Computer Security

Computer Security

(defined)

Computer security, also known as **cybersecurity** or **IT security**, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures. (Wikipedia)

Computer Security

(n.) In the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system. *(Vangie Beal - Webopedia)*

The protection of data, networks and computing power. The protection of data (information security) is the most important. The protection of networks is important to prevent loss of server resources as well as to protect the network from being used for illegal purposes. The protection of computing power is relevant only to expensive machines such as large supercomputers.(PC Magazine)

Computer Security: A Practical Definition

Defining "computer security" is not trivial. The difficulty lies in developing a definition that is broad enough to be valid regardless of the system being described, yet specific enough to describe what security really is. In a generic sense, security is "freedom from risk or danger." In the context of computer science, security is the prevention of, or protection against,

access to information by unauthorized recipients, and

intentional but unauthorized destruction or alteration of that information[1]

This can be re-stated: "Security is the ability of a system to protect information and system resources with respect to confidentiality and integrity." Note that the scope of this second definition includes system resources, which include CPUs, disks, and programs, in addition to information.

1. *Dictionary of Computing,* Fourth Ed. (Oxford: Oxford University Press, 1996).
2. Bryan Pfaffenberger, *Webster's New World Dictionary of Computing Terms,* Sixth Ed. (New York: Simon and Schuster, 1997).

Computer Security

The NIST *Computer Security Handbook* defines the term computer security as:

“the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources” (includes hardware, software, firmware, information/data, and telecommunications)

***C**onfidentiality

***I**ntegrity

***A**vailability

Who Implements....

Confidentiality

- User
- IT administrator
- Network administrator
- Human resources
- Senior management

Integrity

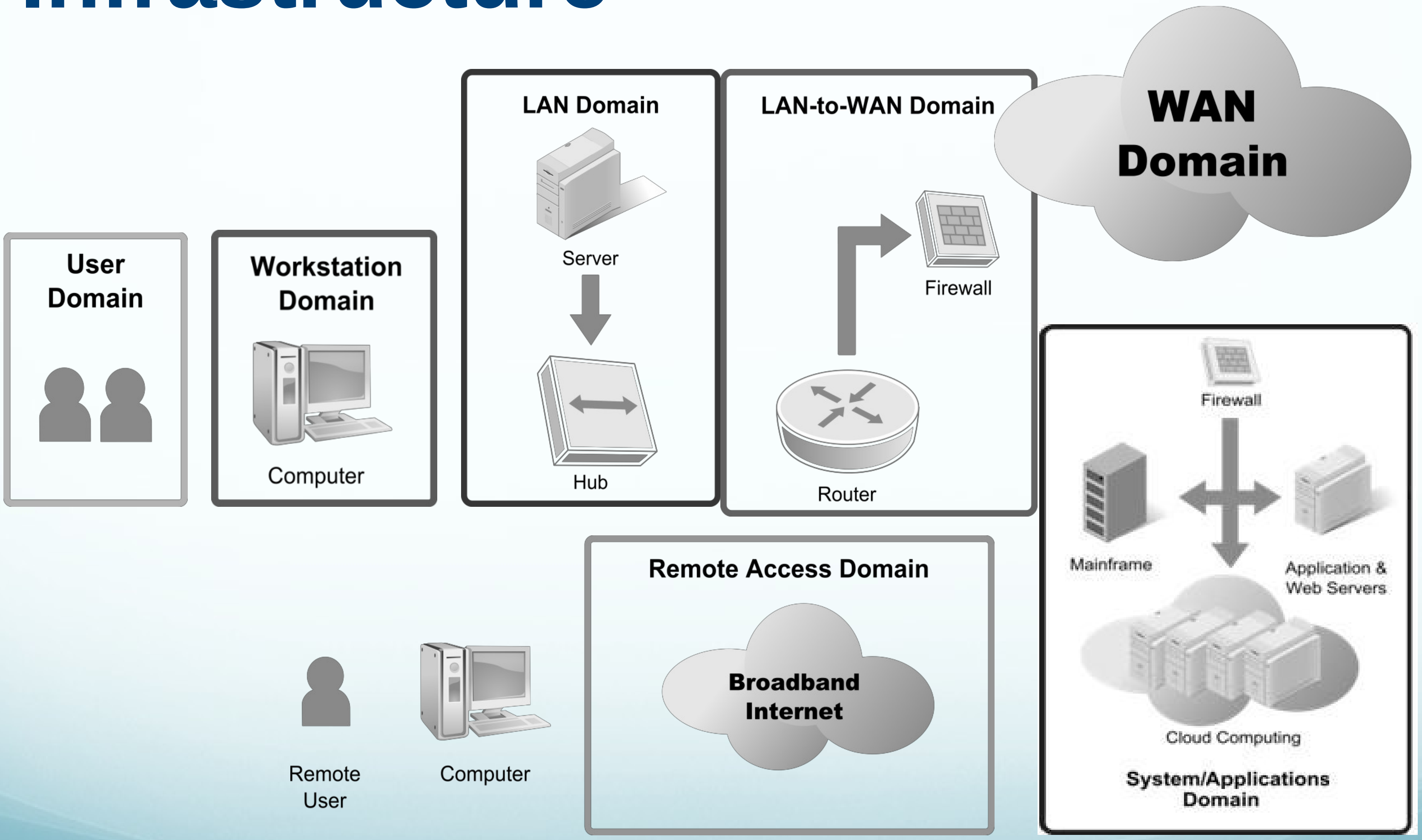
- User
- IT administrator
- Network administrator
- Human resources
- Senior management

Availability

- IT administrator
- Network administrator
- Third-party vendor, for example, telecommunication company

Compliance Laws Driving Computer Security

Seven Domains of a Typical IT Infrastructure



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

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 with personal files
- User downloading photos, music, or videos

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 server configuration guidelines and standards

Common Threats in the LAN/WAN Domain

- Unauthorized probing and port scanning
- Unauthorized access
- Internet Protocol (IP) router, firewall, and network appliance operating system vulnerability
- Local users downloading unknown file types from unknown sources

Common Threats in the LAN/WAN Domain

- Open, public, and accessible data
- Most of the traffic being sent as clear text
- Vulnerable to eavesdropping
- Vulnerable to malicious attacks
- Vulnerable to Denial of Service (DoS) attacks

Common Threats in the LAN/WAN Domain

- Vulnerable to corruption of information and data
- Insecure Transmission Control Protocol/Internet Protocol (TCP/IP) applications
- Hackers and attackers e-mailing Trojans, worms, and malicious software freely and constantly

Common Threats to the Remote Access Domain

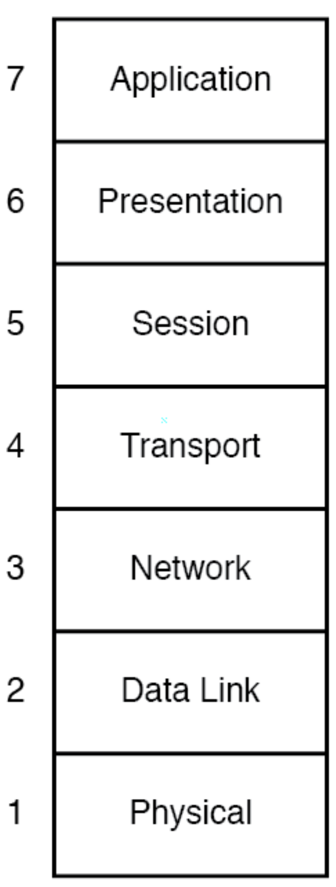
- Brute force user ID and password attacks
- Multiple logon retries and access control attacks
- Unauthorized remote access to IT systems, applications, and data
- Confidential data compromised remotely

Common Threats to the Systems/Applications Domain

- Unauthorized access to data centers, computer rooms, and wiring closets
- Difficult-to-manage servers that require high availability
- Server operating systems software vulnerability management
- Security required by cloud computing virtual environments
- Corrupt or lost data

The OSI Model

- *Open Systems Interconnection (OSI) model.*
- *ISO began work on OSI model following timeline that was close to TCP/IP’s:*
  - *Started in 1970s.*
  - *Progressed on individual standards in 1980s.*
  - *Allowed standards-based vendor products to start appearing by early 1990s.*



7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

OSI Model

The Physical Layer

- Layer 1 of the OSI model is named the physical layer because it is responsible for the transmission and reception of wire level data.

The Data Link Layer

- Layer 2 of the OSI model is named the data link layer and is responsible for link establishment and termination, frame traffic control, sequencing, acknowledgement, error checking, and media access management.

The Network Layer

- Layer 3 of the OSI model is named the network layer and is where routing of network traffic begins. The network layer not only makes the traffic routing decisions but also provides traffic control, fragmentation, and logical addressing (Internet Protocol (IP) addresses).

The Transport Layer

- Layer 4 of the OSI model is named the transport layer and is responsible for message segmentation, acknowledgement, traffic control, and session multiplexing.

The Session Layer

- Layer 5 of the OSI model is named the session layer and is responsible for session establishment, maintenance and termination (the ability to have multiple devices use a single application from multiple locations)..

The Presentation Layer

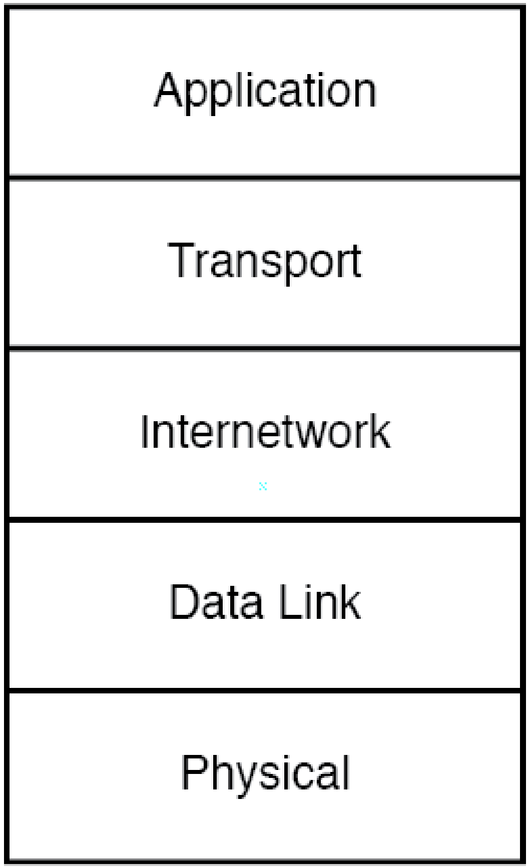
- Layer 6 of the OSI model is named the presentation layer and is responsible for character code translation (i.e. ASCII vs. EBCDIC vs. Unicode), data conversion, compression, and encryption.

The Application Layer

- Layer 7 of the OSI model is named the application layer and is responsible for a number of different things depending on the application; some of these things include resource sharing, remote file access, remote printer access, network management, and electronic messaging (email).

The TCP/IP Model

- *Commonly-used version of TCP/IP model has five layers.*
- *Original TCP/IP model had four layers:*
  - *Bottom two layers of model combined into Network Interface layer (or Network Access layer).*



Application

Transport

Internetwork

Data Link

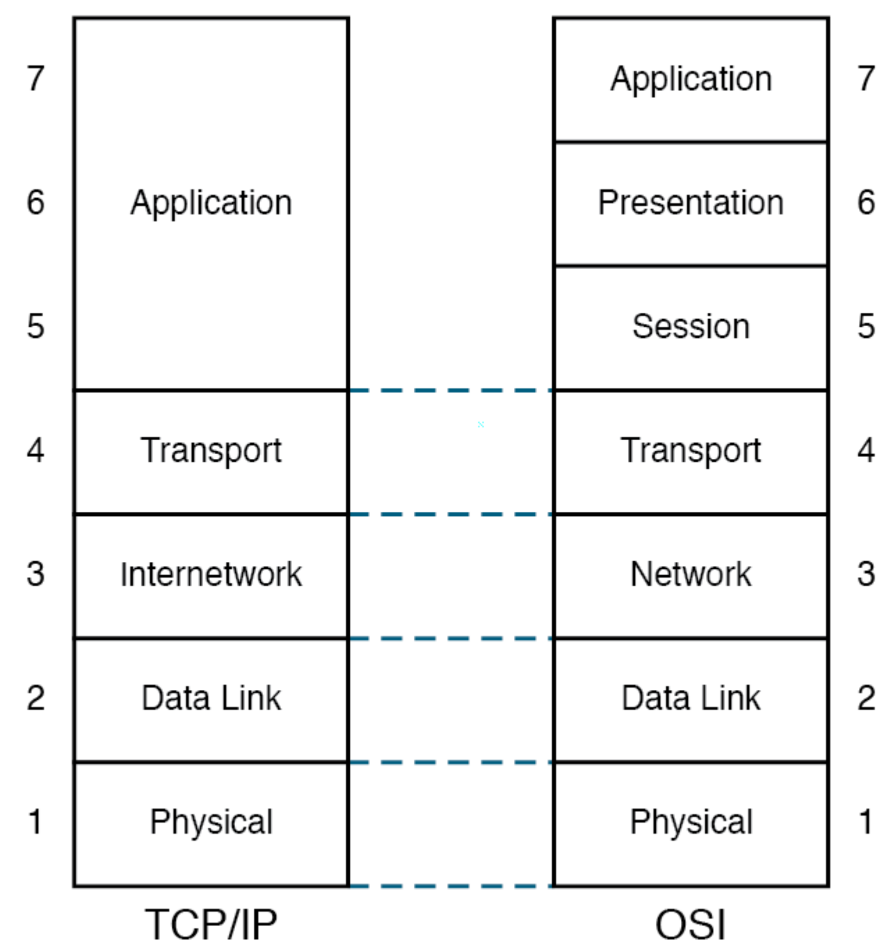
Physical

TCP/IP Model

Comparing TCP/IP to the OSI Model

The biggest differences between the TCP/IP and OSI models exist at the top.

The TCP/IP model defines many functions as part of the application layer, while the OSI model split those functions into multiple layers.



	TCP/IP	OSI	
7	Application	Application	7
6		Presentation	6
5		Session	5
4	Transport	Transport	4
3	Internetwork	Network	3
2	Data Link	Data Link	2
1	Physical	Physical	1

The Data Link Layer

- The link layer is the lowest layer of the TCP/IP model; it is also referred to in some texts as the Network Interface layer or Network Access. The link layer combines the physical and data link layer functions into a single layer.

The Internet Layer

- The Internet layer is the next layer up from the link layer and is associated with the network layer of the OSI model. Functions include traffic routing, traffic control, fragmentation, and logical addressing.

The Transport Layer

- The Transport layer is the next layer and is typically related directly with the same named layer in the OSI model. Functions include message segmentation, acknowledgement, traffic control, session multiplexing, error detection and correction (resends), and message reordering.

The Application Layer

- The Application layer is the highest layer in the TCP/IP model and is related to the session, presentation and application layers of the OSI model. The application layer of the TCP/IP model is used to handle all process-to-process communication functions; these functions were carried out by multiple different layers when referencing the OSI model.

Packet Switching

Questions?