Fundamental Concepts of Cryptography ISEC2000/ISEC5002

Lecture 2: Principles of Information Security

Information Security in connected device/computer network

People aim to provide information protection in data transmission system in order to attain the following objectives

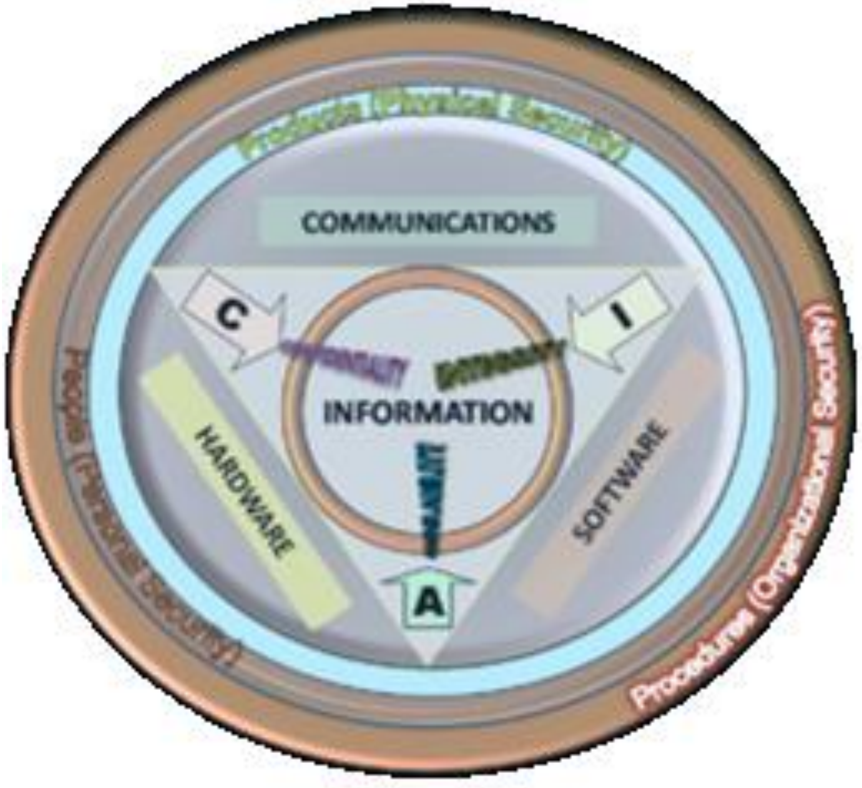
- **Integrity**
- Availability
- **Confidentiality**

With system resources (including hardware, software, *firmware*, information/data and communication channel).

Three key components

- **Confidentiality**: includes data **confidentiality** (assures that private information is not revealed to the unauthorized individuals) and **privacy** (what information is confidential and by whom and to whom such information can be disclosed).
- **Integrity**: includes **data integrity** and *system integrity* (*systems performed as intended*)
- **Availability**: Systems perform/work promptly and service is not interrupted/denied.

The three components are known as CIA


Products (Physical Security)
COMMUNICATIONS
C
I
INFORMATION
HARDWARE
SOFTWARE
A
People (Personnel Security)
Procedures (Organizational Security)

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means of protecting personal privacy and proprietary information.

A loss of confidentiality is the unauthorized disclosure of information.

Integrity

Guarding against improper information modification or destruction, *including* ***information nonrepudiation*** *and authenticity*.

A loss of integrity is the unauthorized modification or destruction of information. We need efficient and effective methods to detect this loss.

Availability

Ensure timely and reliable access to and use of information.

A loss of availability is the disruption of access to or use of information or an information system. This is mainly related to device/computer network systems.

Challenges of computer/network security

- Very complicated.
- When you develop one mechanism for one threat, another possible threat may be created.
- Where to deployment for the developed mechanisms. In which level, IP, application, etc.(firewall investigation)
- This is an endless battle between the users and penetrators/hackers/intruders. (**Where we should start to investigate this war?)**

The OSI Security Architecture

Though computer security has huge challenges, people attempt to solve it in a **systematic approach**. The OSI security architecture was developed in the context of **OSI protocol architecture**.

It focuses on security attacks, mechanism and services. It is useful to system managers as a way of organizing the task of providing security. **(open system interconnection (OSI))**

OSI Security Architecture

- **Security attack**: Any action that compromises the security of information owned by an organization.
- **Security mechanism**: A process that is designed to ***detect, prevent*** or recover from a security attack.
- **Security services**: The services are intended to counter security attacks, and one would make use of one or more security mechanisms.

Security Attacks

- **Passive attacks**: Attempts to learn or make use of information from the system but does not affect system resources. (Listening/no action)
- **Active Attacks**: Attempts to alter system resources or affect its operations. (Action)

Passive Attacks

- Two types of typical passive attacks.
  - Release of message contents.
  - Traffic analysis.
- Passive attacks are hard to detect and we just try to prevent.

Active Attacks

Typical active attacks

- Masquerade.
- ***Replay. (change service process)***
- Modification of message.
- Denial of service.

Security Services

- **Authentication** (peer entity authentication and data origin authentication)
- **Access Control (**authorization, authentication, access approval, and audit.)
- **Data confidentiality** (**connection** confidentiality and **connectionless** confidentiality, traffic flow confidentiality,)
- **Data integrity** (data and communication)
- **Nonrepudiation** (Origin and destination)

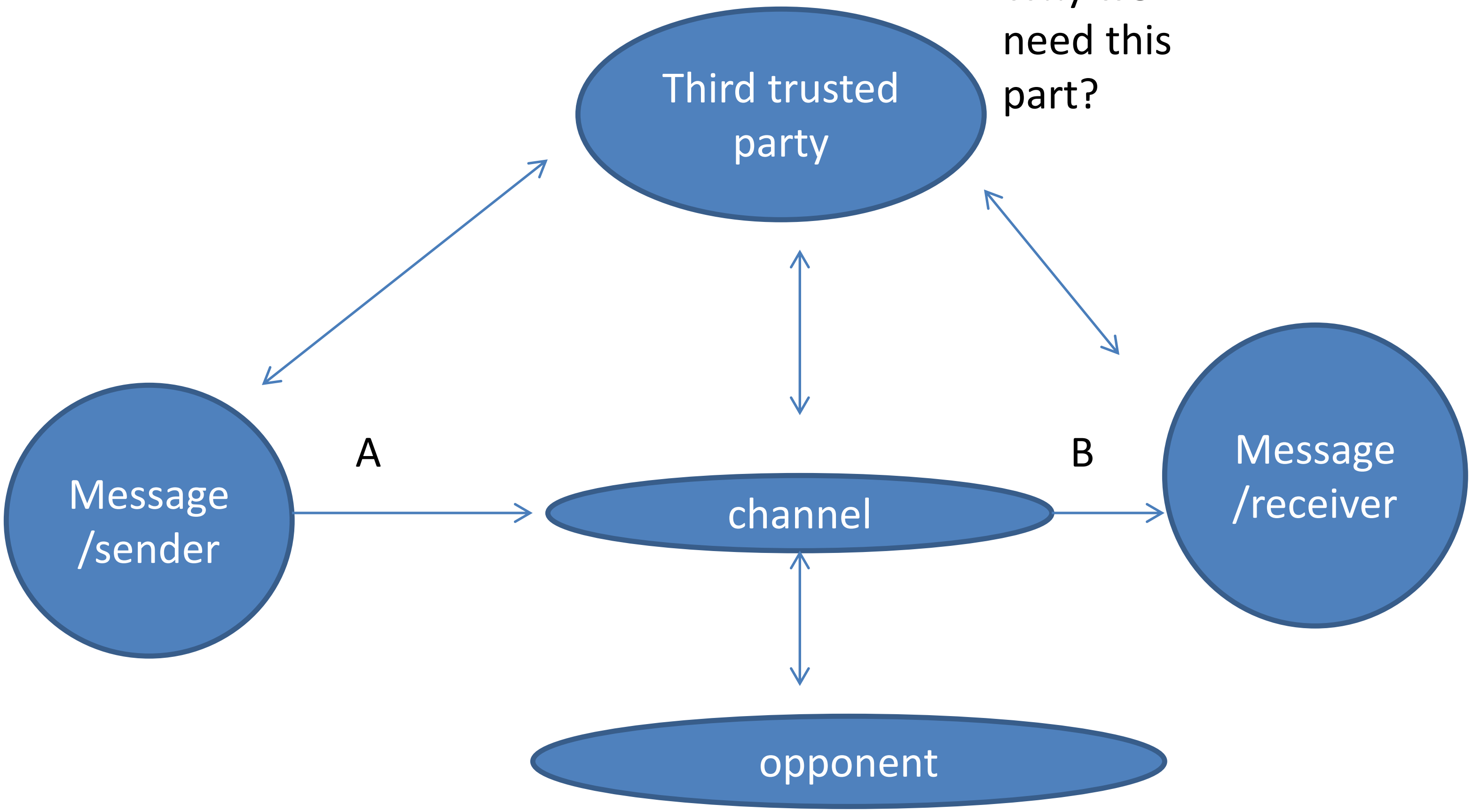
Security Mechanisms (**our aim in this unit**)

- **Encryption**
- **Digital signature**
- Access control
- **Hash functions for integrity check**
- **Authentication exchange protocol**
- Traffic padding (different types of encryptions for communications, or adding additional data in your network traffic to make it more difficult to identify the sender, receiver, and/or the data being transmitted.)
- Routing
- notarization

Security Mechanisms (Network part)

- Trusted functionality (third party authority, trust policy, etc.).
- Security label (security level indicator, etc.)
- Event detection.
- Security audit.
- Security recovery.

A Network Security Model



Why we need this part?

Security Architecture Model

Information channel: TCP/IP connection

A: security related transformation including encryption, authentication, etc.

B: security related transformation including decryption, verification, etc.

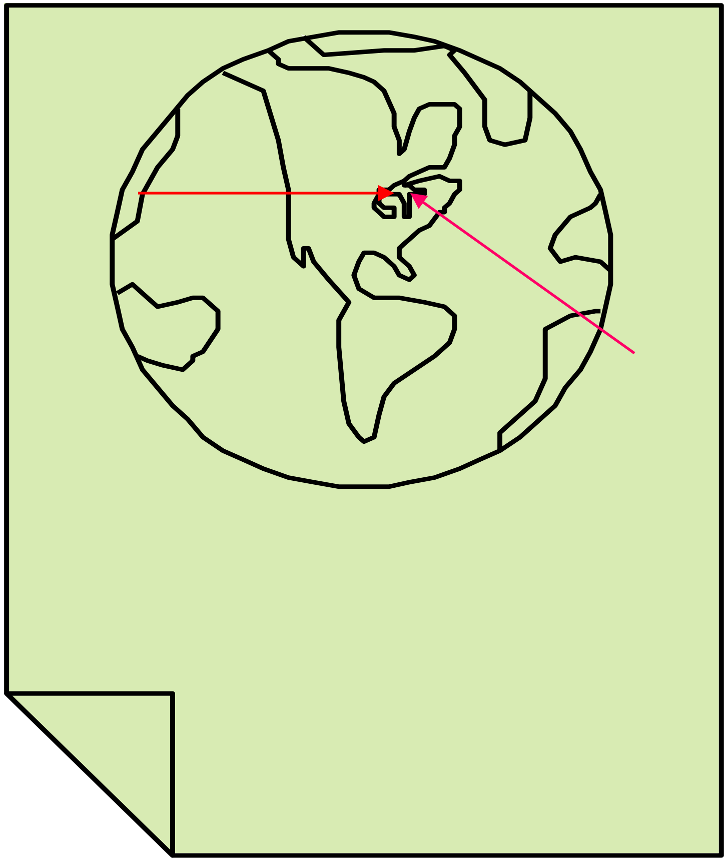
Third party: either in charge of key distribution or **arbitrator** for disputes.

Opponent: can be hackers or any possibly threats.

The typical Problems of Network Security

- The Internet is so open and it allows an attacker to attack from anywhere in the world from their home desk.

- They just need to find **one** vulnerability: a security analyst needs to detect and close **every possible** vulnerabilities.



Hacking networks

Phase 1: Reconnaissance (pick-up)

- **Dumpster Diving or skipping diving**:*is a technique used to retrieve information that could be used to carry out an attack on a computer network.*

  Google, Newsgroups, Web sites

  Social Engineering

  - Phishing: fake email
  - Pharming: fake web pages
- Who is Database & arin.net
- Domain Name Server Interrogations

Hacking Networks

Phase 2: Scanning (find possible vulnerability)

War Driving: Can I find a wireless network?

War Dialing: Can I find a modem to connect to?

This is too old.

Network Mapping: What IP addresses exist, and what ports are open on them?

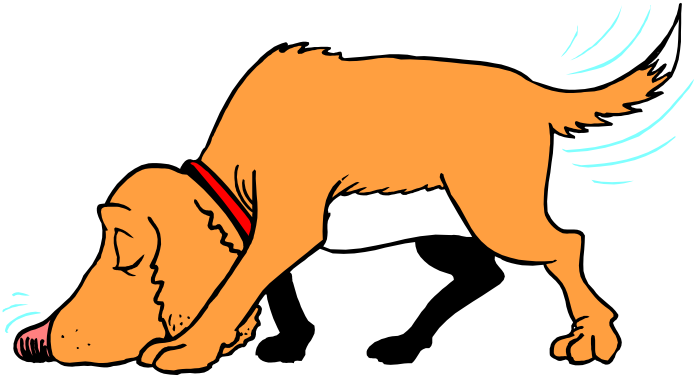
Vulnerability-Scanning Tools: What versions of software are implemented on devices?

Hacking Networks:

Phase 3: Gaining Access

Network Attacks:

- Sniffing (Eavesdropping)
- IP Address Spoofing
- Session Hijacking

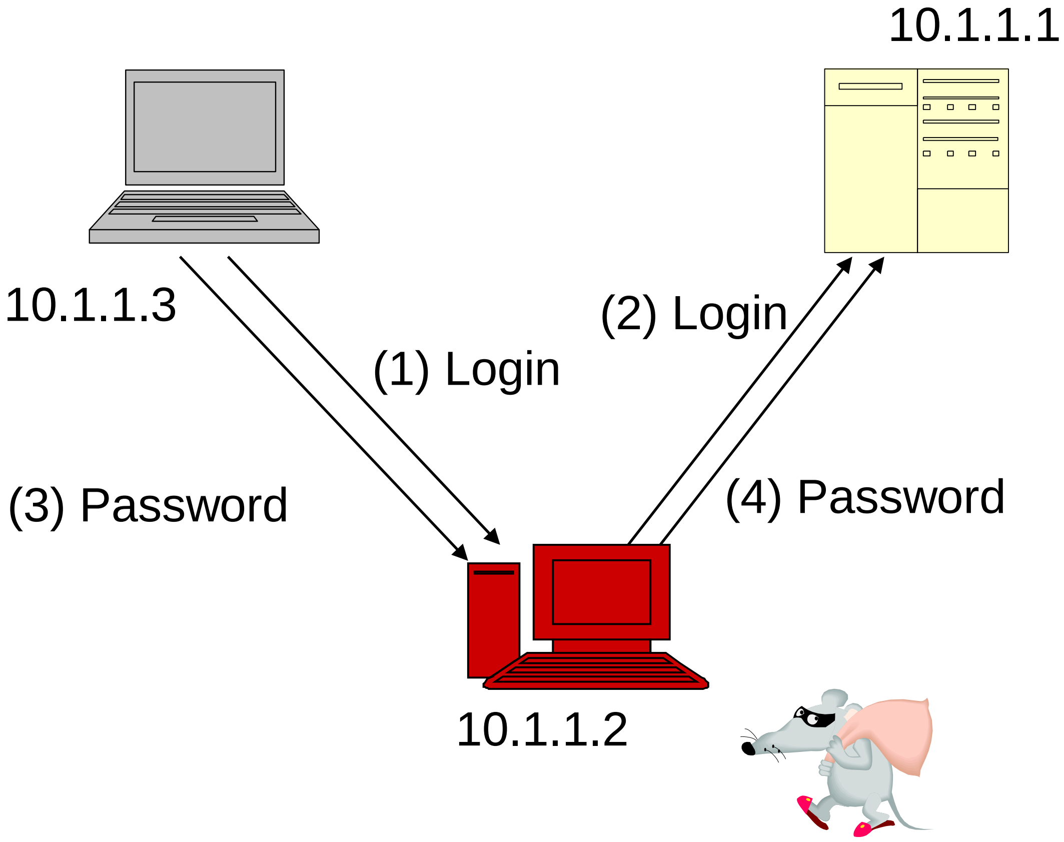


Login: Ginger Password: Snap

System Attacks:

- **Buffer Overflow**
- Password Cracking
- Web Protocol Abuse
- Denial of Service
- Trap Door
- Virus, Worm, Trojan horse,

Man-in-the-Middle Attack



10.1.1.1

10.1.1.3

(2) Login

(1) Login

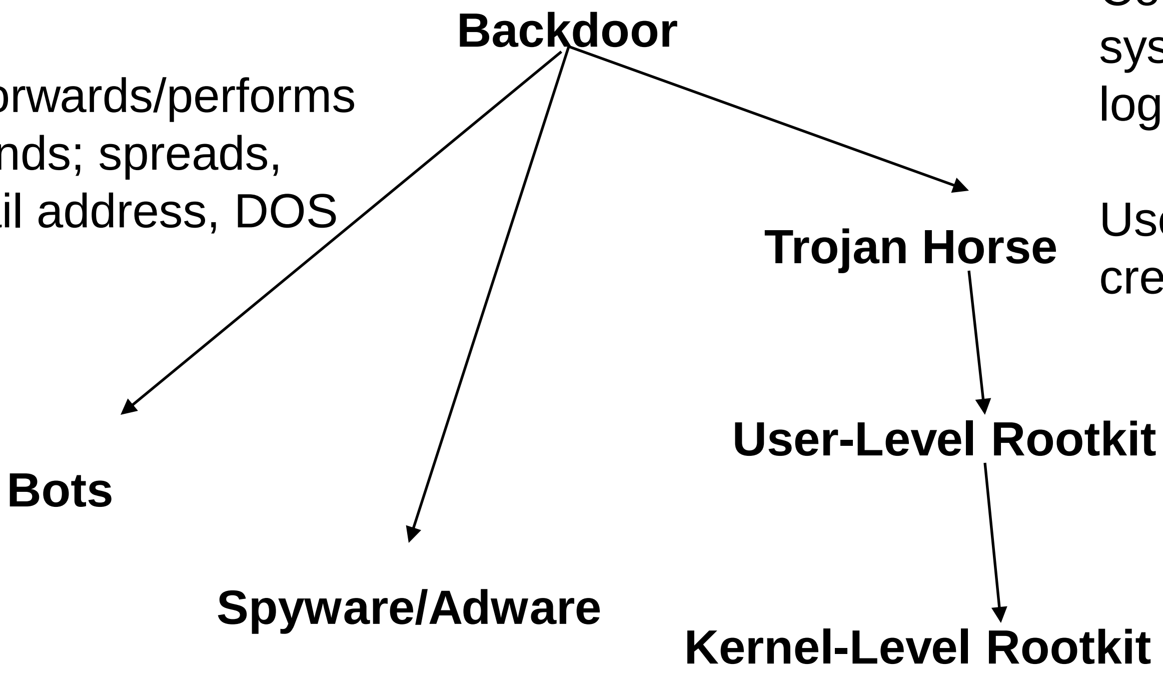
(3) Password

(4) Password

10.1.1.2

Hacking Networks:

Phase 4: Exploit/Maintain Access



Backdoor

Trojan Horse

User-Level Rootkit

Kernel-Level Rootkit

Bots

Spyware/Adware

Slave forwards/performs commands; spreads, list email address, DOS attacks

Control system:
system commands,
log keystrokes, password

Useful utility actually creates a backdoor.

Replaces system executables: e.g. Login, ls, du

Replaces OS kernel: e.g. process or file control to hide

Spyware: Collect info: keystroke logger, collect credit card #s,
AdWare: insert ads, filter search results

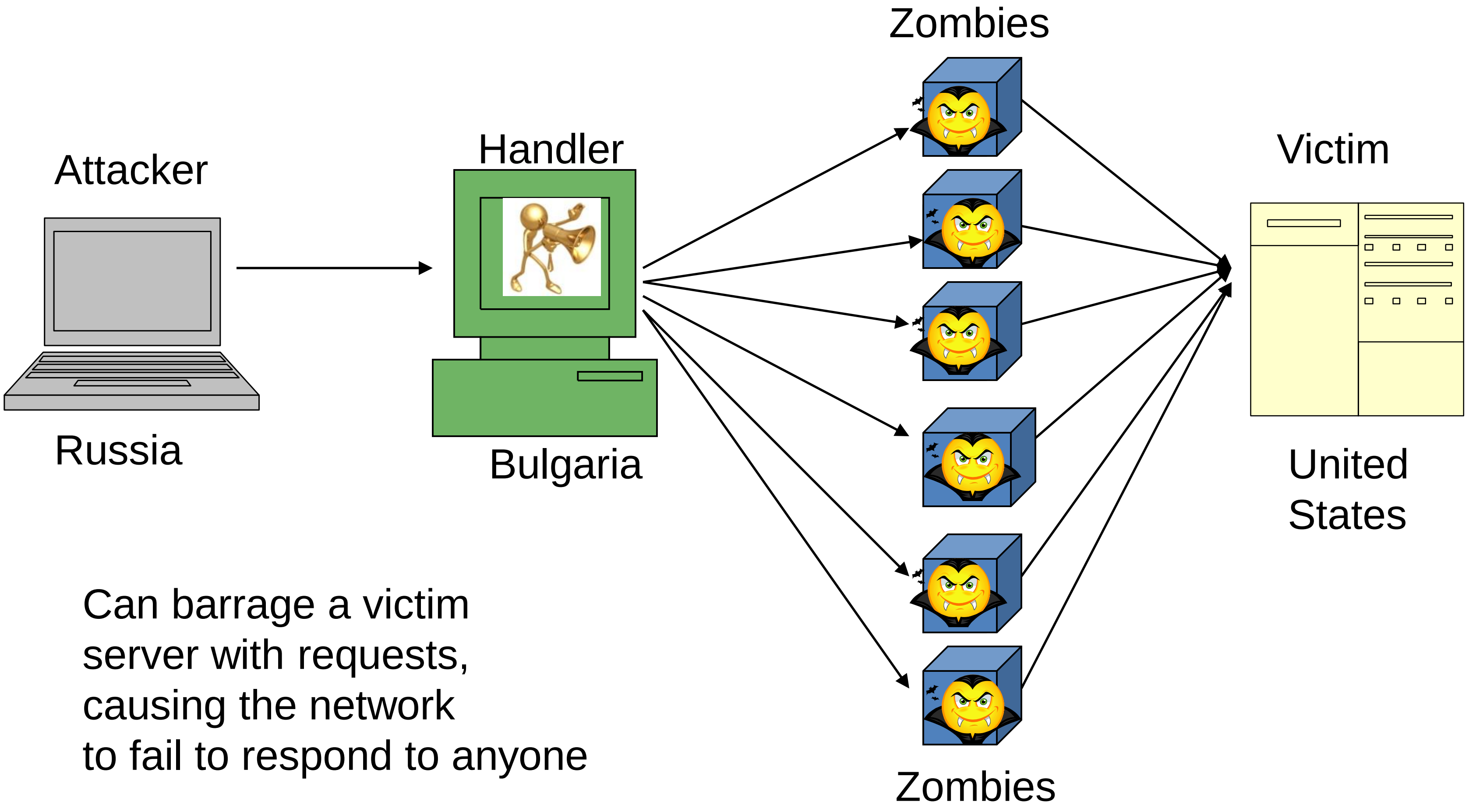
What exactly is an internet bot?

They are software applications that perform repetitive tasks automatically or on a schedule over the internet, tasks that would be too mundane or time-consuming for an actual person.

Or programs designed to secretly install themselves on unprotected or vulnerable computers and carry out whatever actions they demand.

http://au.norton.com/botnet

Distributed Denial of Service

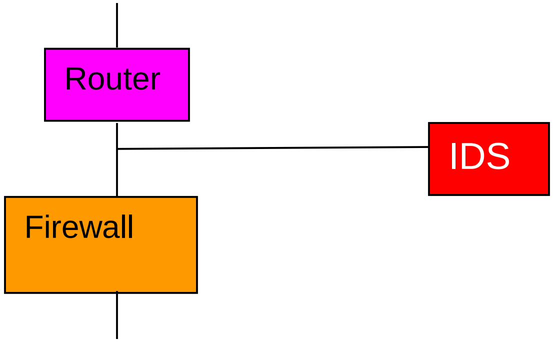


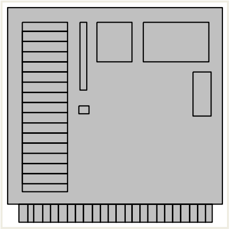
Can barrage a victim
server with requests,
causing the network
to fail to respond to anyone

What we can do technically?

- Packet filters
- Firewalls
- Access control
- Intrusion detection
- Encryption
- Digital signatures

Intrusion Detection Systems (IDS) Intrusion Prevention Systems (IPS)





Network IDS=NIDS

- Examines packets for attacks
- Can find worms, viruses, org-defined attacks
- Warns administrator of attack
- IPS=Packets are routed through IPS

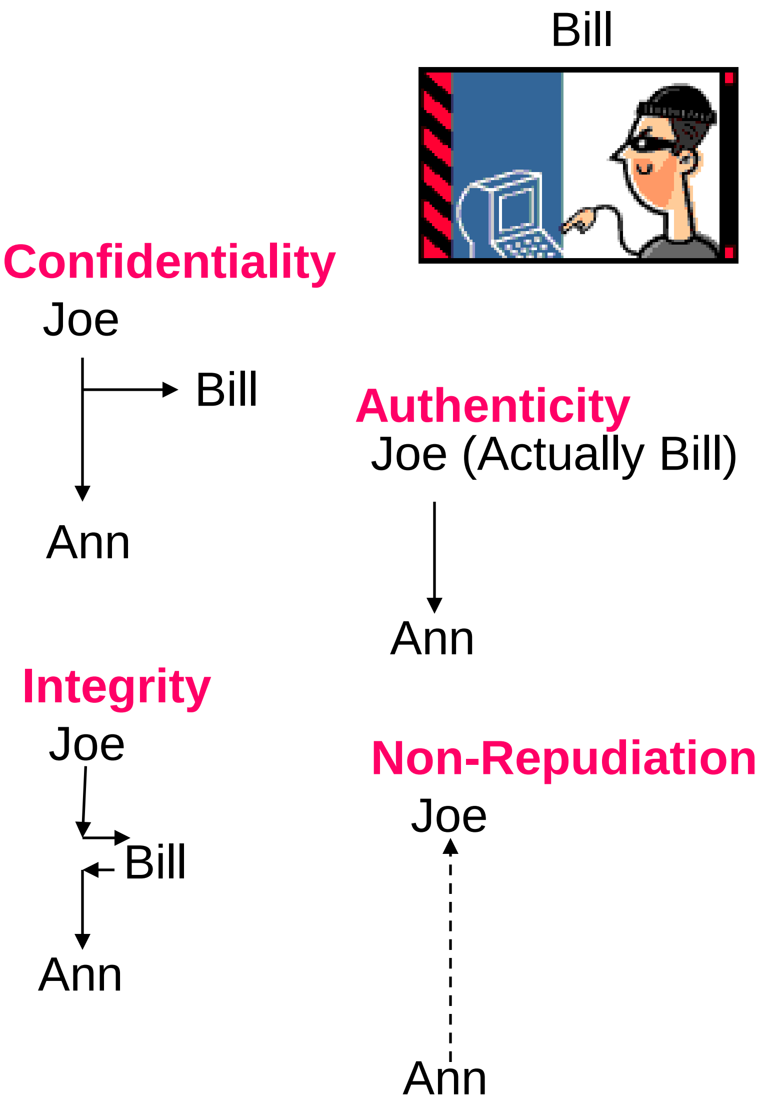
Host IDS=HIDS

- Examines actions or resources for attacks
- Recognize unusual or inappropriate **behavior**

E.g., Detect modification or deletion of special files

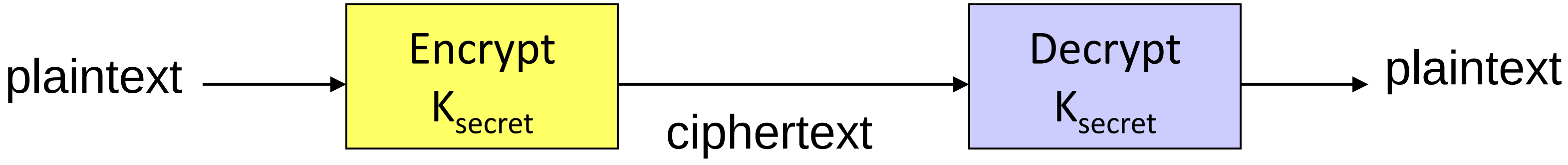
Data Privacy

- **Confidentiality**: Unauthorized parties cannot access information (->Secret Key Encryption
- **Authenticity**: Ensuring that the actual sender is the claimed sender. (->Public Key Encryption)
- **Integrity**: Ensuring that the message was not modified in transmission. (->Hashing)
- **Nonrepudiation**: Ensuring that sender cannot deny sending a message at a later time. (->Digital Signature)



Encryption – Secret Key

Examples: **DES**, AES



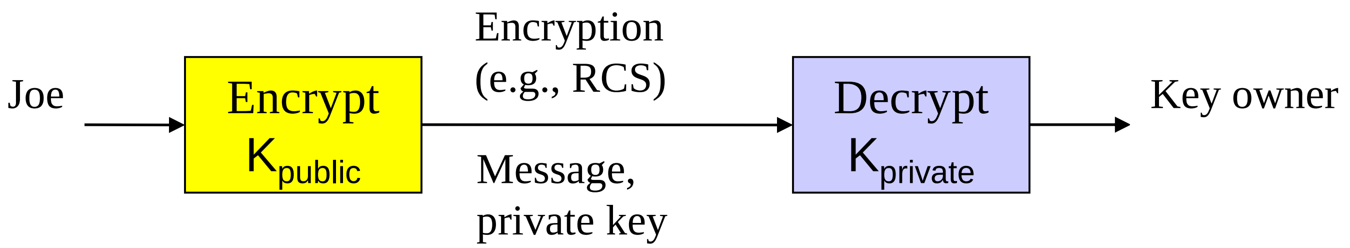
$$P = D(K_{secret}, E(K_{secret},P))$$

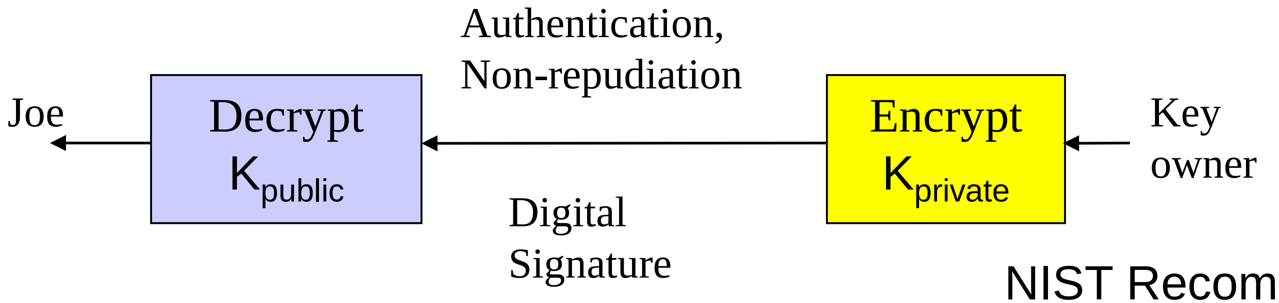
3DES

Public Key Encryption

Examples: RSA, ECC, Quantum

$$P = D(k_{PRIV}, E(k_{PUB},P))$$





NIST Recommended

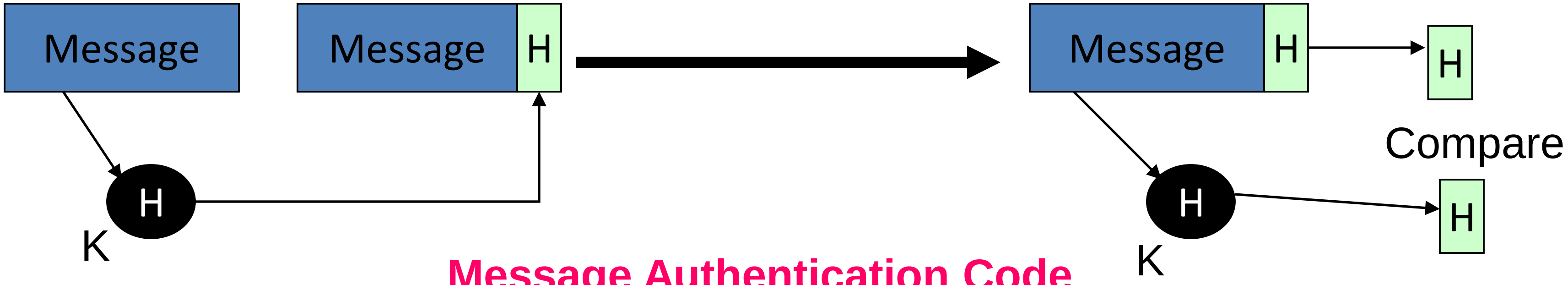
$$P = D(k_{PUB}, E(k_{PRIV},P))$$

RSA 1024 bit

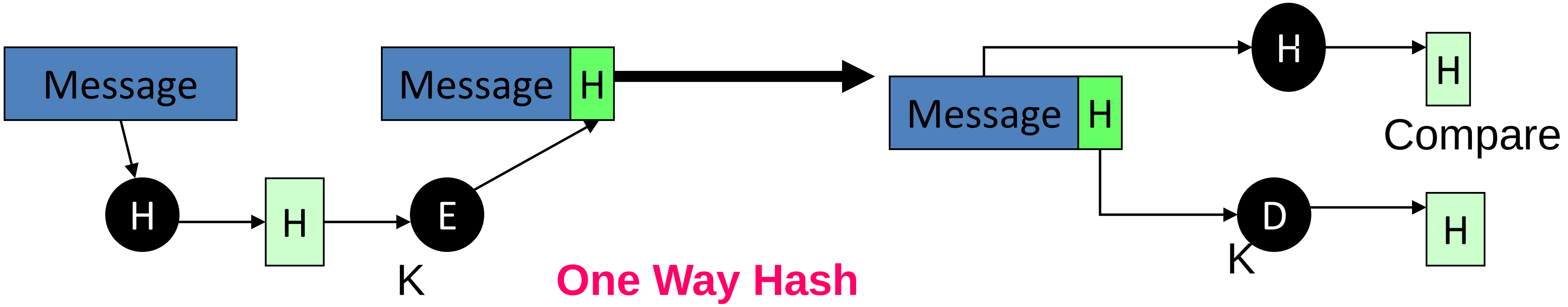
Secure Hash Functions

Examples: SHA1, SHA2, MD2, MD4, MD5

Ensures the message was not modified during transmission



Message Authentication Code

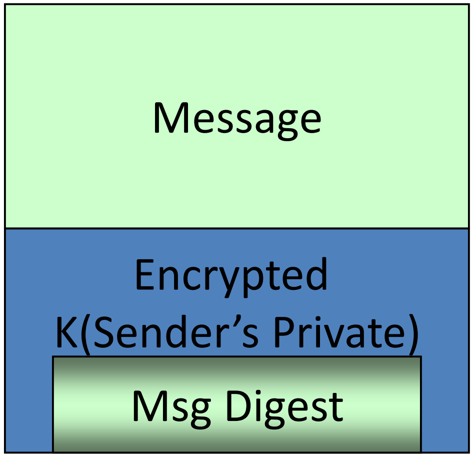


One Way Hash

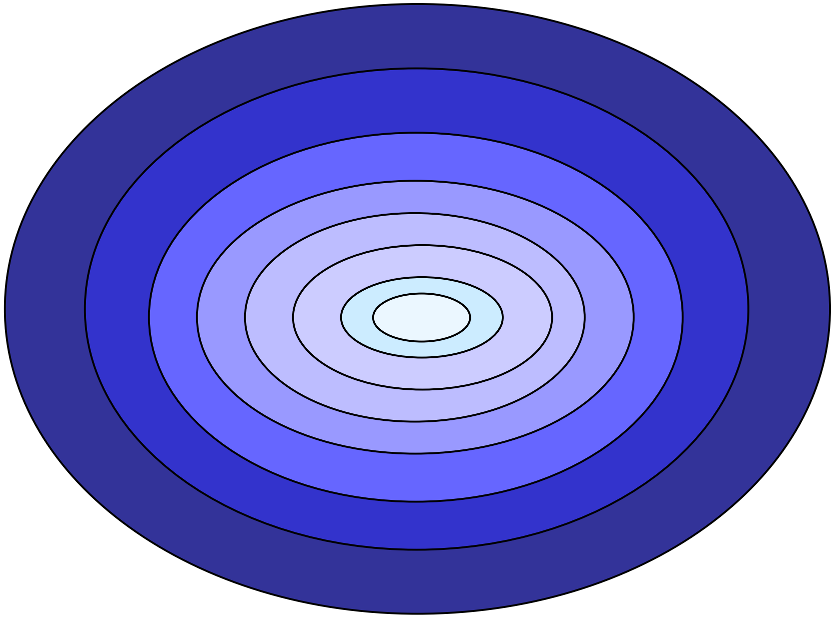
NIST Recommended: SHA-1, SHA-2
2011: SHA-2

Digital Signature

- Electronic Signature
- Uses public key algorithm
- Verifies integrity of data
- Verifies identity of sender: non-repudiation

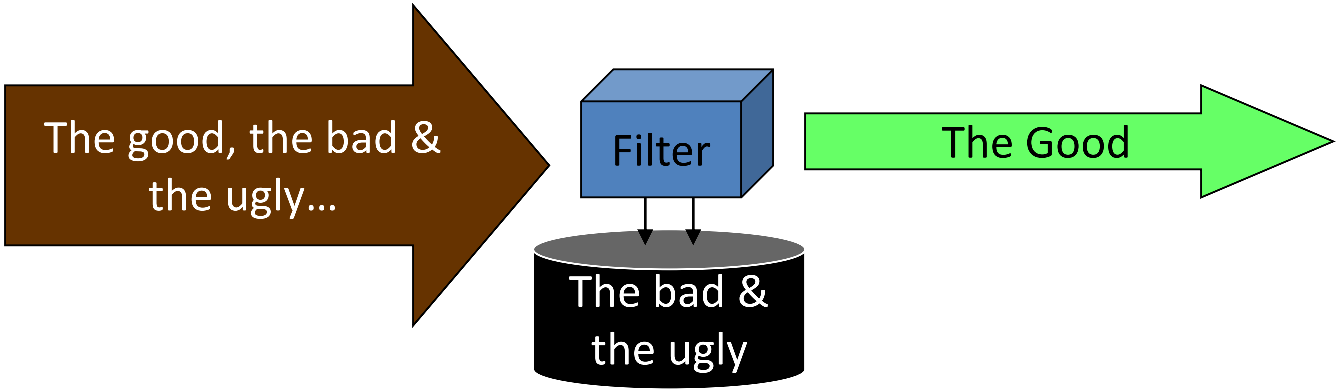


Security: Defense in Depth



Border Router
Perimeter firewall
Internal firewall
Intrusion Detection System
Policies & Procedures & Audits
Authentication
Access Controls

Packet Filters

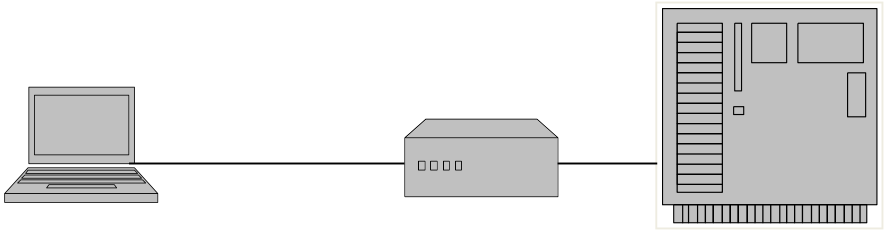


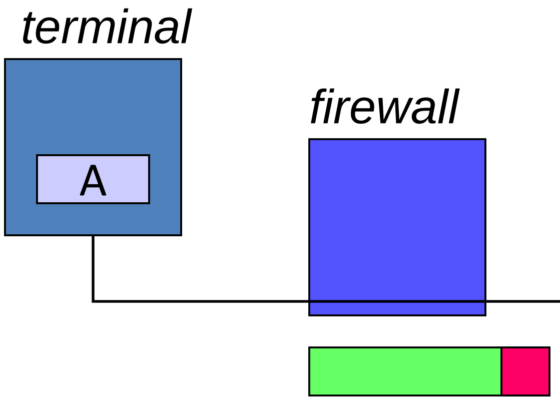
Route Filter: Verifies sources and destination of IP addresses

Packet Filter: Scans headers of packets and discards if rule set failed (e.g., Firewall or router)

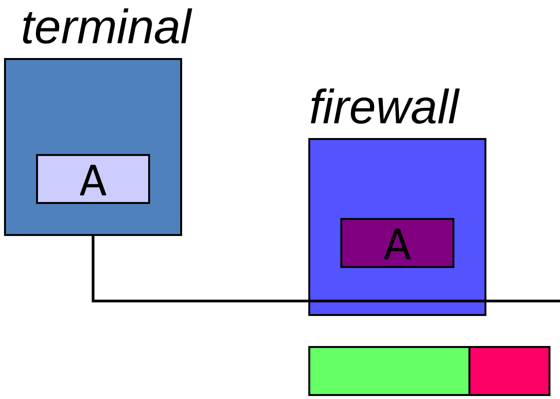
Content Filter: Scans contents of packets and discards if rule set failed (e.g., Intrusion Prevention System or firewall)

Firewall Configurations





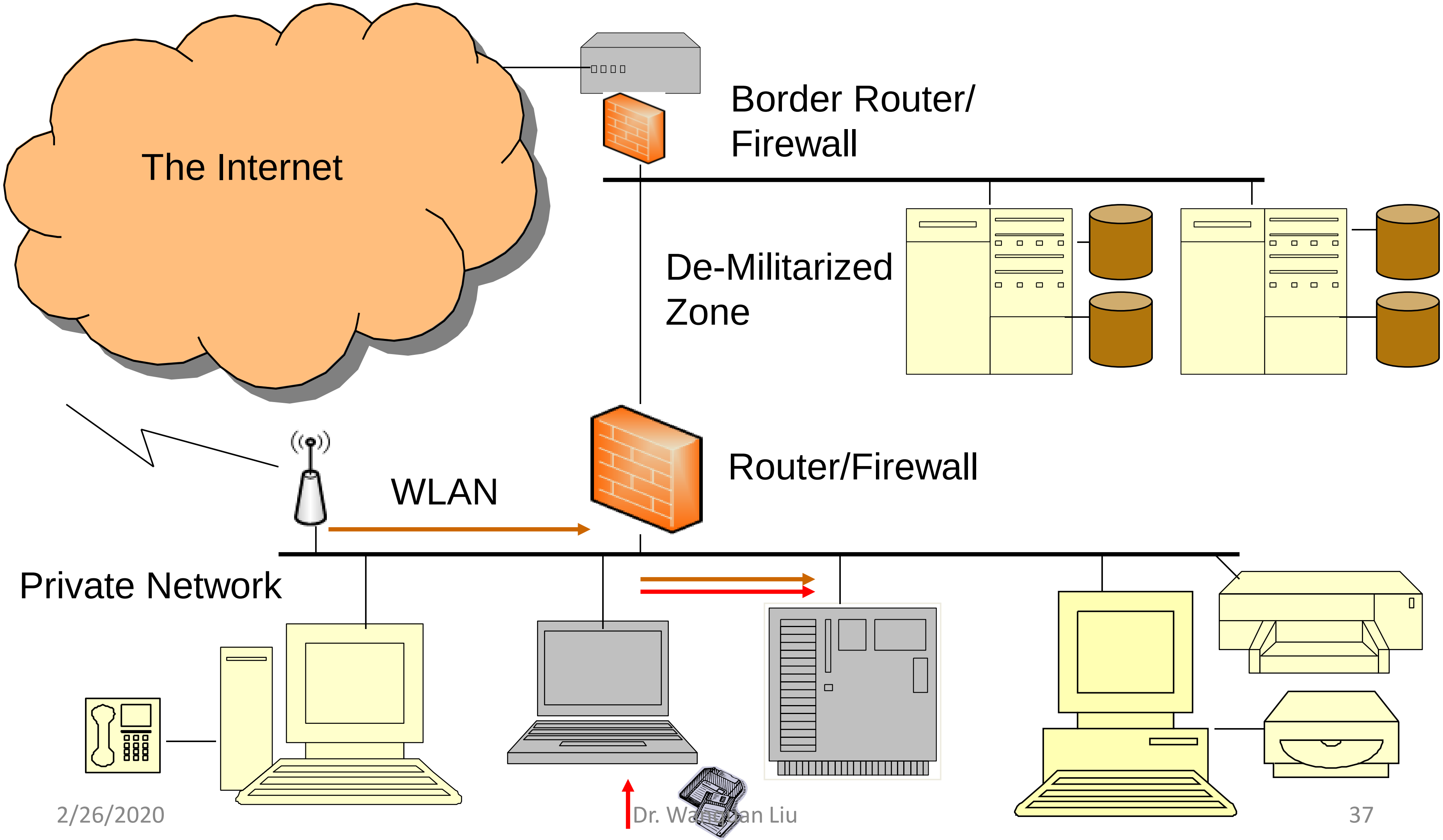
Router Packet Filtering:
Packet header is inspected
Single packet attacks caught
Very little overhead in firewall: very quick
High volume filter



Stateful Inspection
State retained in **firewall memory**
Most multi-packet attacks caught
More fields in packet header inspected
Little overhead in firewall: quick

Logical Access Control

How would access control be improved?



DMZ (demilitarized zone)

A DMZ (demilitarized zone) is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet. External-facing servers, resources and services are located in the DMZ so they are accessible from the Internet but the rest of the internal LAN remains unreachable.

Summary

- Computer security concept
- Security attacks
- Security mechanisms
- Security services
- Typical network security problems
- Possible solutions