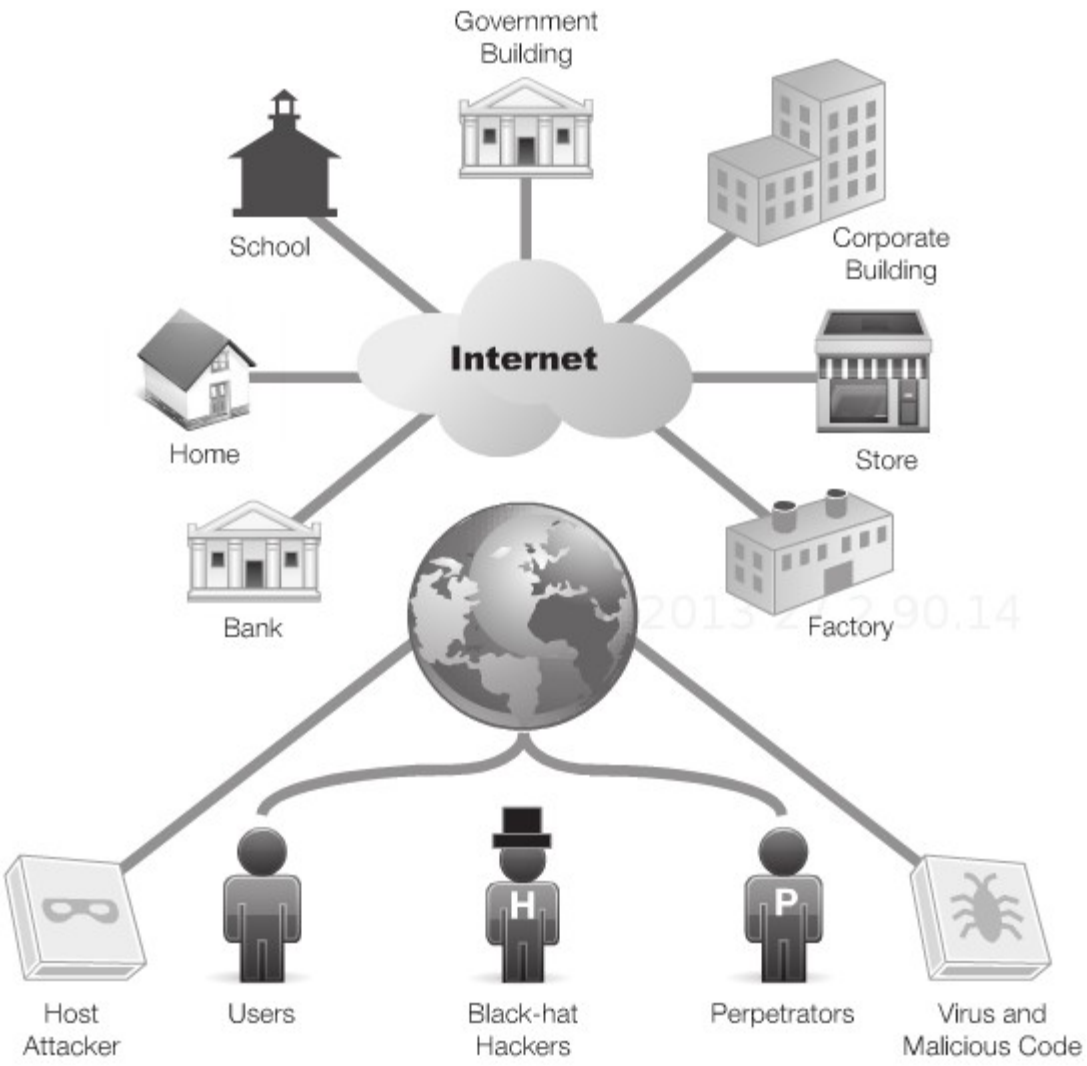
- What information system security is
- What the tenets of information systems security are
- What the seven domains of an IT infrastructure are
- What the weakest link in an IT infrastructure is
- How an IT security policy framework can reduce risks
- How a data classification standard affects an IT infrastructure's security needs

Goals

- Relate how availability, integrity and confidentiality requirements affect the seven domains of a typical IT infrastructure
- Descibe the threats and vulnerabilities commonly found within the seven domains
- Identify a layered security approach throughout the seven domains
- Develop an IT security policy framework to help reduce risk

What is “Enterprise Security”

- Basics of communication
  - One-to-one
  - One-to-many
  - Many-to-one
  - Many-to-many
- WWW
- Cyberspace


Government Building
School
Corporate Building
Internet
Home
Store
Bank
Factory
H
P
Host Attacker
Users
Black-hat Hackers
Perpetrators
Virus and Malicious Code

Why Enterprise Security

- Because you can't wait for thing to go bad – because when they do, they go bad in a BIG way

The Web

- Connects Wed sites, Web pages, digital content
- Cyberspace is the collection of
  - Web
  - Users
  - Networks
  - Applications that can “communicate”
  - eCommerce

Cyber security

- Cyberspace are not automatically secure
- The heart of problem is the lack of security in TCP/IP communications protocol
- Protocol ?
- IT is in great need of proper security controls

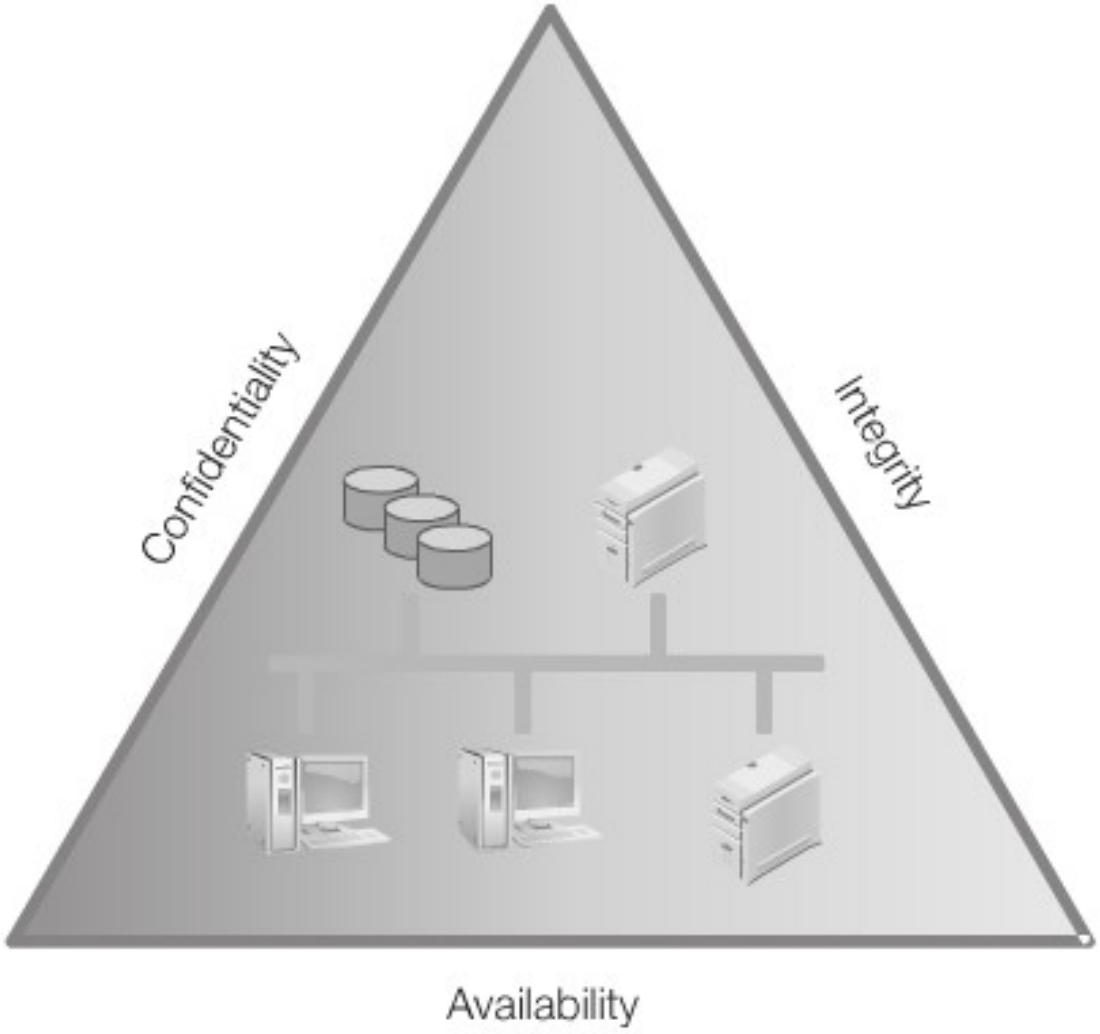
Definitions

- **Risks** – probability that something bad could happen to an “asset”
- **Threat** - actions that poses potential damage or data compromise
  - Virus – software designed to cause damage to system, application or data
  - Malware (malicious code) – code that causes specific action
- **Vulnerability** - Any weakness that allow a threat to occur (or be realized)

Defining Information Systems Security

- An **information system** consists of the hardware, operating system, and application software that work together to collect, process, and store data for individuals and organizations.
- **Information systems security** is the collection of activities that protect the information system and the data stored in it

Three tenets of Information Systems Security

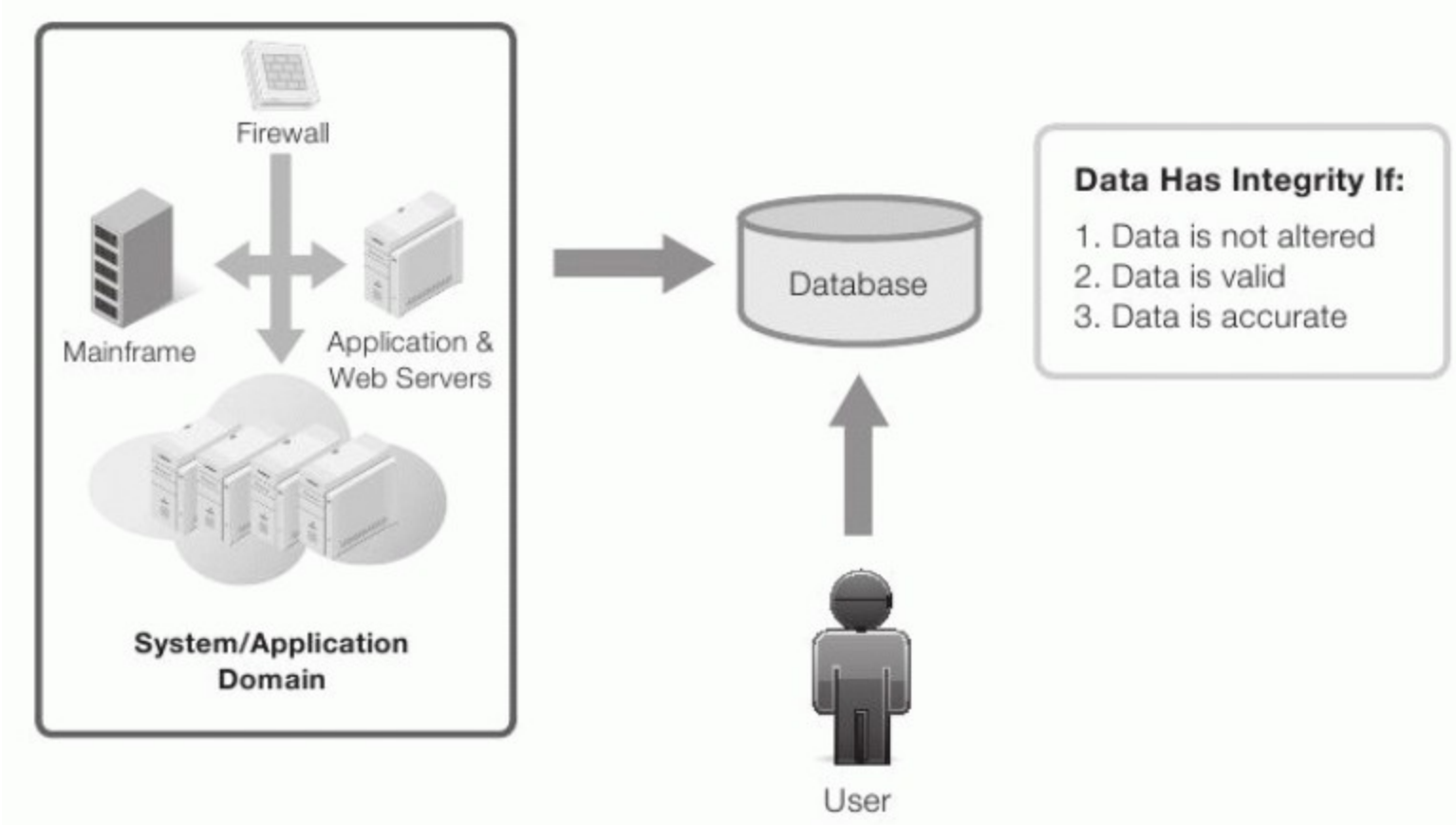


Three tenets of Information Systems Security

- **Availability** – Information must be available to authorized users when available
  - Uptime, downtime, availability, mean time to failure, mean time to repair,...
- **Integrity** – Only authorized users can access and change information
- **Confidentiality** – Only authorized users can see sensitive information

Three tenets of Information Systems Security

- Data integrity



Seven Domains of a Typical IT Infrastructure

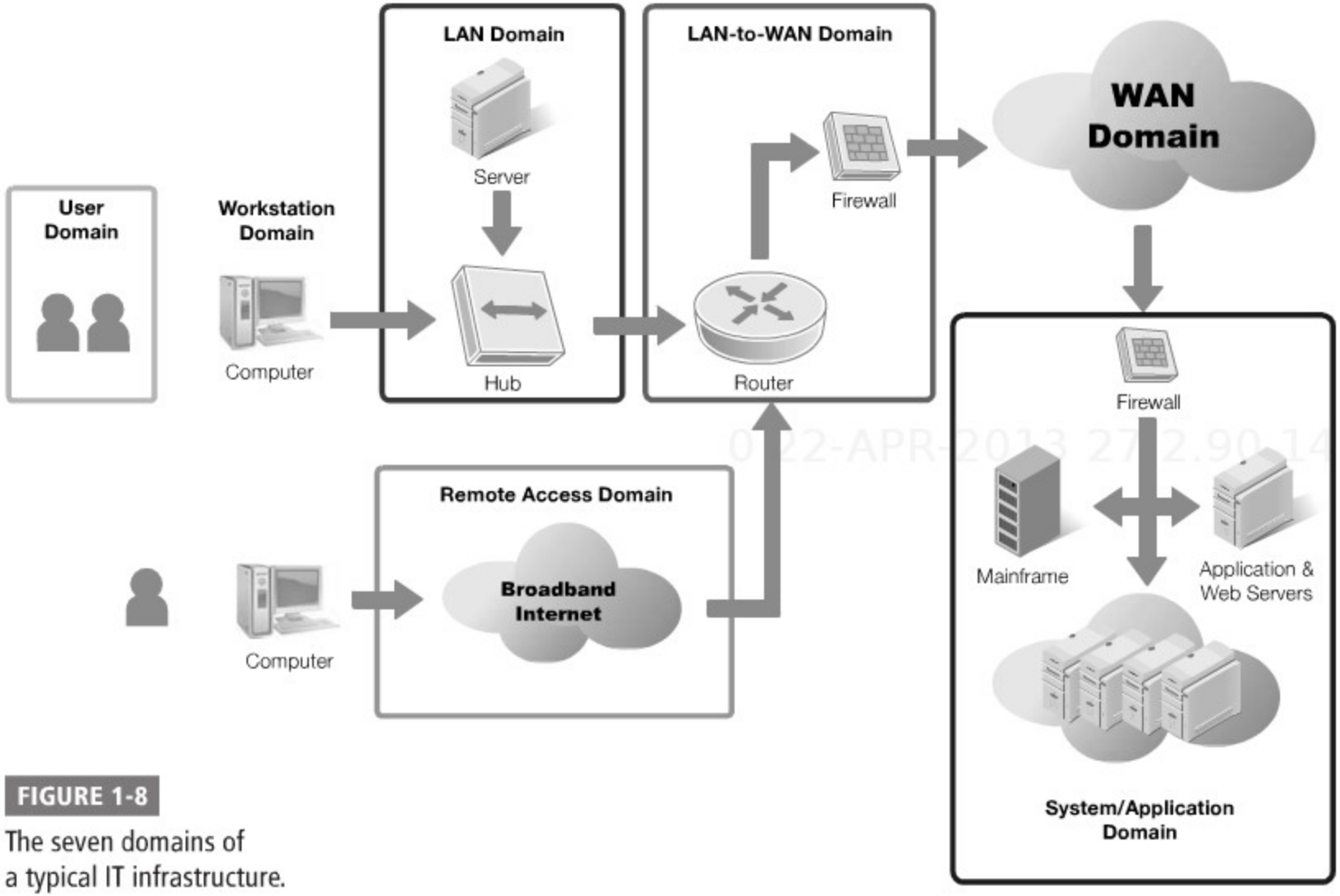


FIGURE 1-8

The seven domains of a typical IT infrastructure.

Seven Domains of a Typical IT Infrastructure

- **User Domain** - defines the people who access an organization's information system
- **Workstation Domain** - is where most users connect to the IT infrastructure. It can be a desktop computer, or any device that connects to your network.
- **LAN Domain** - is a collection of computers connected to one another or to a common connection medium. Network connection mediums can include wires, fiber optic cables, or radio waves.

- **LAN-to-WAN Domain** - is where the IT infrastructure links to a wide area network and the Internet.
- **WAN Domain** - connects remote locations. WAN services can include dedicated Internet access and managed services for customer's routers and firewalls.
- **Remote Access Domain** - connect remote users to the organization's IT infrastructure. The scope of this domain is limited to remote access via the Internet and IP communications.
-

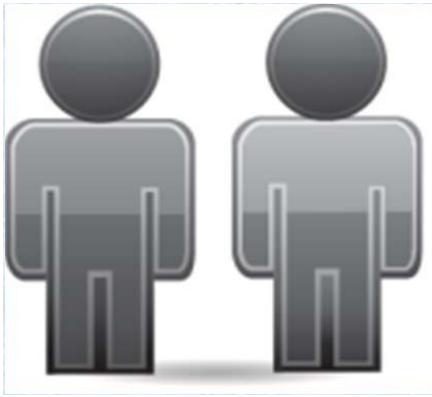
- **System Application Domain** - holds all the mission-critical systems, applications, and data.

Seven Domains of a Typical IT Infrastructure

- For each domain
  - Roles and tasks
  - Responsibilities
  - Accountability

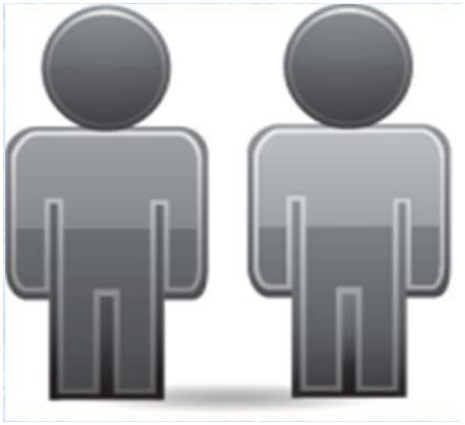
Common Threats in the User Domain

- Lack of user awareness
- User apathy toward policies
- User violating security policy
- User inserting CD/DVD/USB with personal files
- User access to media with questionable lineage (inserting, copying)



Common Threats in the User Domain

- User downloading photos, music, or videos
- User destructing systems, applications, and data
- Disgruntled employee attacking organization or committing sabotage
- Employee blackmail or extortion



Common Threats in the Workstation Domain

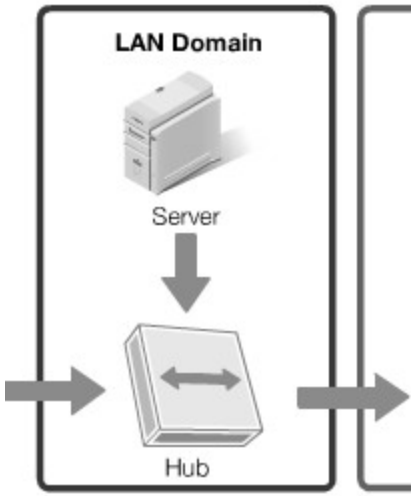
- Unauthorized workstation access
- Unauthorized access to systems, applications,
- and data
- Desktop or laptop operating system vulnerabilities
- Desktop or laptop application software vulnerabilities or patches
-

Common Threats in the Workstation Domain

- Viruses, malicious code, and other malware
- User inserting CD/DVD/USB into organization computer
- User downloading photos, music, or videos via Internet

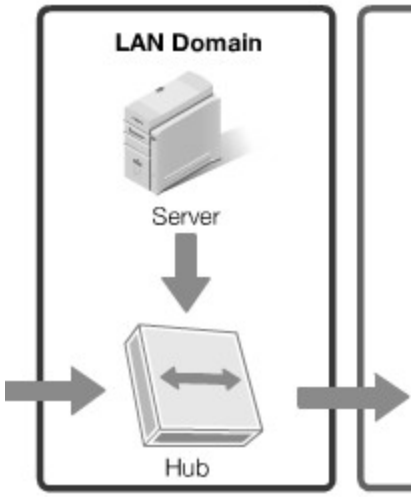
Common Threats in the LAN Domain

- Unauthorized physical access to LAN
- Unauthorized access to systems, applications, and data
- LAN server operating system vulnerabilities
- LAN server application software vulnerabilities and software patch updates
-



Common Threats in the LAN Domain

- Rogue users on WLANs
- Confidentiality of data on WLANs
- LAN servers have different hardware, OS and softwares, making it difficult to manage and troubleshoot



Common Threats in the LAN-to-WAN Domain

- Unauthorized probing and port scanning
- Unauthorized access
- Internet Protocol (IP) router, firewall, and network appliance operating system vulnerability
- IP router, firewall, and network appliance configuration file errors or weakness
- Remote users can access the organization's infrastructure and download sensitive data
- Local users downloading unknown file types from unknown sources (surfing) WAN
- Accessing malicious web sites

Common threats in WAN domain

- Open, public, easily accessible to anyone that wants to connect
- Most Internet traffc is sent in cleartext.
- Vulnerable to eavesdropping
- Vulnerable to malicious attacks
- Vulnerable to denial of service (DoS), distributed denial of service (DDoS), TCP SYN fooding, and IP spoofng attacks
- Vulnerable to corruption of information and data
- TCP/IP applications are inherently insecure (HTTP, FTP, TFTP, etc.).

Threats in Remote Access Domain

- Brute-force user ID and password attacks
- Multiple logon retries and access control attacks
- Unauthorized remote access to IT systems, applications, and data
- Private data or confdential data is compromised remotely.
- Data leakage in violation of existing data classifcation standards
- Mobile worker laptop is stolen
- Mobile worker token or other authentication are stolen

Threats in System/Application Domain

- Unauthorized access to data centers, computer rooms, and wiring closets
- Servers must sometimes be shutdown to perform maintenance.
- Cloud computing virtual environments are by default not secure.
- Client-server and Web applications are susceptible to attack.
- Unauthorized accessed to systems.
- Private data is compromised.

Threats in System/Application Domain

- Data is corrupted or lost.
- Backed-up data may be lost as backup media is reused.
- Recovering critical business functions may take too long to be useful.
- IT systems may be down for an extended period after a disaster.

IT Security Policy Framework

- An IT security policy framework contains four main components:
  - Policy
  - Standard
  - Procedures
  - Guidelines

IT Security Policy Framework

- **Policy**—A policy is a short written statement that the people in charge of an organization have set as a course of action or direction. A policy comes from upper management and applies to the entire organization.
- **Standard**—A standard is a detailed written defnition for hardware and software and how it is to be used. Standards ensure that consistent security controls are used throughout the IT system.

IT Security Policy Framework

- **Procedures**—These are written instructions for how to use policies and standards. They may include a plan of action, installation, testing, and auditing of security controls.
- **Guidelines**—A guideline is a suggested course of action for using the policy, standards, or procedures. Guidelines can be specifc or fexible regarding use.

Data Classifcation Standards

- The goal and objective of a data classifcation standard is to provide a consistent defnition for how an organization should handle and secure different types of data
- Typically include the following major categories:
  - Private data
  - Confidential
  - Internal used only
  - Public domain data

Summary

- Introducing information systems security and the system security profession
- A common definition of a typical IT infrastucture
- Risks, threats and vulnerabilities within the seven domains. Each of these domains requires the use of strategies to reduce risks, threats and vulnerabilities
- IT security framework
- Data classification standards provide organization with a roadmap for how to handle different types of data

Thank You!