

L23-CS8421-Security-1

Computing Security Part 1

CS8421

Computing Systems

Dr. Ken Hoganson

Class

Will

Start

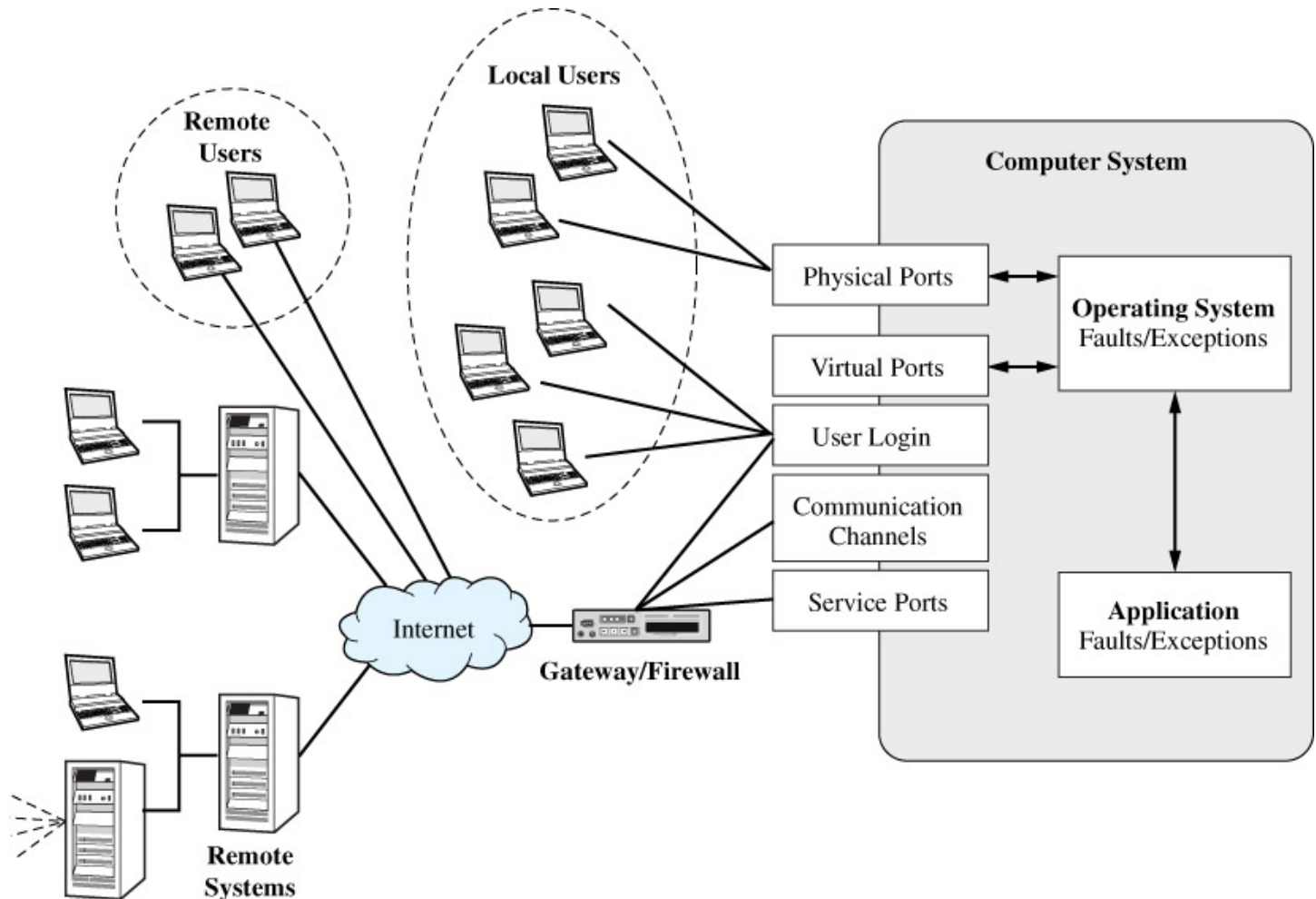
Momentarily...

- Computing systems must be protected from threats, both internal and external:
 - unauthorized access.
 - malicious modification or destruction
 - accidental introduction of inconsistency
 - theft of information/data for gain
 - theft of competitive information
- In general, protecting against accidental data loss is easier than intentional.

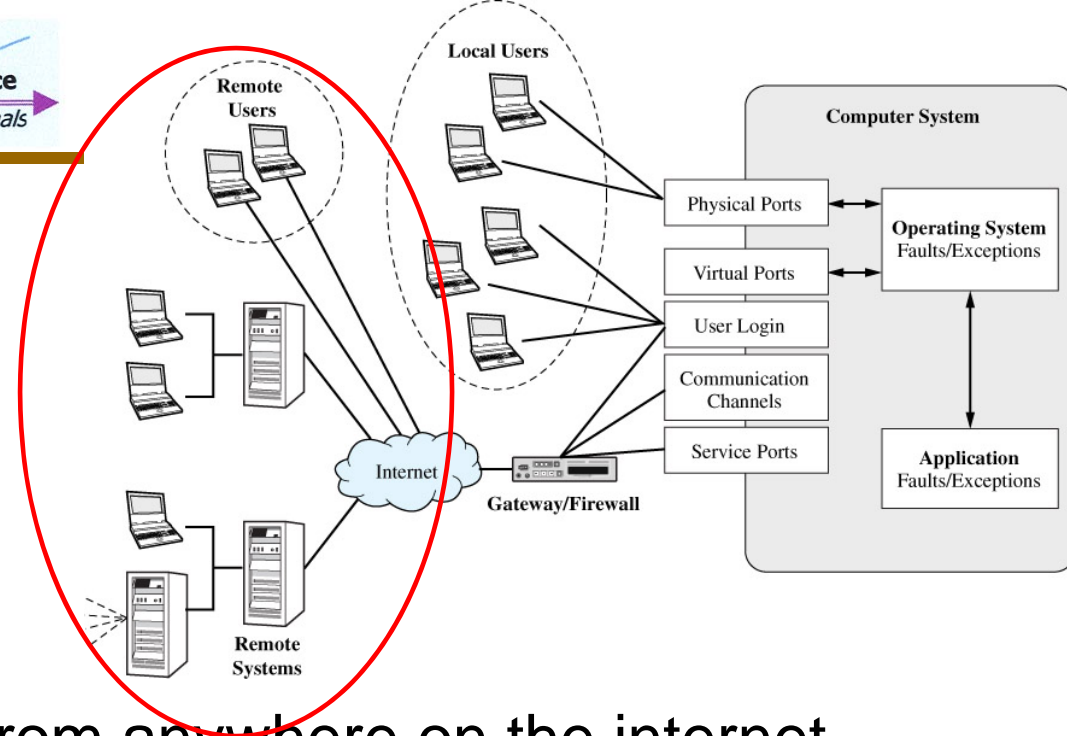
- Has become a large and critically important aspect of computing and information technology
- Attacks can cause loses in millions and billions of dollars in loses.
- Threats come from many sources and different motivations.
- Defensive techniques and technologies build a multi-level “defense-in-depth”
- Greatest weaknesses are human:
 - Systems with openings due to poor operations
 - Systems with openings due to poor design
 - Software vulnerabilities: OS and applications
 - Human error and laziness

- Identity theft: credit card and other personal data
- Financial theft/fraud/redirect funds
- Steal technology or corporate trade secrets
- Malicious harm from disgruntled employees
- Malicious harm from competitors
- “Just to prove I can” ego-driven hackers
- Foreign powers seeking to harm the a nation, its citizens, and its allies:
 - Defense/military secrets: strategic, tactical, technology, weapons
 - Financial system: bring down the financial and banking systems, stock market, internet access

➤ Access pathways for potential threats

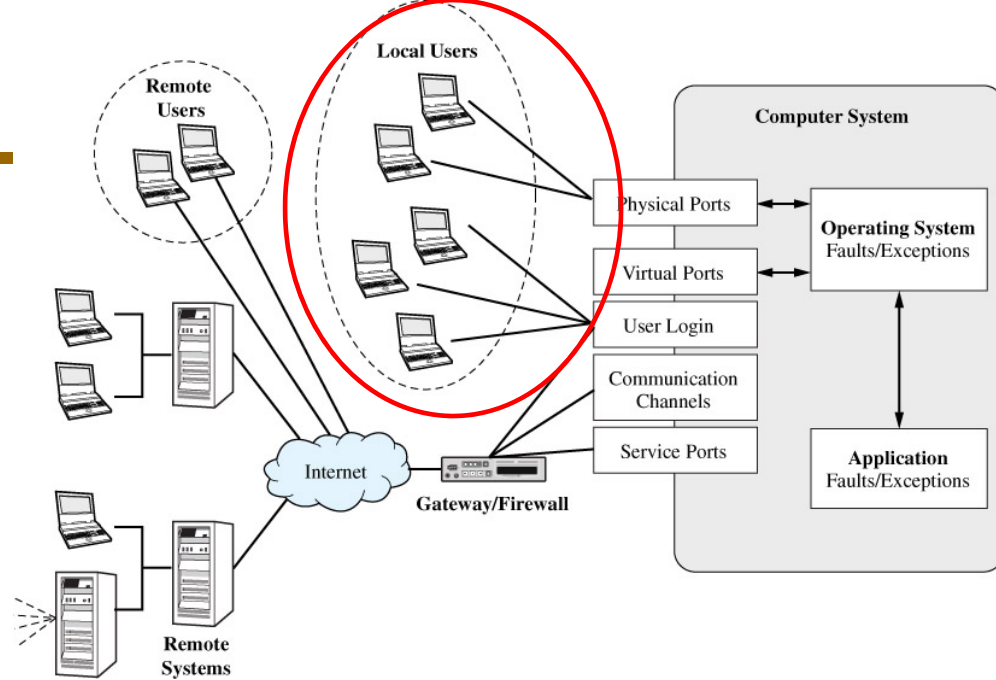


Threats from the Internet



- Remote users/customers from anywhere on the internet
 - General public: clients/customers
 - Through authorized remote systems, part of the firm or an authorized electronic business customer
 - General through multiple levels of systems/LANs, to hide or confuse the electronic trail used to identify hackers
- Gateway/firewall protections
 - Can limit access to authorized users
 - Can limit functions/actions that can be performed.
 - Can detect and deny specific attack techniques

Threats from Local Users



Employees connected to LANs or servers/mainframes/clusters

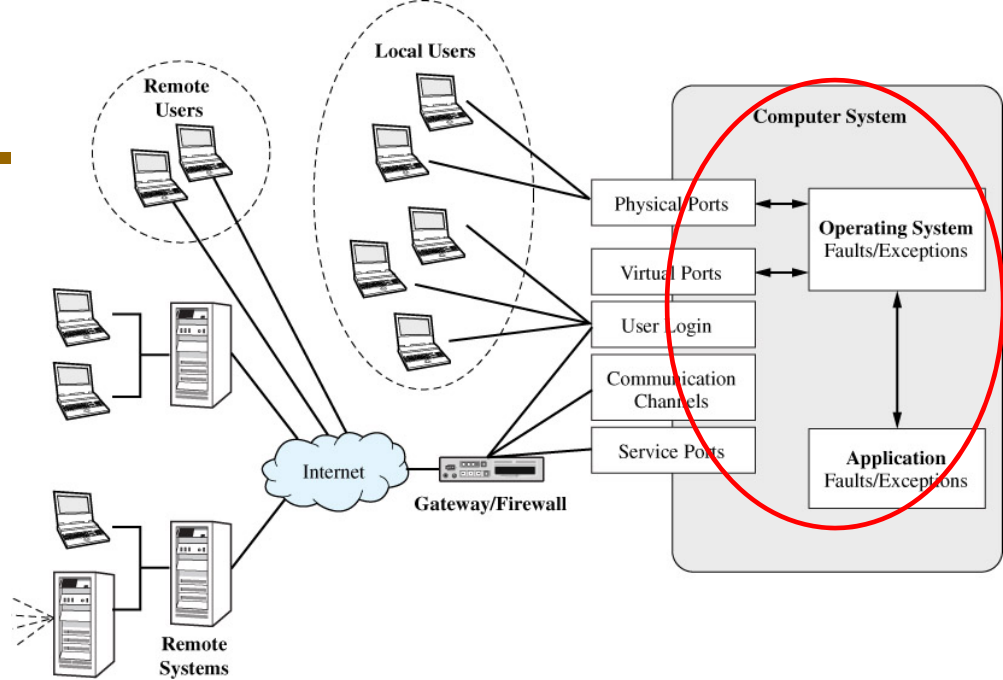
- Direct connect through wired ports on the server/mainframe:
 - Limited number and usually limited to authorized IT employees
 - May include CEO, CIO
- LAN-connected users access through “virtual ports”

Protection:

- Login account/password authentication
- Privilege restrictions
- Real-time automated checking of processes and activities

Threats from Within the System

5



Once system access has been authorized, threats are from application and operating system flaws and vulnerabilities

- Allow a hacker to hijack an application and redirect an authorized and privileged process.
- LAN-connected users access through “virtual ports”

Protection:

- Login account/password authentication
- Privilege restrictions
- Real-time automated checking of processes and activities

- Decompose and understand an attack, to create a better defense.
- Criminal: obtain evidence from:
 - Computer hard-drives
 - Databases
 - communications logs and records
- Creating electronic tools/searches to:
 - slog through databases and records
 - To examine hard-drives to recover encrypted data, and erased/deleted data

A system is secure if:

- All known system weaknesses have been patched, fixed, blocked, or solved in some way.
- A policy exists to govern the granting of user accounts and access, and application program accounts and privileges
- A policy for monitoring and detecting attacks and security events is in place

- Security Policy is based on the answers to these questions:
 - Who do you trust?
 - How much do you trust them?
- Computer Security commonly refers to the mechanisms and technologies available to enforce the Security Policy

- Physical Security
- Authentication
- System Security
- Monitoring and Detection
- Secure Communications
- People

- Verify that someone is who they say they are
- Verify that automated access is valid and approved by policy

- Various identification methods:
 - Password
 - Key-based protocol
 - Identity card
 - Readable chip
 - Biometric (fingerprint, iris, other)
 - Multiple methods combined:
 - ATM card also requires a PIN

- Password weaknesses
 - When the user selects the password
 - Brute-force dictionary Attack
 - Guessed based on data about a real person
 - Authorized users can be contacted “spoofed” into revealing their account password or key information
 - Random/system generated password
 - Are difficult to remember, tend to be writtend down, and hence vulnerable.

- Weaknesses of electronic chips and ID cards
 - Physical: can be lost or stolen
 - Perhaps can be forged
 - May wear out over time, requiring replacement and destruction of old ID cards

- Individual unique signatures:
 - Retinal Scan
 - Fingerprint
 - Genetic - saliva
 - Facial Recognition
 - Voice Recognition
 - Gait - how you walk has been shown to be unique and identifiable
 - Written signature
 - Speaking/writing style
 - Knowledge (i.e. mother's maiden name)
- These are difficult to fake, but may be possible
- Strongest when combined:
 - ID card + PIN + Fingerprint

- Mechanisms to control what an authenticated user (or process) can do.
 - File Protection
 - Memory Protection
 - Web Protection
- Devices to protect system from unauthorized access
 - Firewalls
 - Virus Detection Software
 - Spyware Detection Software
- Protect communications with encryption

- Computer codes to prevent the understanding of encrypted information – data is scrambled
- Various techniques to translate information that can only be decrypted by authorized recipient who holds the digital key
- Raw data without the decryption key is useless
- Constant competition: every new encryption scheme is a challenge to see if it can be broken, which leads to new encryption schemes, etc.

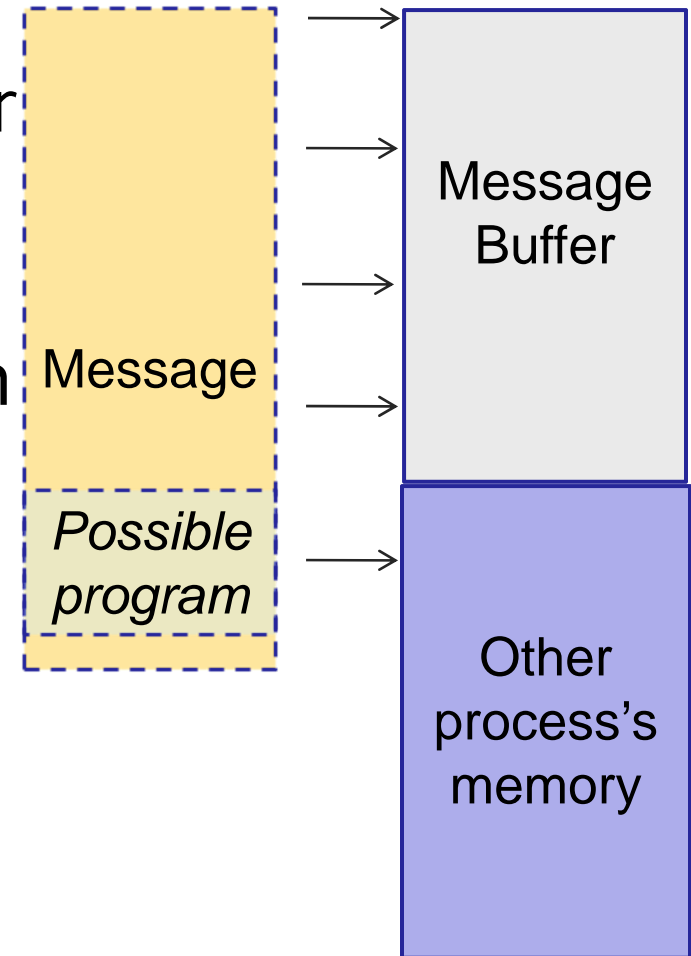
- System Attacks:
 - Trojan Horse: appears legitimate but contains malware (malicious software):
 - Virus
 - Worm
 - Trap Door
 - Stack & Buffer Overflow
 - Denial of Service

- A **computer virus** is a computer program that can copy itself and infect a computer without permission or knowledge of the user.
- The term "virus" is also often used erroneously to refer to many different types malware and adware programs.
- A virus may modify itself as occurs in a metamorphic virus, making detection more difficult.
- A virus can spread from one computer to another when its host is taken to the uninfected computer, either on a physical device or in a communication.
- Viruses can spread to other computers by infecting files on a file system that is networked or accessed by another computer.
- Content Source: Wikipedia

- A **computer worm** is a self-replicating computer program that uses a network to send copies of itself to other machines without requiring human intervention.
- Unlike a virus, a worm does not need to attach itself to a program, file, or communication.
- Worms cause harm to the network, by consuming bandwidth, (denial of service attack) while viruses target files and data to corrupt.

- A way to bypass the normal security protections
- Intentionally inserted into applications and systems to:
 - aid system support staff
 - provide unauthorized access
- Requires system level access to create a trap-door, but once created, allows privileged access.
- Requires a system-level or low-level software examination to detect, so are often difficult to detect or automate protection against.

- Overflow a buffer or stack data structure.
- Message/ data transfer larger than buffer size.
- If insufficient memory protection, then overflow can corrupt data or programs.
- Possibly leading to unauthorized execution of program



- Technique
 - Indeterminate length read: `read(file,buffer)` (reads as much data as the remote system sends)
 - Fixed length read of defined quantity of data: `read(file,buffer,100)` (Read 100 bytes)
- Inadequate memory bounds checking
- Inadequate checking of the validity of the data that is received
- Fix: Test/check all messages&transfers, and build in process memory bounds checking.

- Hijack user input stream. Insert a command into a SQL input.
- Possible when the application does not validate user input.
- Example:
 - SELECT TOTAL FROM LINE_ITEM WHERE ID_NO =XXX
 - User Input for XXX is an error/command:

"104;UPDATE LINE_ITEM SET TOTAL=500000 WHERE ID_NO =3287"

- Does not break into the system or corrupt data.
- Instead, overloads system with bogus messages.
- Legitimate messages cannot get through or are delayed.
- Access to system for service is denied.

- Can be done fairly easily – automated.
- Can be protected by looking for multiple messages from the same network ID (or similar)

**End
Of
Today's
Lecture.**

