Introduction To Information Systems Security

Contents

- History of information security.
- Information Systems Security.
- Risks, Threats, and Vulnerabilities.
- Tenets of Information Systems Security.
- The Seven Domains of a Typical IT Infrastructure.

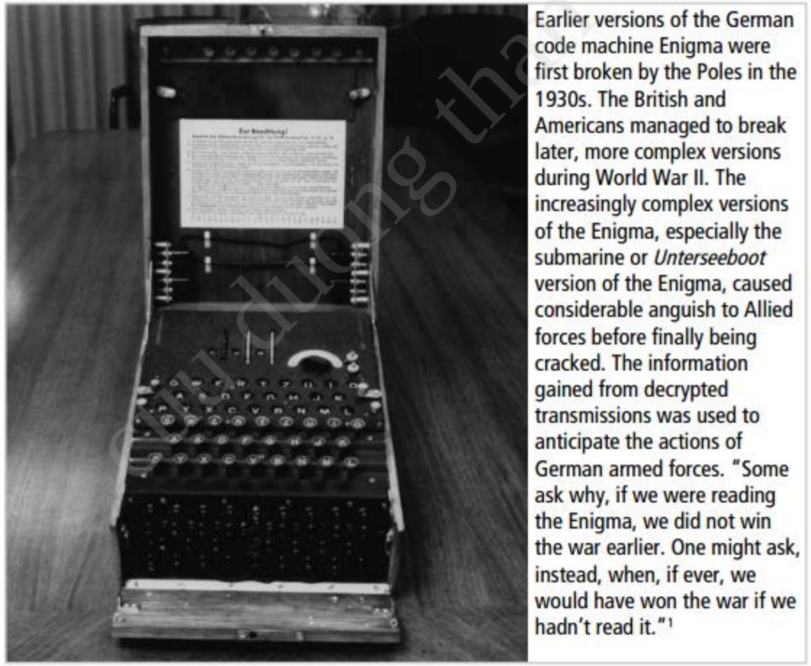
1. History of information security

History of information security

- The 1960s
- The 1970s and 80s
- The 1990s
- 2000 to Present

History of information security (cont.)

- The history of information security begins with **computer security**
- Secure physical locations, hardware, and software from threats



Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."[1]

Figure 1-1 The Enigma

History of information security (cont.)

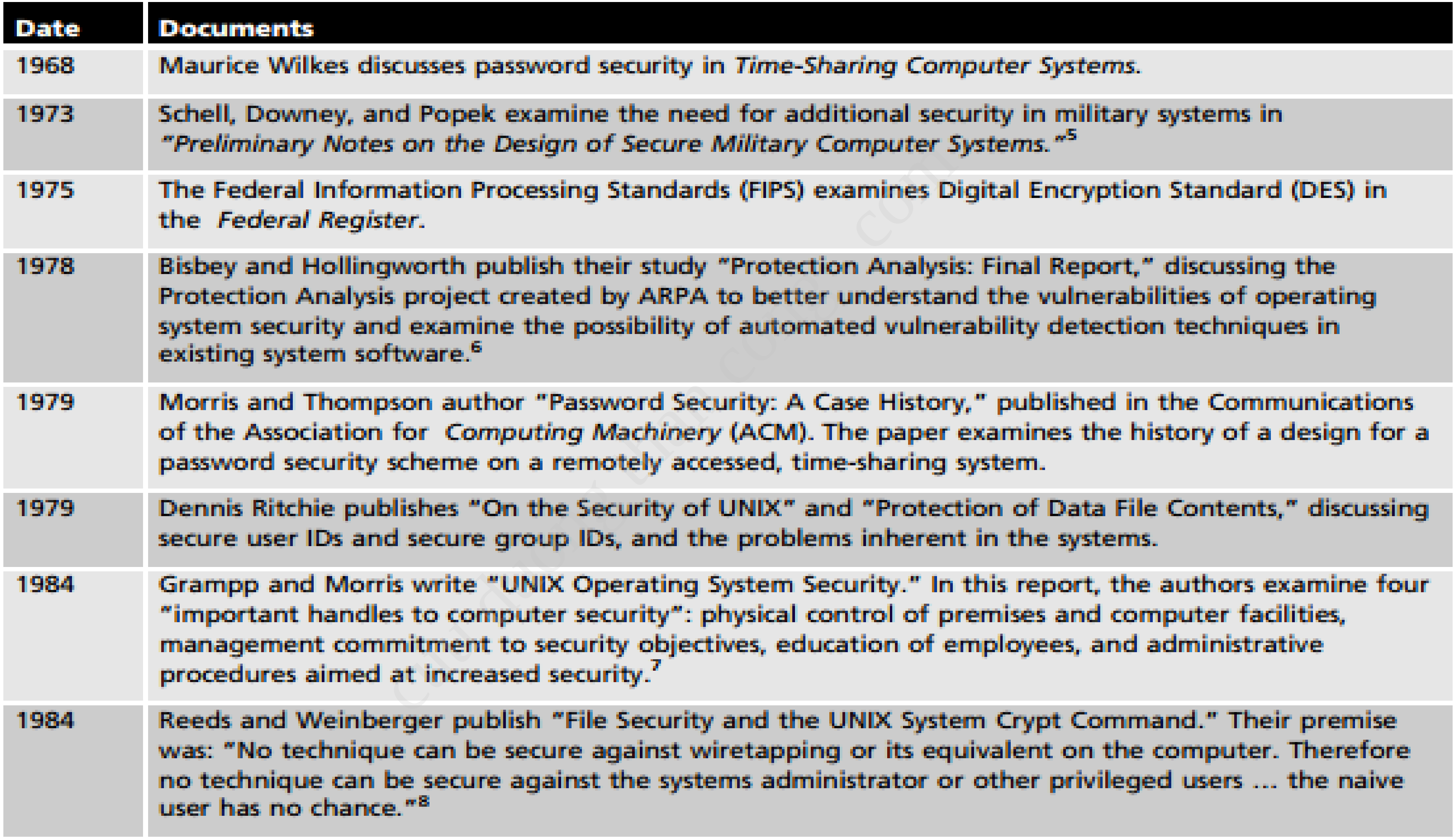
The 1960s:

- During the Cold War, many more mainframes were brought online to accomplish more complex and sophisticated tasks.
- Larry Roberts, known as the founder of the Internet, developed the project which was called ARPANET

History of information security (cont.)

The 1970s and 80s: Network security

- ARPANET became popular and more widely used, and the potential for its misuse grew:
  - protect data from unauthorized remote users
  - lack of safety procedures for dial-up connections
  - nonexistent user identification and authorization to the system



Date	Documents
1968	Maurice Wilkes discusses password security in *Time-Sharing Computer Systems*.
1973	Schell, Downey, and Popek examine the need for additional security in military systems in *"Preliminary Notes on the Design of Secure Military Computer Systems."*[5]
1975	The Federal Information Processing Standards (FIPS) examines Digital Encryption Standard (DES) in the *Federal Register*.
1978	Bisbey and Hollingworth publish their study "Protection Analysis: Final Report," discussing the Protection Analysis project created by ARPA to better understand the vulnerabilities of operating system security and examine the possibility of automated vulnerability detection techniques in existing system software.[6]
1979	Morris and Thompson author "Password Security: A Case History," published in the Communications of the Association for *Computing Machinery* (ACM). The paper examines the history of a design for a password security scheme on a remotely accessed, time-sharing system.
1979	Dennis Ritchie publishes "On the Security of UNIX" and "Protection of Data File Contents," discussing secure user IDs and secure group IDs, and the problems inherent in the systems.
1984	Grampp and Morris write "UNIX Operating System Security." In this report, the authors examine four "important handles to computer security": physical control of premises and computer facilities, management commitment to security objectives, education of employees, and administrative procedures aimed at increased security.[7]
1984	Reeds and Weinberger publish "File Security and the UNIX System Crypt Command." Their premise was: "No technique can be secure against wiretapping or its equivalent on the computer. Therefore no technique can be secure against the systems administrator or other privileged users ... the naive user has no chance."[8]

Table 1-1 Key Dates for Seminal Works in Early Computer Security

History of information security (cont.)

The 1990s:

- The Internet has become an interconnection of millions of networks
- Industry standards for interconnection of networks: **de facto standards**
- e-mail encryption

History of information security (cont.)

2000 to Present

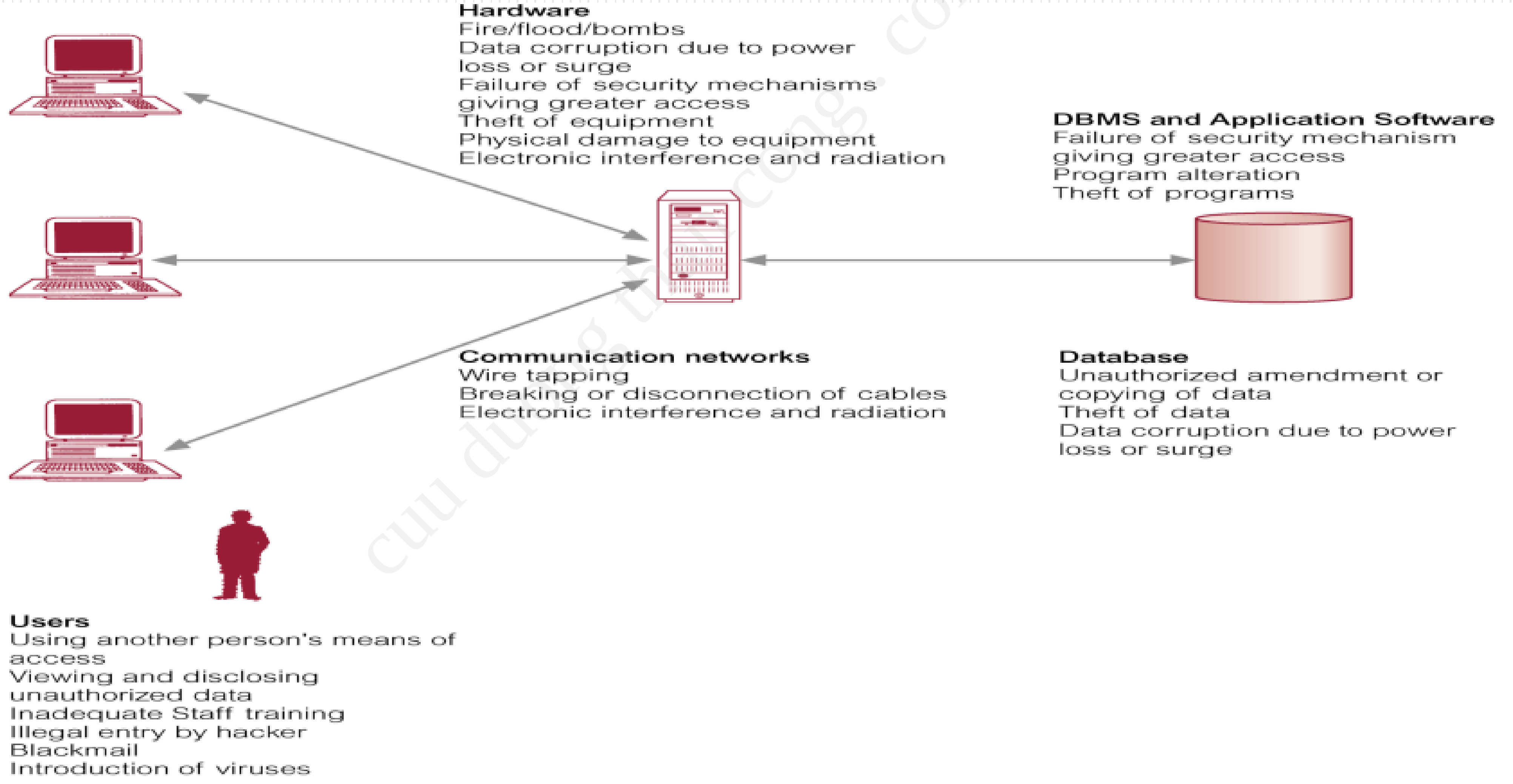
- Today, the Internet brings millions of unsecured computer networks into continuous communication with each other.
- Security?

2. Information Systems Security

Information system

- 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.

The Components of Information Systems



Hardware
Fire/flood/bombs
Data corruption due to power loss or surge
Failure of security mechanisms giving greater access
Theft of equipment
Physical damage to equipment
Electronic interference and radiation

DBMS and Application Software
Failure of security mechanism giving greater access
Program alteration
Theft of programs

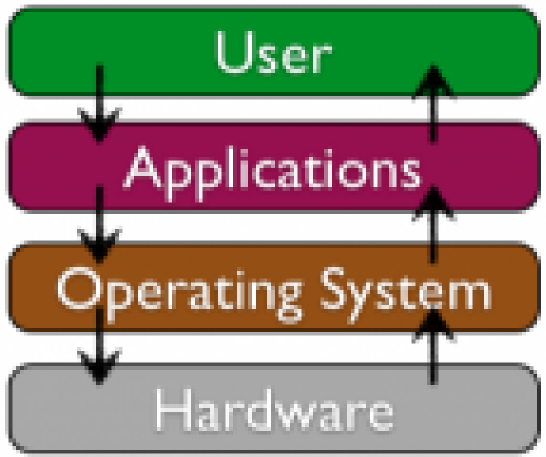
Communication networks
Wire tapping
Breaking or disconnection of cables
Electronic interference and radiation

Database
Unauthorized amendment or copying of data
Theft of data
Data corruption due to power loss or surge

Users
Using another person's means of access
Viewing and disclosing unauthorized data
Inadequate Staff training
Illegal entry by hacker
Blackmail
Introduction of viruses

The Components of Information Systems

- **Hardware:** Information systems hardware is the part of an information system you can touch – the physical components of the technology. Computers, keyboards, disk drives, network devices.
- **Software:** is a set of instructions that tells the hardware what to do. Software is not tangible – it cannot be touched.
  - Applications,
  - Operating systems



The Components of Information Systems

- **Data:** as a collection of facts. For example, your street address, the city you live in, and your phone number are all pieces of data. Like software, data is also intangible.
- **People:** help-desk workers, systems analysts, programmers. The people involved with information systems are an essential element

The Components of Information Systems

- **Procedures:** Procedures are written instructions for accomplishing a specific task.
- **Networks**: A network is a connected collection of devices that can communicate with each other

Information systems security

- Information systems security is the collection of activities that protect the information system and the data stored in it

3. Risk, Threat, and Vulnerabilitie

Risk

- Risk is the likelihood that something bad will happen to an asset.
- In the context of IT security, an asset can be a computer, a database, or a piece of information.

Examples:

- Losing data
- Losing business because a disaster has destroyed your building
- Failing to comply with laws and regulations

Threat

- A threatis any action that could damage an asset.
- Information systems face both natural and human-induced threats

Examples:

- Flood, earthquake, fire, …
- Virus, DDOS

The most common threats

- Malicious software
- Hardware or software failure
- Internal attacker
- Equipment theft
- External attacker
- Natural disaster
- Industrial espionage
- Terrorism

Threat Types

- **Disclosure threats**: occurs any time unauthorized users access private or confidential information that is stored on a network resource or while it is in transit between network resources.

Two techniques

- Sabotage: the destruction of property or obstruction of normal operations
- Espionage: the act of spying to obtain secret information

Threat Types (cont.)

- Alteration threats: making unauthorized changes to data on a system
- Example: modify database files, operating systems, application software, and even hardware devices

Threat Types (cont.)

- Denial or Destruction Threats: Denial or destruction threats make assets or resources unavailable or unusable.
- Example: DOS/DDOS

Vulnerability

- A vulnerabilityis a weakness that allows a threat to be realized or to have an effect on an asset.

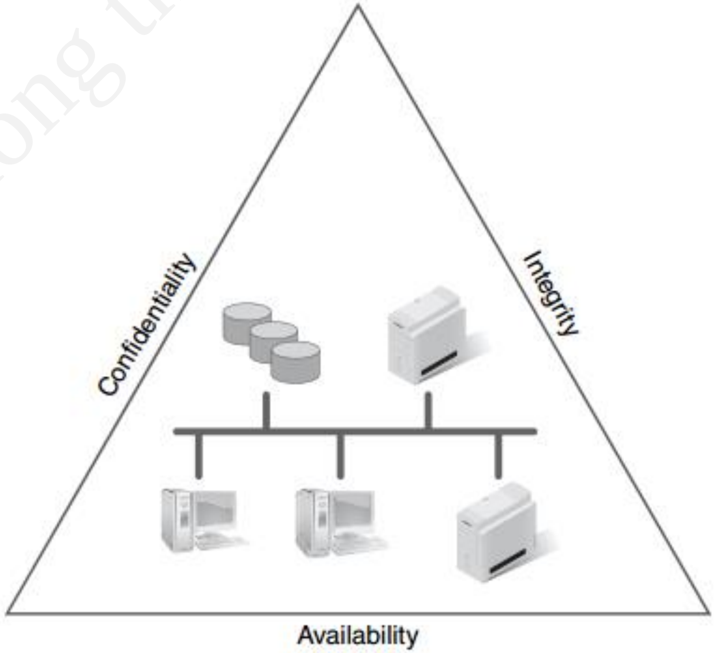
Examples:

- Buffer overflow.
- IIS Error

3. Tenets of Information Systems Security

2. Tenets of Information Systems Security

- **Confidentiality**: Only authorized users can view information.
- **Integrity**: Only authorized users can change information.
- **Availability**: Information is accessible by authorized users whenever they request the information.



a) Confidentiality

- Confidential information includes the following:
  - ❑Private data of individuals (Full name, Mailing address, Date of birth, …)
  - ❑Intellectual property of businesses
  - ❑National security for countries and governments

- Security control: is something an organization does to help reduce risk.

Security control

Example:

- Conducting annual security awareness training for employees
- where security controls should be used
- Designing a layered security solution for an IT infrastructure
- Performing periodic security risk assessments, audits, and penetration tests on websites and IT infrastructure.
- Enabling security incident and event monitoring at your Internet entry and exit points

Security control

Example (cont):

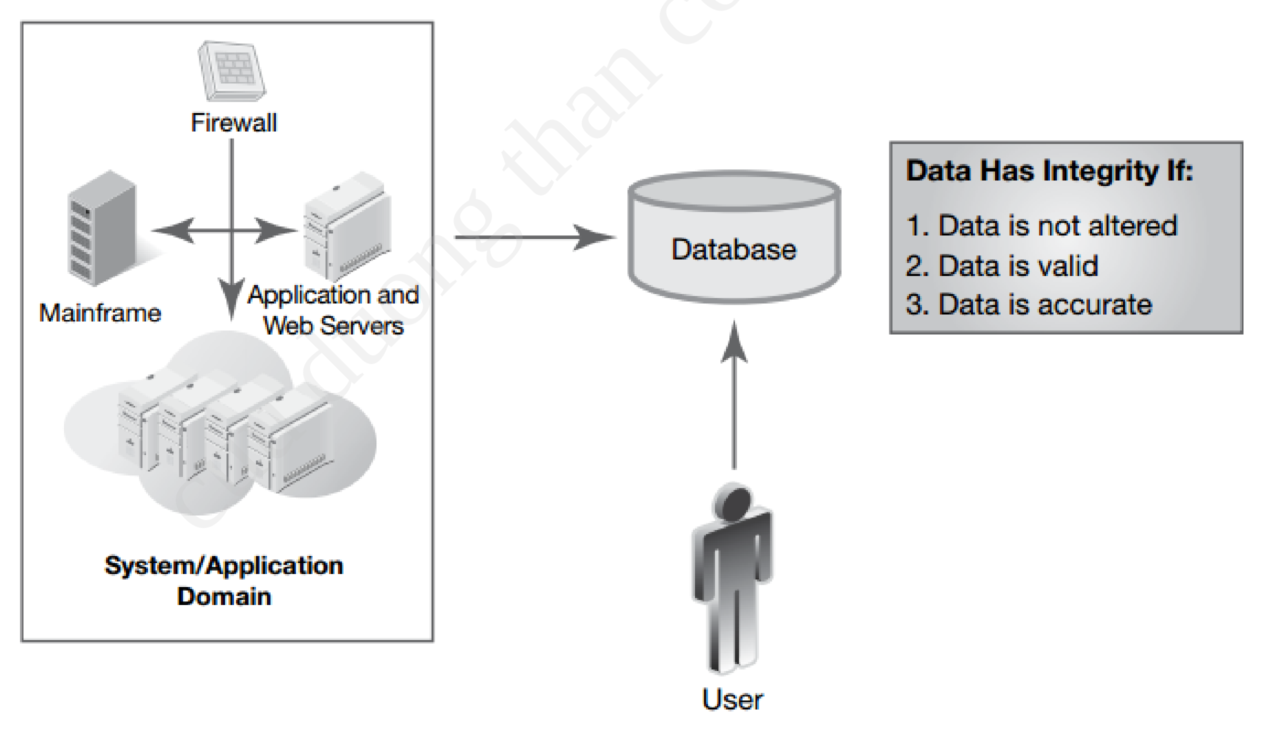
- Using automated workstation and server antivirus and malicious software protection.
- Using access control.

Ensuring data confidentiality

- Defining policies, standards, procedures, and guidelines to protect confidential data.
- Access control.
- Using cryptography techniques.
- Encrypting data that cross the public Internet.
- Encrypting data that are stored within databases and storage devices.

b) Integrity

- Integrity deals with the validity and accuracy of data.
- Ensuring data cannot be altered by unauthorized people.



Data Has Integrity If:

1. Data is not altered
2. Data is valid
3. Data is accurate

Ensuring data integrity

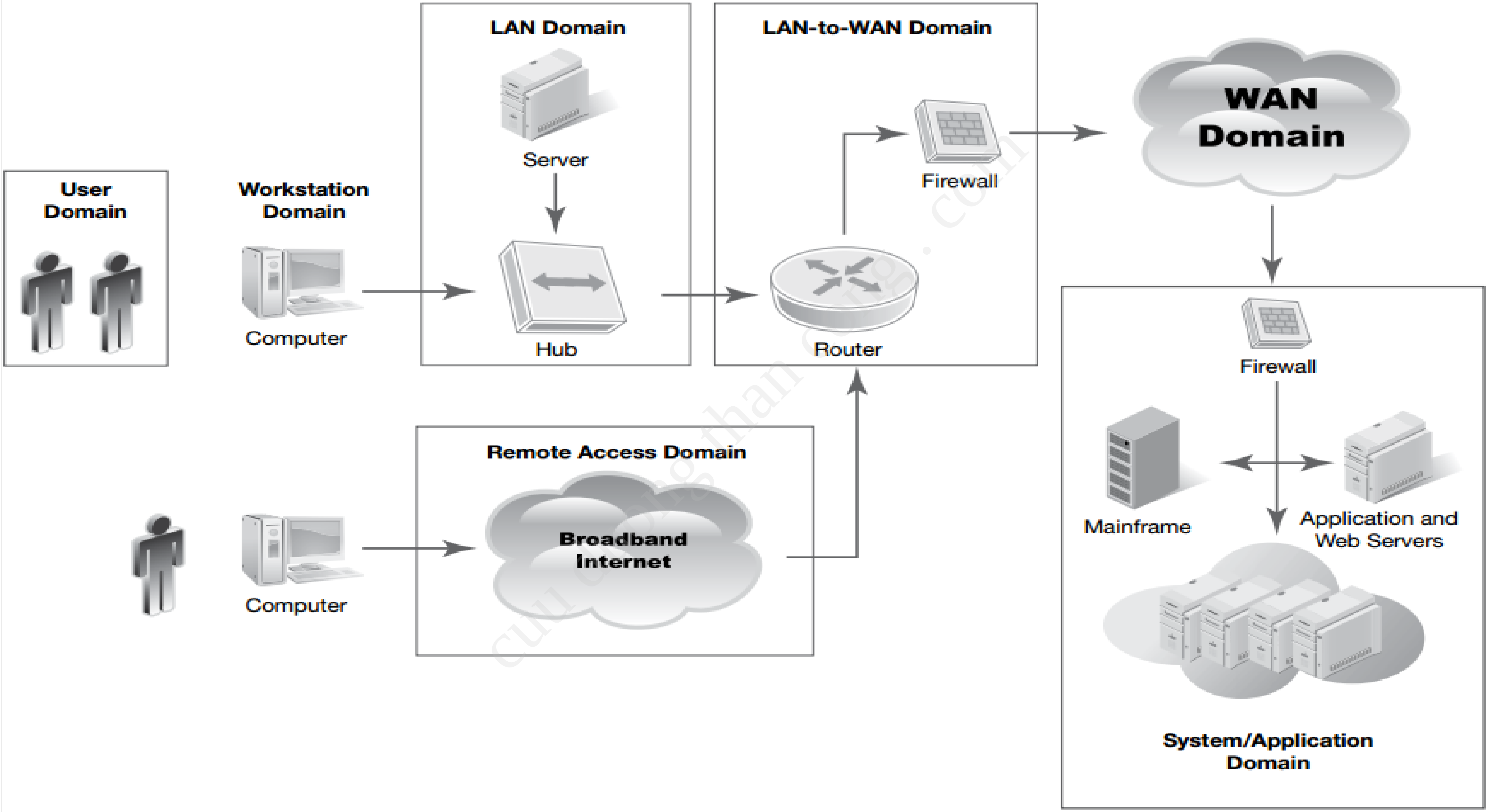
- Digital signature.
- Hashing.
- Access Control.
- Authentication protocols

c) Available

Common availability time measurements include the following:

- Uptime: is the total amount of time that a system, application, and data are accessible
- Downtime: is the total amount of time that a system, application, and data are not accessible.
- Availability: A = (Total Uptime) / (Total Uptime + Total Downtime).

4. The Seven Domains of a Typical IT Infrastructure


LAN Domain
LAN-to-WAN Domain
WAN Domain
User Domain
Workstation Domain
Server
Firewall
Hub
Router
Computer
Firewall
Remote Access Domain
Broadband Internet
Computer
Mainframe
Application and Web Servers
System/Application Domain

a) User Domain

- The User Domain defines the people who access an organization’s information system.
- **Roles and tasks:** Users can access systems, applications, and data depending upon their defined access rights. Employees must conform to the staff manual and policies

Risks, Threats, and Vulnerabilities in the User Domain

RISK, THREAT, OR VULNERABILITY	MITIGATION
Unauthorized access	Conduct security awareness training
Lack of user awareness	Conduct security awareness training
User apathy toward policies	Conduct annual security awareness training
User insertion of CDs and USB drives with personal photos, music, and videos	Disable internal CD drives and USB ports. Enable automatic antivirus scans for inserted media drives, files, and email attachments
User downloads of photos, music, and videos	Enable content filtering and antivirus canning for email attachments. Content-filtering network devices are configured to permit or deny specific domain names in accordance with AUP definitions

Risks, Threats, and Vulnerabilities in the User Domain

RISK, THREAT, OR VULNERABILITY	MITIGATION
User destruction of systems, applications, or data	Restrict users’ access to only those systems, applications, and data needed to perform their jobs. Minimize write/delete permissions to the data owner only
Attacks on the organization or acts of sabotage by disgruntled employees	Track and monitor abnormal employee behavior, erratic job performance, and use of IT infrastructure during off-hours. Begin IT access control lockout procedures based on AUP monitoring and compliance
Employee blackmail	Track and monitor abnormal employee behavior and use of IT infrastructure during off-hours. Enable intrusion detection system/intrusion prevention system (IDS/IPS) monitoring for sensitive employee positions and access.

b) Workstation Domain

- A workstationcan be a desktop computer, a laptop computer, a special-purpose terminal, or any other device that connects to your network.
- **Roles and tasks:** configuring hardware, hardening systems, and verifying antivirus files

Risks, Threats, and Vulnerabilities in the Workstation Domain

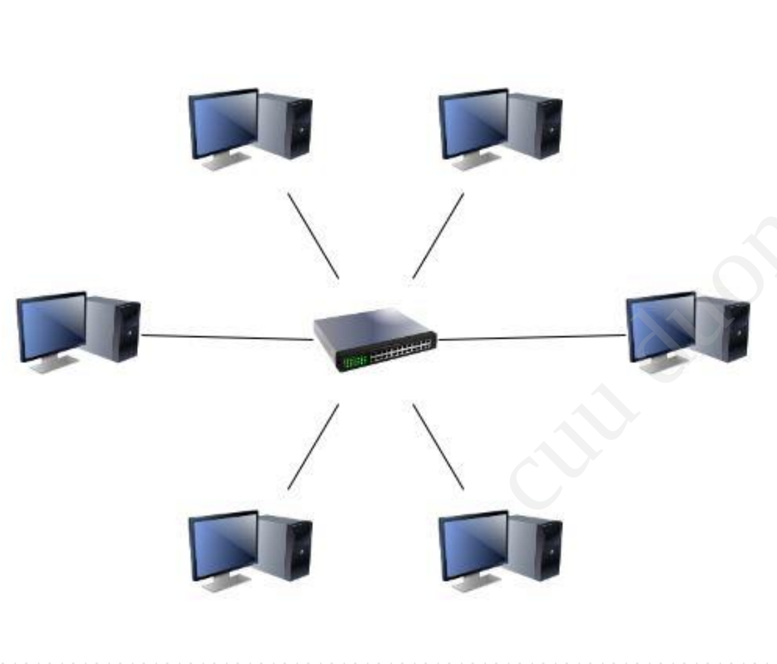
RISK, THREAT, OR VULNERABILITY	MITIGATION
Unauthorized access to workstation	Enable password protection on workstations for access.
Unauthorized access to systems, applications, and data	Define strict access control policies, standards, procedures, and guidelines
Desktop or laptop computer operating system software vulnerabilities and software patch updates	Define a workstation operating system vulnerability window policy and standard. Update application software
Infection of a user's workstation or laptop computer by viruses, malicious code, or malware	Use workstation antivirus and malicious code policies, standards, procedures, and guidelines

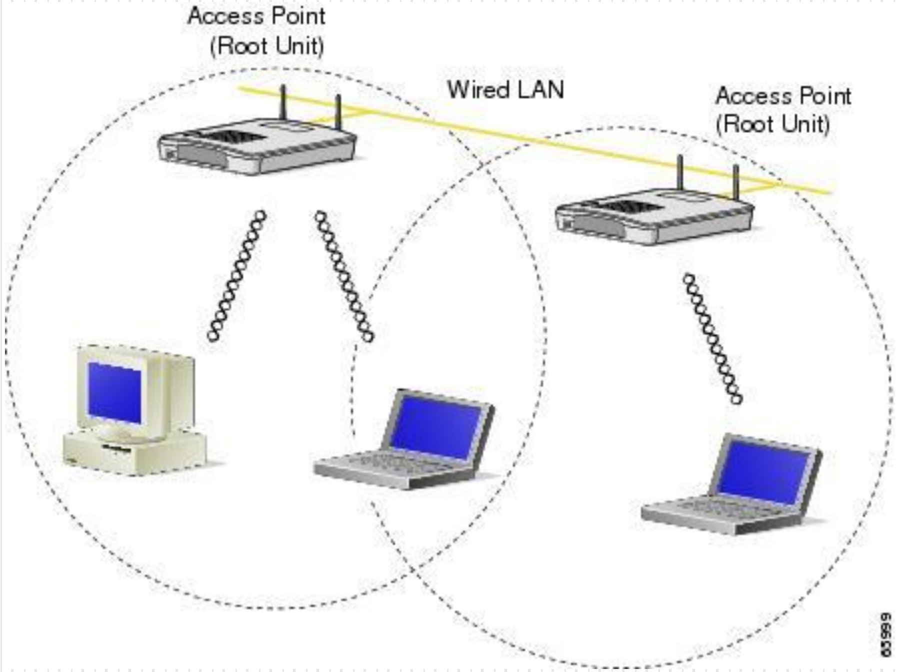
Risks, Threats, and Vulnerabilities in the Workstation Domain

RISK, THREAT, OR VULNERABILITY	MITIGATION
User downloads of photos, music, or videos via the Internet	Use content filtering and antivirus scanning at Internet entry and exit.
User insertion of CDs, digital video discs (DVDs), or universal serial bus (USB) thumb drives into the organization’s computers	Deactivate all CD, DVD, and USB ports. Enable automatic antivirus scans for inserted CDs, DVDs, and USB thumb drives that have files.

LAN Domain

- A local area network (LAN)is a collection of computers connected to one another or to a common connection medium.





LAN Domain

Roles and tasks:

Management of the physical components includes:

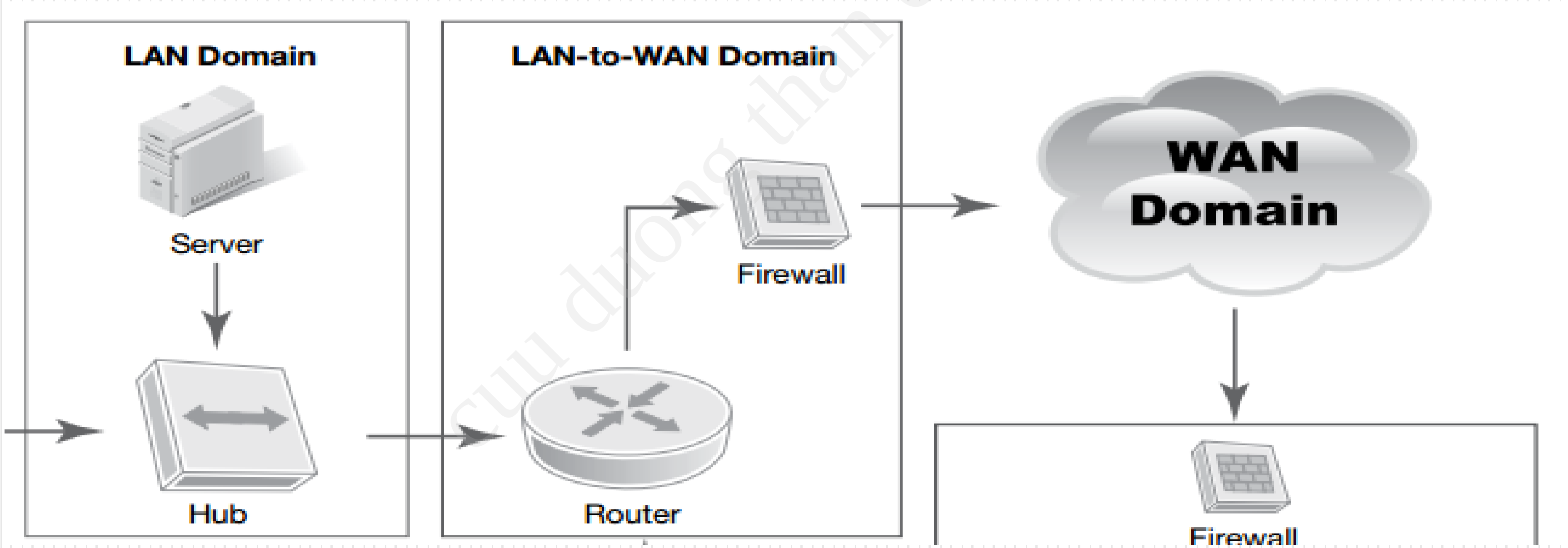
- Cabling
- NICs
- LAN switches
- Wireless access points (WAPs)

Risks, Threats, and Vulnerabilities Commonly Found in the LAN Domain

RISK, THREAT, OR VULNERABILITY	MITIGATION
Unauthorized access to LAN	Computer rooms are secure.
Unauthorized access to systems, applications, and data	Access control policies. read/write/delete privileges on specific documents
LAN server operating system software vulnerabilities	vulnerability assessments
LAN server application software vulnerabilities and software patch updates	software patching
Unauthorized access WLANs	Access control
Compromised confidentiality of data transmissions via WLAN	Implement encryption between workstation and WAP to maintain confidentiality.

LAN-to-WAN Domain

- The LAN-to-WAN Domain is where the IT infrastructure links to a wide area network and the Internet



LAN-to-WAN Domain

- Transmission Control Protocol (TCP).
- User Datagram Protocol (UDP).
- Both TCP and UDP use port numbers to identify the application or function

LAN-to-WAN Domain

- Roles and tasks:
  - Routers: routing, access control lists.
  - Firewalls: Packet filtering
  - Demilitarized zone (DMZ): web, proxy, email servers
  - Intrusion detection system (IDS)
  - Intrusion prevention system (IPS)

Risks, Threats, and Vulnerabilities Commonly Found in the LAN-to-WAN Domain

RISK, THREAT, OR VULNERABILITY	MITIGATION
Unauthorized network probing and port scanning	Disable ping. IDS/IPS
DOS/DDOS attack	?
IP router, firewall, and network appliance operating system software vulnerability	vulnerability assessments
LAN server application software vulnerabilities and software patch updates	update devices
IP router, firewall, and network appliance configuration file errors or weaknesses	Firewall, Encryption
Unknown email attachments and embedded URL links received by local users	Antivirus, Conduct security awareness training

WAN Domain

- The Wide Area Network (WAN) Domain connects remote locations.
- Roles and tasks:
  - WAN communication links
  - IP network design
  - Firewall
  - router configuration
  - VPNs, SNMP

Risks, Threats, and Vulnerabilities Commonly Found in the WAN Domain

RISK, THREAT, OR VULNERABILITY	MITIGATION
Most Internet traffic sent in cleartext	Use encryption and VPN tunnels
DOS/DDOS attack	?
Vulnerable to eavesdropping	Use encryption and VPN tunnels
Vulnerable to malicious attacks	IDS/IPS
Vulnerable to corruption of information and data	Use encryption and VPN tunnels

Remote Access Domain

- The Remote Access Domain connects remote users to the organization’s IT infrastructure.
- Roles and tasks:
  - Laptop VPN client software
  - Secure browser software
  - Cell phones, smartphones
  - VPN routers, VPN firewalls
  - Secure Sockets Layer (SSL)/VPN web server

Risks, Threats, and Vulnerabilities Commonly Found in the Remote Access Domain

RISK, THREAT, OR VULNERABILITY	MITIGATION
Brute-force user ID and password attacks	Password policies
Unauthorized remote access to IT systems, applications, and data	?
A mobile worker’s laptop is stolen	Multi-factor authentication
Private data or confidential data compromised remotely	Encrypt all private data within the database or hard drive

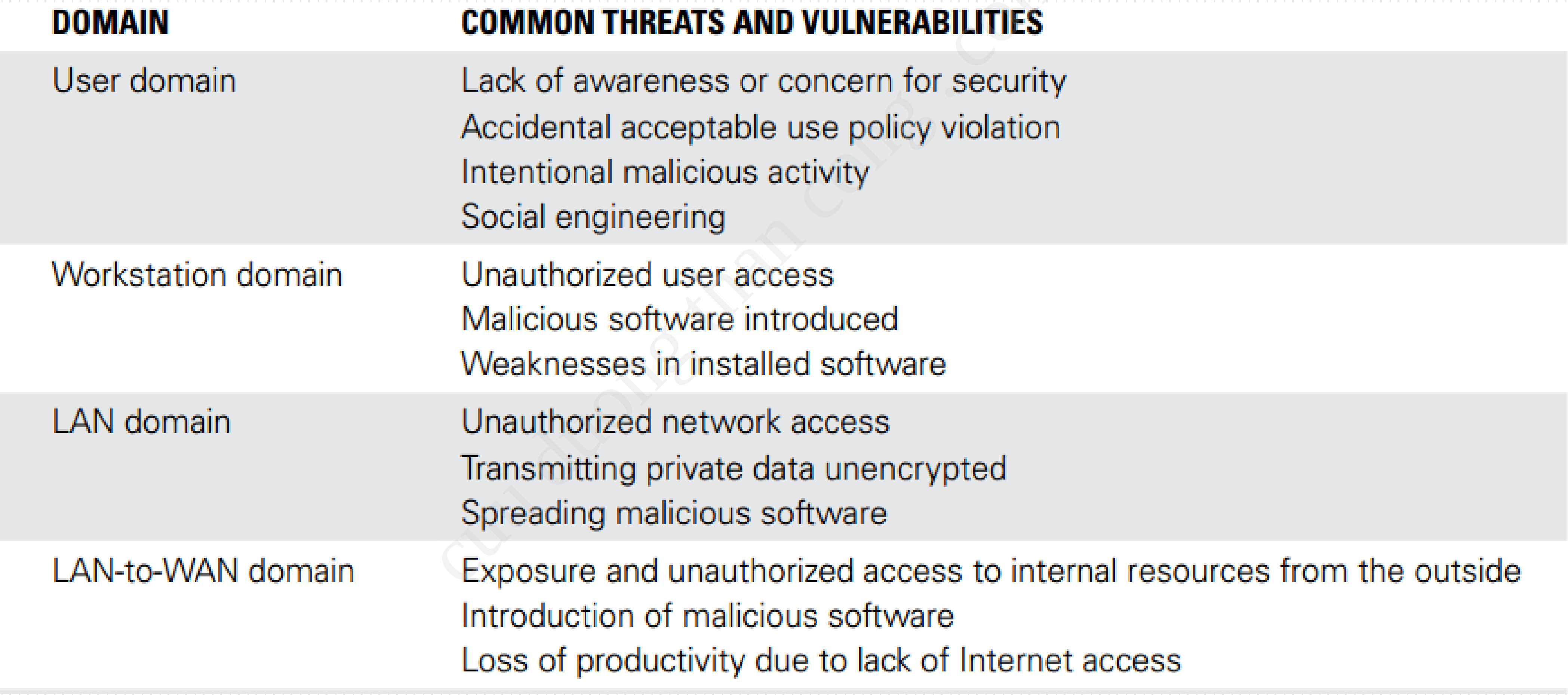
System/Application Domain

- The System/Application Domain holds all the mission-critical systems, applications, and data
- Roles and tasks: The System/Application Domain consists of hardware, operating system software, applications, and data

RISK, THREAT, OR VULNERABILITY

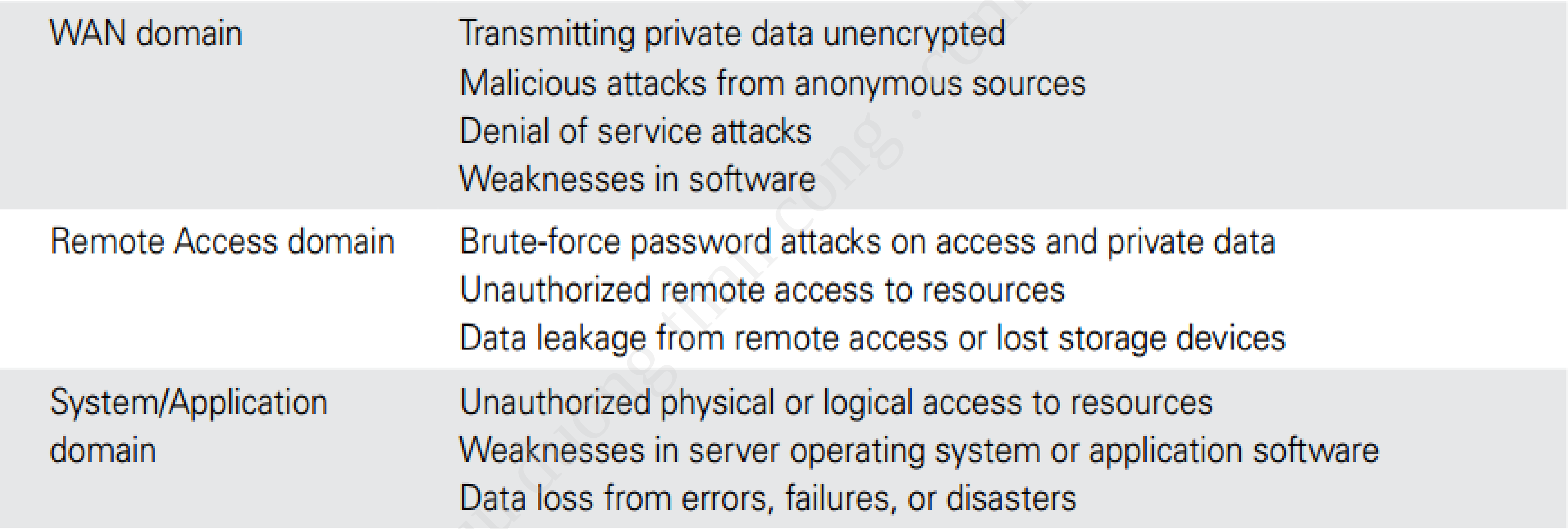
RISK, THREAT, OR VULNERABILITY	MITIGATION
Unauthorized access to data centers, computer rooms, and wiring closets	Password policies
Downtime of servers to perform maintenance	?
Loss or corruption of data	Backup
Server operating systems software vulnerability	update

Common threats and vulnerabilities in the seven domains of an IT infrastructure



DOMAIN	COMMON THREATS AND VULNERABILITIES
User domain	Lack of awareness or concern for security Accidental acceptable use policy violation Intentional malicious activity Social engineering
Workstation domain	Unauthorized user access Malicious software introduced Weaknesses in installed software
LAN domain	Unauthorized network access Transmitting private data unencrypted Spreading malicious software
LAN-to-WAN domain	Exposure and unauthorized access to internal resources from the outside Introduction of malicious software Loss of productivity due to lack of Internet access

Common threats and vulnerabilities in the seven domains of an IT infrastructure



WAN domain	Transmitting private data unencrypted Malicious attacks from anonymous sources Denial of service attacks Weaknesses in software
Remote Access domain	Brute-force password attacks on access and private data Unauthorized remote access to resources Data leakage from remote access or lost storage devices
System/Application domain	Unauthorized physical or logical access to resources Weaknesses in server operating system or application software Data loss from errors, failures, or disasters

Thanks