NETWORK SECURITY

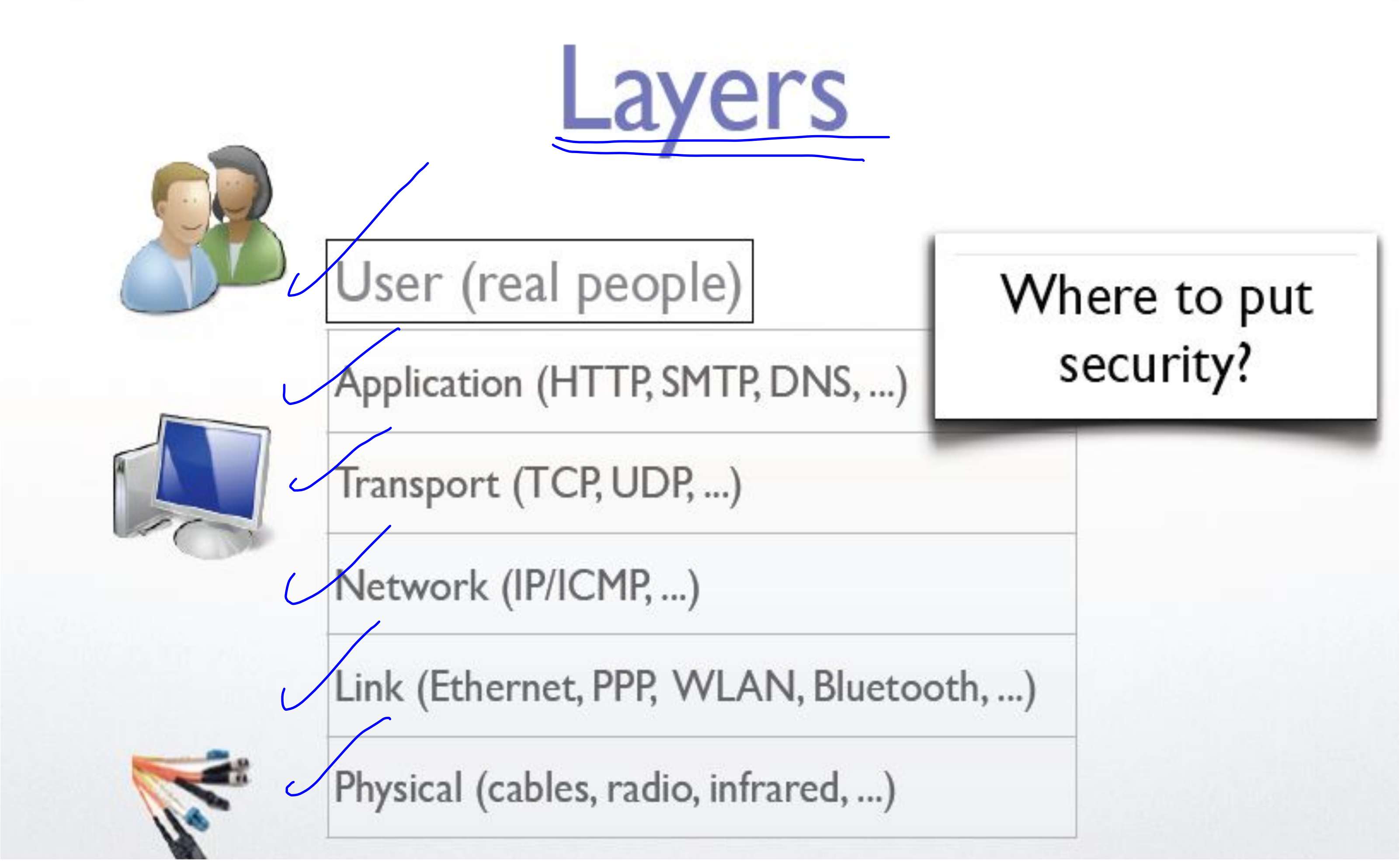
BY: DR. ALA BERZINJI

PROBLEMS OF NETWORK SECURITY

The Internet allows an attacker to attack from anywhere in the world from their home desk.

They just need to find one vulnerability: a security analyst need to close every vulnerability.

NETWORK LAYERS



Layers

✓ User (real people)

✓ Application (HTTP, SMTP, DNS, ...)

✓ Transport (TCP, UDP, ...)

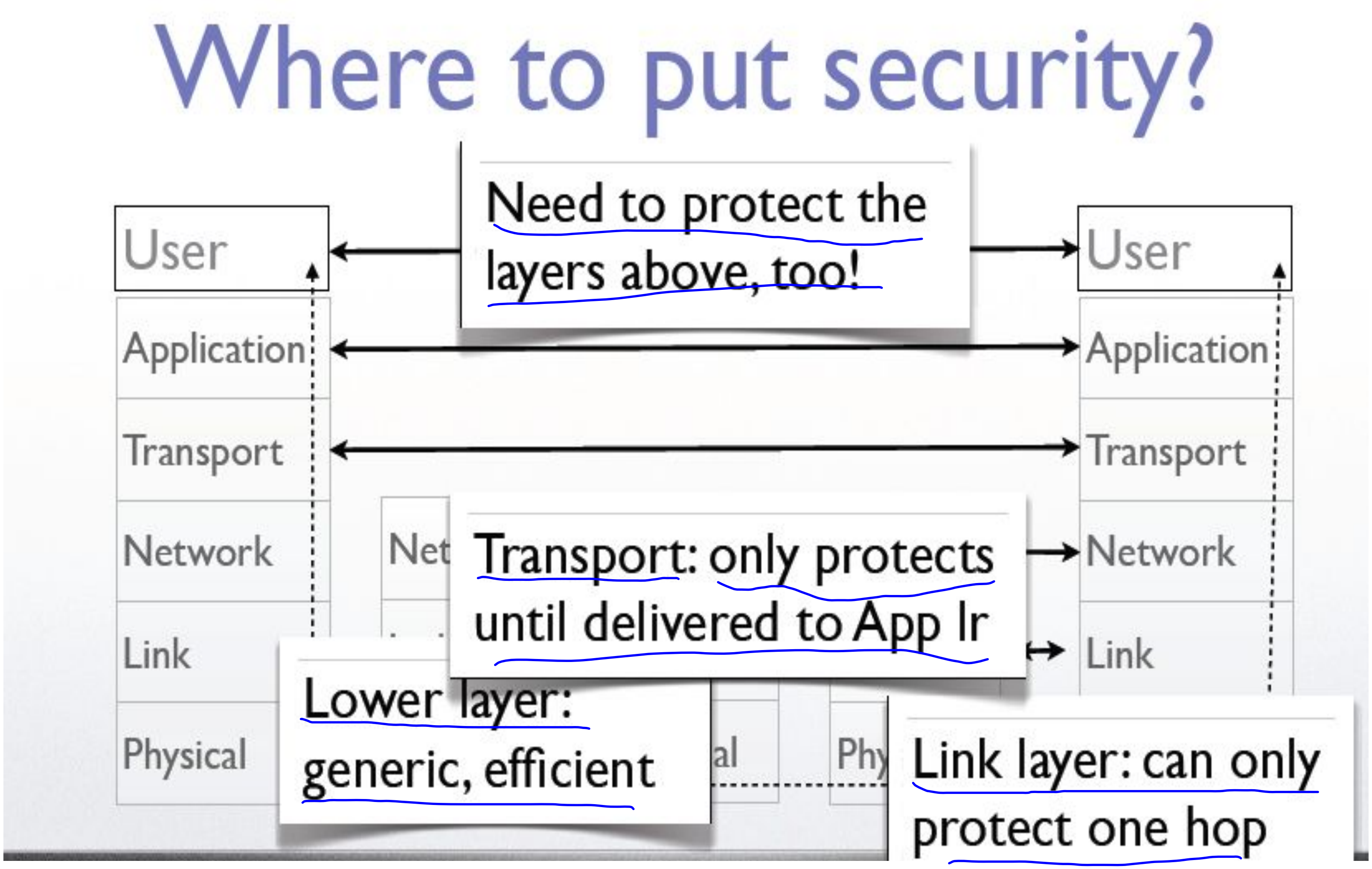
✓ Network (IP/ICMP, ...)

✓ Link (Ethernet, PPP, WLAN, Bluetooth, ...)

✓ Physical (cables, radio, infrared, ...)

Where to put security?

NETWORK LAYERS



Where to put security?

Need to protect the layers above, too!

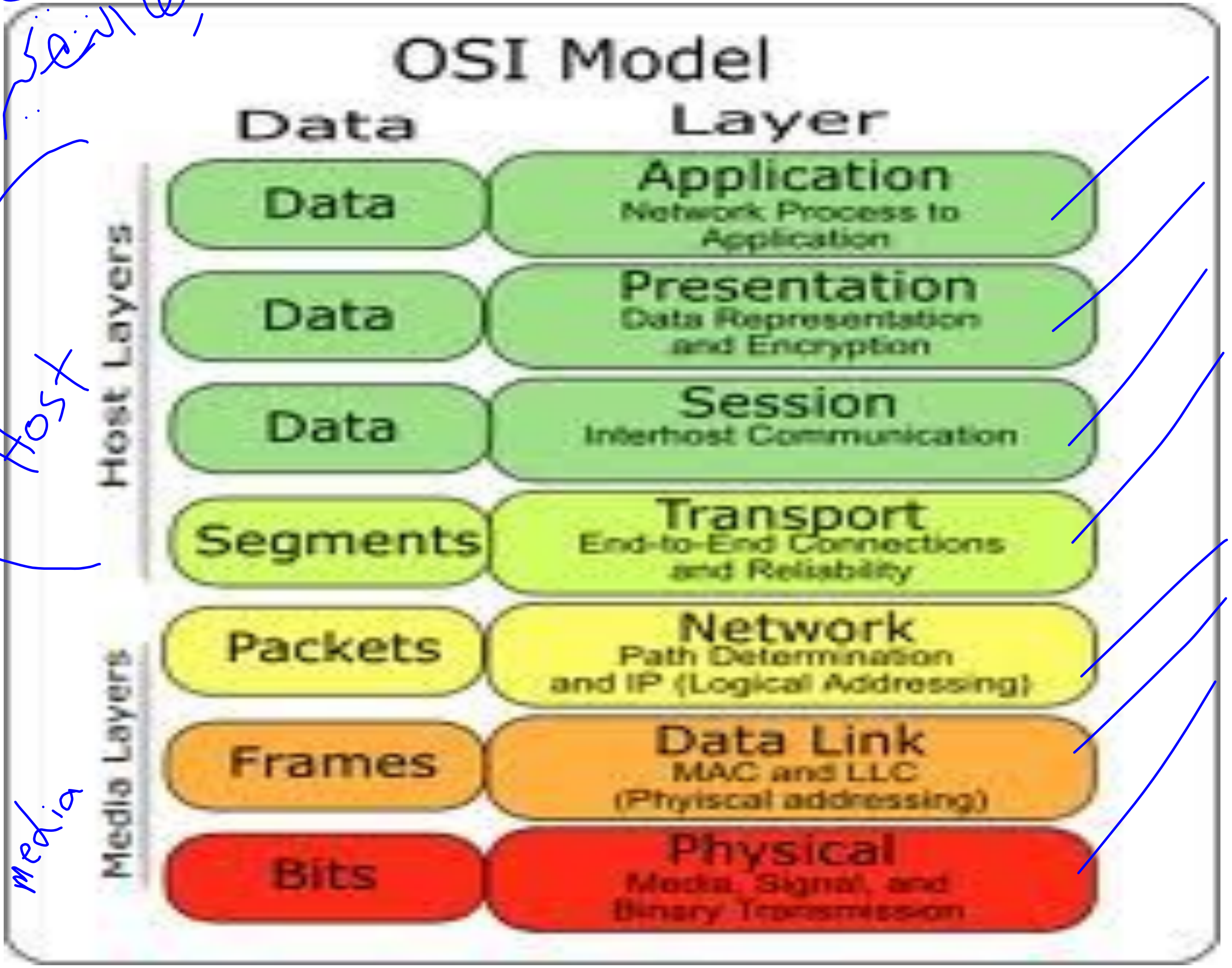
Transport: only protects until delivered to App lr

Lower layer: generic, efficient

Link layer: can only protect one hop

OSI MODEL

مهام الطبقات
هي التي تحمل
فيها المستخدم



OSI Model

	Data	Layer
Host Layers	Data	**Application** Network Process to Application
	Data	**Presentation** Data Representation and Encryption
	Data	**Session** Interhost Communication
	Segments	**Transport** End-to-End Connections and Reliability
Media Layers	Packets	**Network** Path Determination and IP (Logical Addressing)
	Frames	**Data Link** MAC and LLC (Phyiscal addressing)
	Bits	**Physical** Media, Signal, and Binary Transmission

Host

Media

EXAMPLE ATTACKS

Application layer:

- Email scams, “phishing”: ask for password
- Email spoofing: mail “from” anyone
- Modem hijacking
- DNS cache poisoning (attack host-based identification)

EXAMPLE ATTACKS

Transport layer:

- Denial of Service: e.g. SYN flooding
- Connection hijacking, ISN guessing
- Initial Sequence Number of TCP connection, “random nonce”

EXAMPLE ATTACKS

Network layer:

- IP spoofing: easy to fake source address, hard but not always impossible to see response (attacks address-based id)
- Routing attacks: spoofing, DoS “the best route anywhere is here!”

EXAMPLE ATTACKS

Link layer:

- Broadcast storms (DoS)
- MAC-address spoofing (local network)

ATTACK ENHANCEMENT

Distributed DoS attacks:

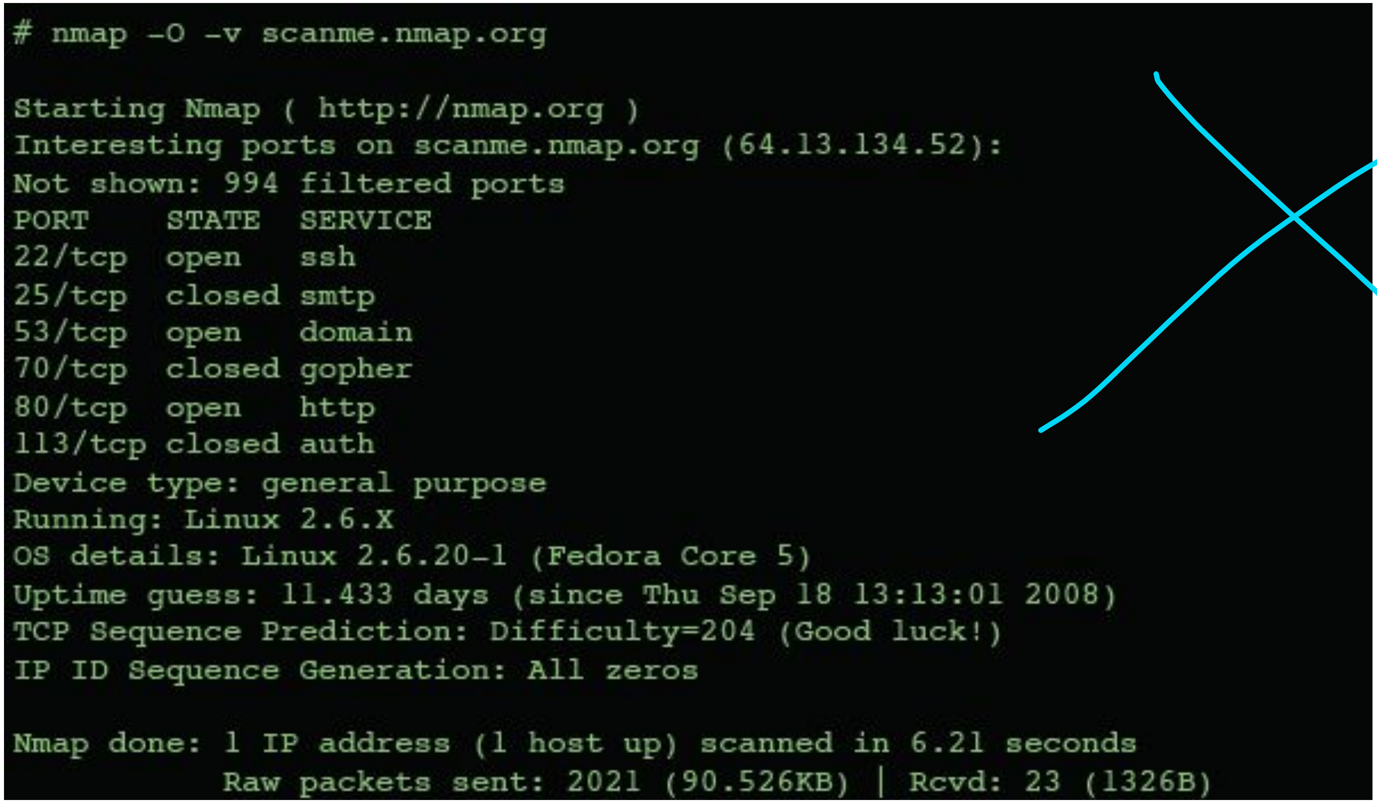
- Spread by viruses, creating “botnets” (remote-controlled PCs)
- Harder to trace and protect against
- Big business

ATTACK PREPARATION

Host fingerprinting:

- Remotely check properties of TCP/IP implementation, to find out what type of O.S./hardware and servers to attack
- e.g. detect Windows version

FINGERPRINT EXAMPLE



```
# nmap -O -v scanme.nmap.org

Starting Nmap ( http://nmap.org )
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 994 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
25/tcp   closed smtp
53/tcp   open   domain
70/tcp   closed gopher
80/tcp   open   http
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime guess: 11.433 days (since Thu Sep 18 13:13:01 2008)
TCP Sequence Prediction: Difficulty=204 (Good luck!)
IP ID Sequence Generation: All zeros

Nmap done: 1 IP address (1 host up) scanned in 6.21 seconds
           Raw packets sent: 2021 (90.526KB) | Rcvd: 23 (1326B)
```

PROTECTION APPLICATION LAYER

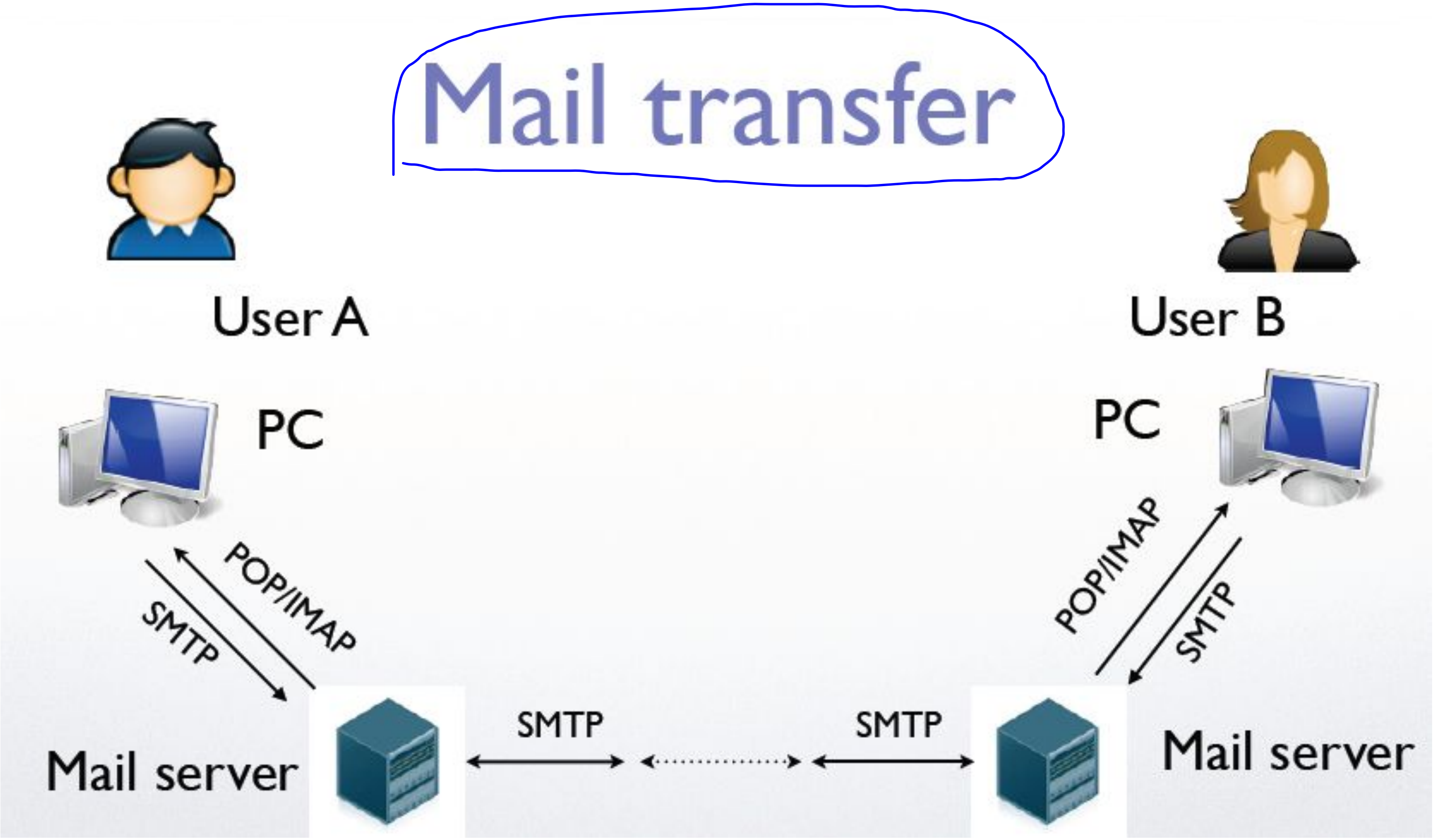
Secure email (S/MIME, PGP)

- Application-to-application (“user-to-user”) authentication, confidentiality, regardless of lower layers

Secure email transport:

- SMTP over TLS: conf/auth between mail servers, transport from source to dest
- IMAP/POP over TLS: conf/auth when client fetches mail from server

PROTECTION APPLICATION LAYER



PROTECTION APPLICATION LAYER

HTTP over TLS (“https:”)

- Confidentiality and authentication(unilateral or mutual) between browser and web server
- Note “attack from layer above”
- When data delivered to browser, no longer (or before sent from browser)

PROTECTION APPLICATION LAYER

DNS (Domain Name System)

- Translation host name – IP address (etc)

DNS security extensions:

- Data origin auth, integrity, key distribution
- Protect against e.g. cache poisoning
- Slowly being adapted

PROTECTION TRANSPORT LAYER

TLS (Transport Layer Security) (or SSL, Secure Sockets Layer)

- “layer between” app/transport, provides transparent auth/conf for any application using TCP, e.g. web browser/server

PROTECTION TRANSPORT LAYER

SASL (Simple Authentication and Security Layer)

- Authentication (optionally confidentiality) which can be “turned on” and negotiated in an already open connection
- Used e.g. in secure SMTP

PROTECTION TRANSPORT LAYER

Initial Sequence Number (ISN) selection

- Improved randomization of ISNs
- Protects against hijacking

PROTECTION NETWORK LAYER

VPN (Virtual Private Network)

- Create virtual network over unprotected Internet
- Typically tunneling: encapsulate and multiplex traffic over one secure connection
- Simple example: ssh port forwarding

IPSEC "SUBLAYER"

Sub-protocols

- IP Authentication Header (AH): integrity, data origin authentication, anti-replay
- Encapsulating Security Payload (ESP): confidentiality, limited traffic flow confidentiality, plus above

SA (security association): end-to-end logical connection (note: IP is connectionless)

PROTECTION LINK LAYER

WiFi networks (radio): easy to eavesdrop

- WEP: Wired Equivalent Privacy/Wireless Encryption Protocol - useless (broken in seconds)
- WPA: WiFi Protected Access - often useless
- WPA2 - less useless

Don’t rely on these - use higher-layer security

PROTECTION LINK LAYER

Protection against spoofing and interception in wired networks:

- Network topology and filtering switches
- Avoid broadcast communication

FIREWALLS

Design principle: Complete Mediation

- All traffic has to pass through firewall (including wireless, dial-up etc)

NAT (Network Address Translation): only ports in use can receive incoming traffic

Packet filtering

HONEYPOT

Honeypot: looks like a real system, attractive target

Harmless if attacked, not used for "real" work, but simulates real use "Trap" used to collect info about attacks and attackers

HACKING NETWORKS
PHASE 1: RECONNAISSANCE

Physical Break-In

Social Engineering

Phishing: fake email

Pharming: fake web pages

WhoIs Database

Domain Name Server Interrogations

HACKING NETWORKS
PHASE 2: SCANNING

War Driving: Can I find a wireless network?

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

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

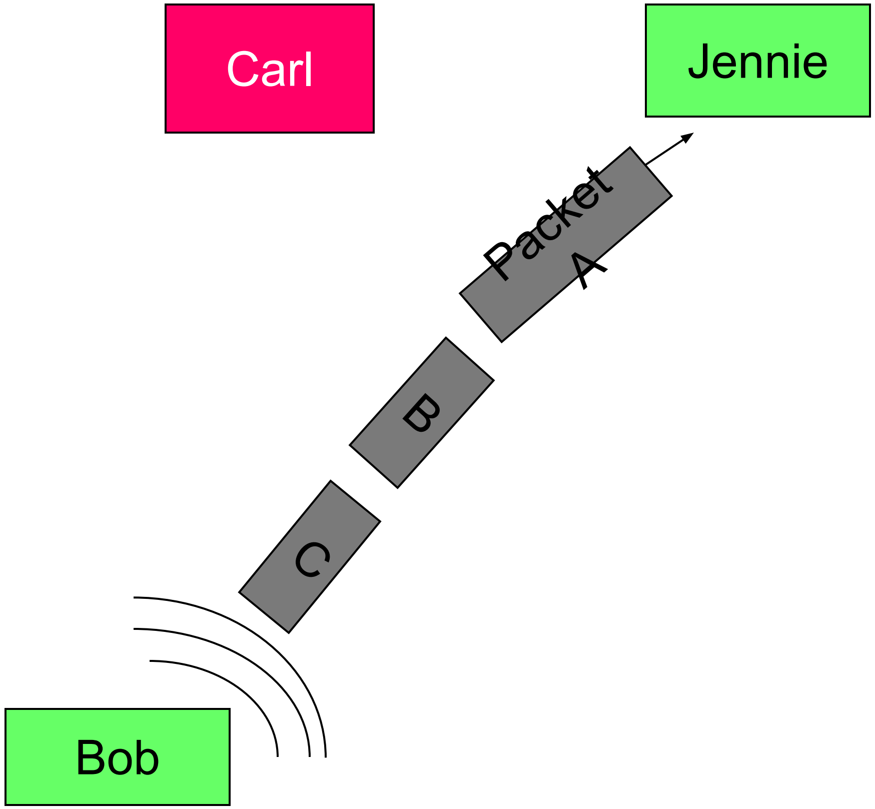
Vulnerability-Scanning Tools: What versions of software are implemented on devices?

PASSIVE ATTACKS

Eavesdropping: Listen to packets from other parties = Sniffing

Traffic Analysis: Learn about network from observing traffic patterns

Footprinting: Test to determine software installed on system = Network Mapping



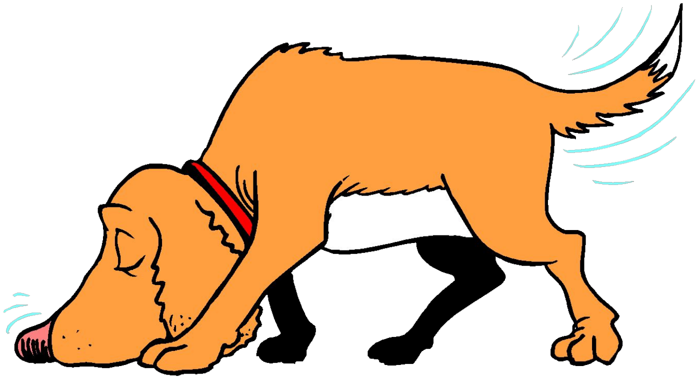
HACKING NETWORKS: PHASE 3: GAINING ACCESS

Network Attacks:

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

System Attacks:

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



Login: Ginger Password: Snap

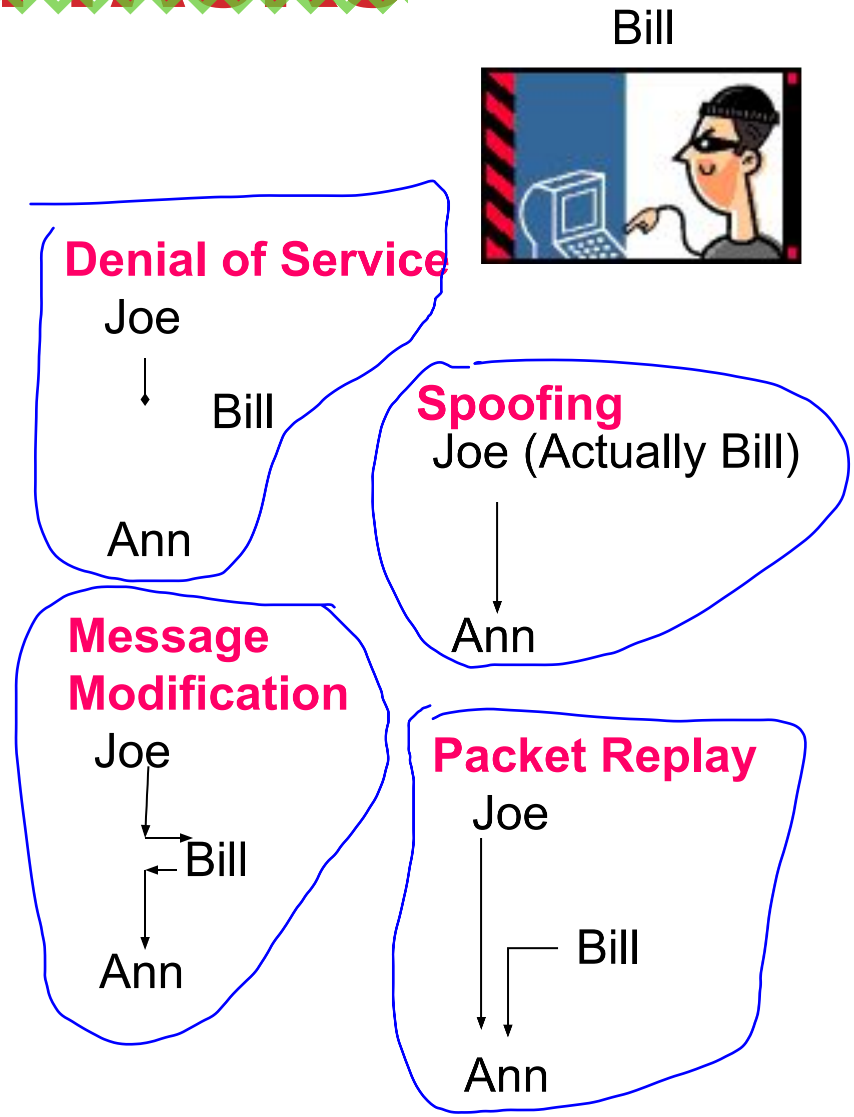
SOME ACTIVE ATTACKS

Denial of Service: Message did not make it; or service could not run

Masquerading or Spoofing: The actual sender is not the claimed sender

Message Modification: The message was modified in transmission

Packet Replay: A past packet is transmitted again in order to gain access or otherwise cause damage



Bill

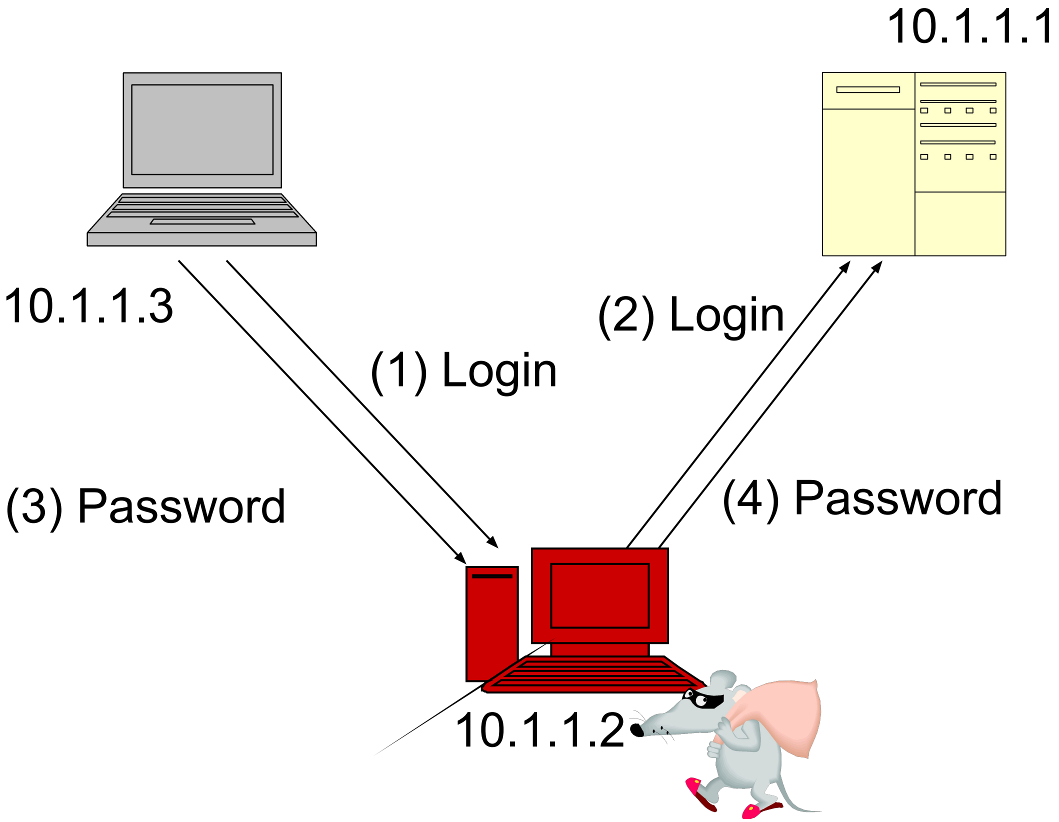
Denial of Service
Joe
Bill
Ann

Spoofing
Joe (Actually Bill)
Ann

Message Modification
Joe
Bill
Ann

Packet Replay
Joe
Bill
Ann

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

SQL INJECTION

Java Original: “SELECT * FROM users_table WHERE username=” + “’” + username + “’” + “ AND password = “ + “’” + password + “’”;

Inserted Password: Aa’ OR ‘’=’

Java Result: “SELECT * FROM users_table WHERE username=’anyname’ AND password = ‘Aa’ OR ‘ ‘ = ‘ ‘;

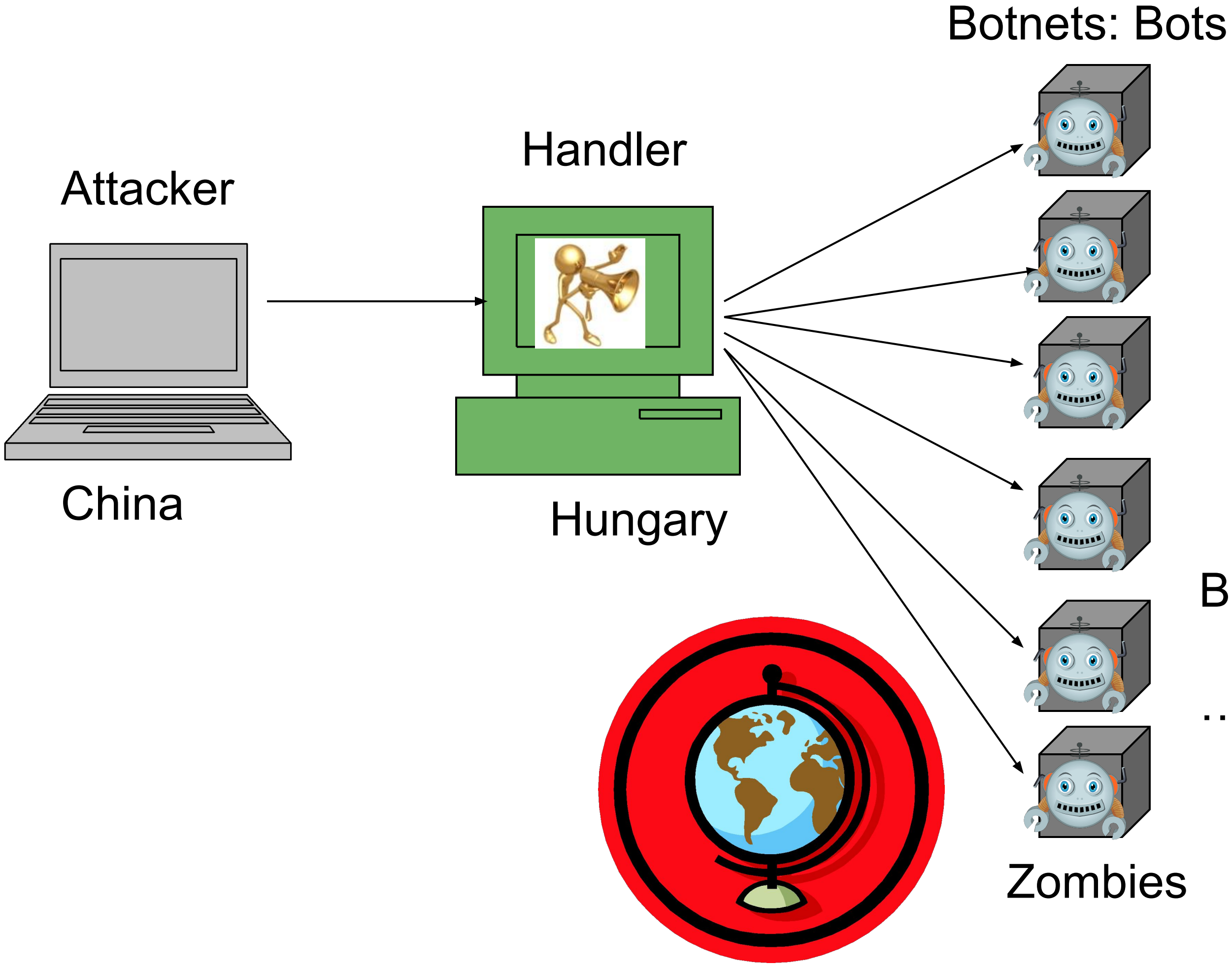
Inserted Password: foo’;DELETE FROM users_table WHERE username LIKE ‘%

Java Result: “SELECT * FROM users_table WHERE username=’anyname’ AND password = ‘foo’; DELETE FROM users_table WHERE username LIKE ‘%’

Inserted entry: ‘|shell(“cmd /c echo “ & char(124) & “format c:”)|’

Welcome to My System
Login:
Password:

BOTNETS



Botnets: Bots

Handler

Attacker

China

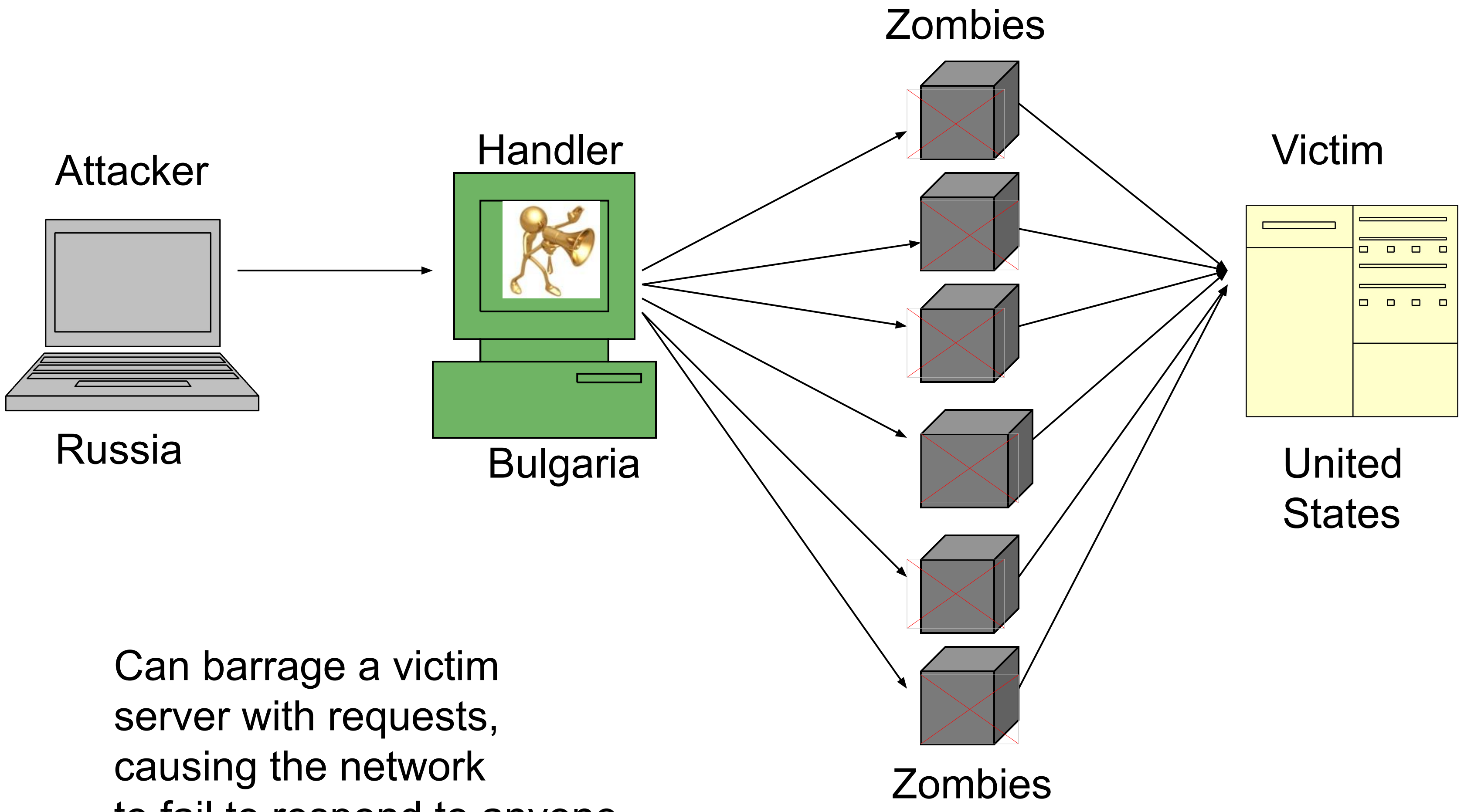
Hungary

Zombies

Bots: Host illegal movies, music, criminal web sites, …

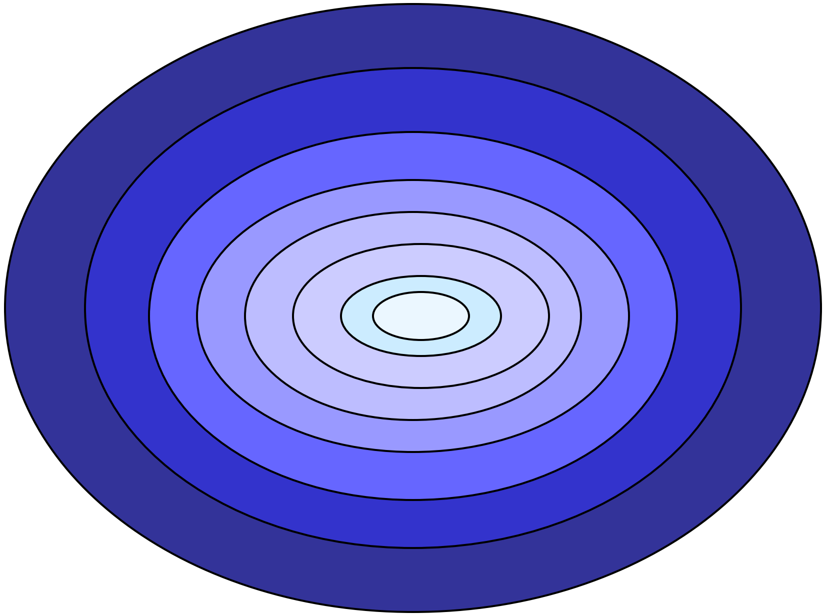
Forward Spam for financial gain

DISTRIBUTED DENIAL OF SERVICE



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

SECURITY: DEFENSE IN DEPTH



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

BASTION HOST

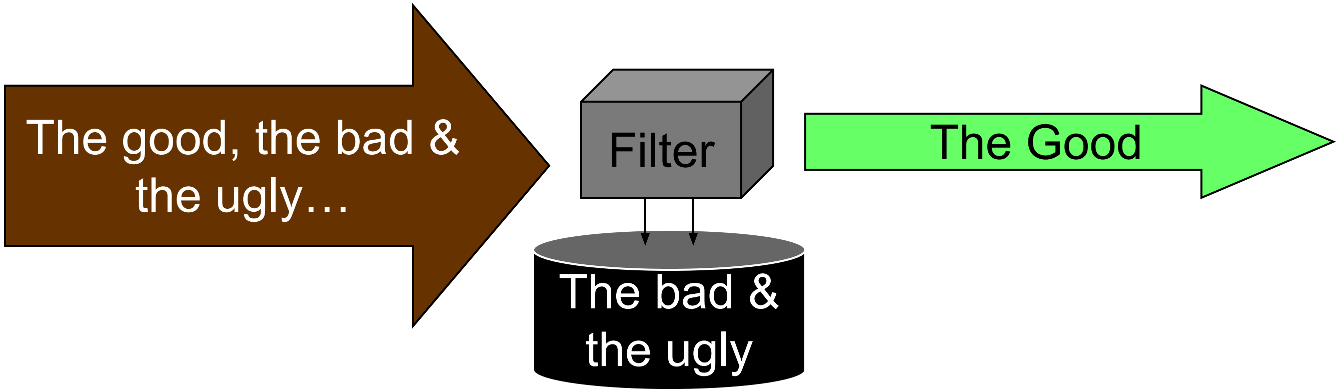
Computer fortified against attackers

Applications turned off

Operating system patched

Security configuration tightened

FILTERS



Route Filter: **Verifies sources and destination of IP addresses**

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

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

HONEYPOT & HONEYNET

Honeypot: A system with a special software application which appears easy to break into

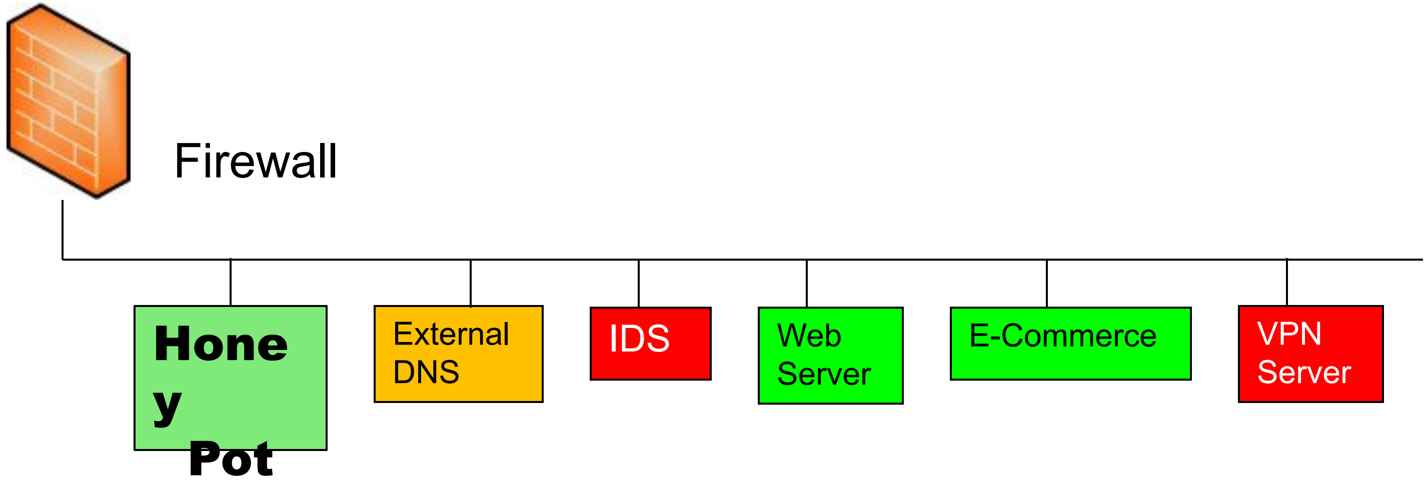
Honeynet: A network which appears easy to break into

Purpose: Catch attackers

All traffic going to honeypot/net is suspicious

If successfully penetrated, can launch further attacks

Must be carefully monitored



DATA PRIVACY

حلول الاسئلة
الموجودة في
30 صور تالية

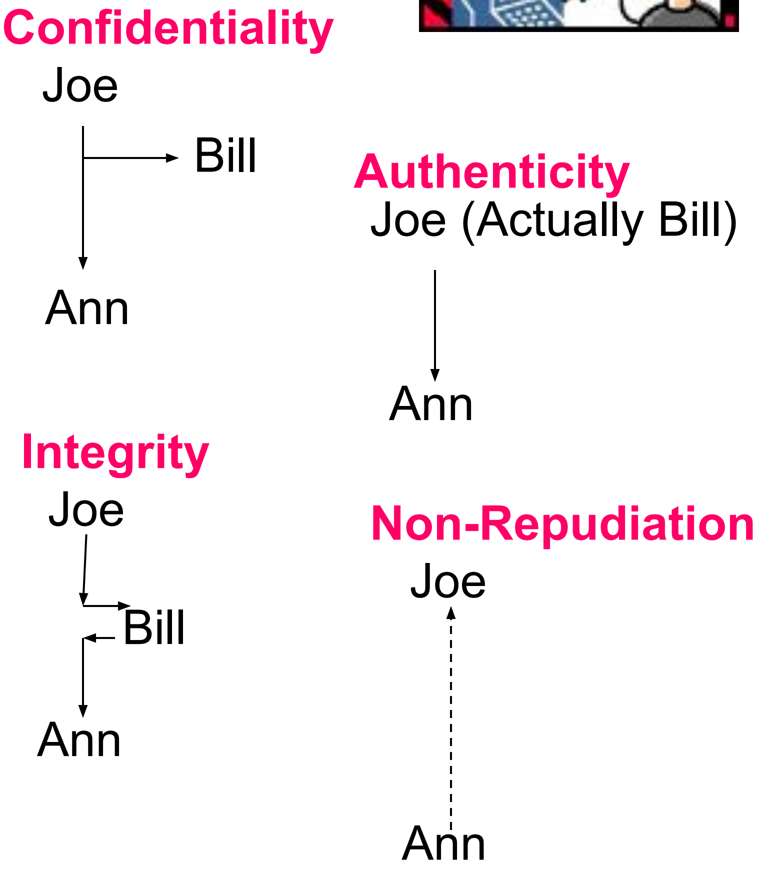
Confidentiality: Unauthorized parties cannot access information (->Secret Key Encryption

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)

Bill



Confidentiality
Joe
Bill
Ann
Authenticity
Joe (Actually Bill)
Ann
Integrity
Joe
Bill
Ann
Non-Repudiation
Joe
Ann