Network Security

Outline

1. Networking Fundamentals Quick Review
2. Network Security Treats
3. Network Security Controls

Networking Fundamentals Quick Review

Computer networks

- Support communication among computers
  - Hosts (computers), routers, network links, protocols
- Each machine has multiple addresses
  - MAC address, IP address
- Each message from the sender to receiver may stop at many intermediate hops till it reaches its destination (routing)

Terminology

- Packet
  - A chunk of data (usually < 1500 bytes) sent across a network
- Media Access Control (MAC) address
  - 48-bit number uniquely identifying a networked device
  - Assigned when the device is built and never changes
  - Only used on the local network
- IP address
  - A unique, 32-bit number identifying a computer on the network
- Port
  - 16-bit number identifying which application on a computer a packet is meant for
  - Some ports are assigned to specific protocols
    - 80 is http, 443 is https, 22 is SSH, etc.
- Protocols control sending, receiving of messages + define data format
  - e.g., TCP, IP, HTTP, 802.11

Internet protocol stack

- Formally there are 7-layers (OSI model) but can be simplified to 5 main layers
- Each layer has a specific function and faces unique security threats
- Each layer wraps the data using headers and footers

Application (HTTP, FTP, SSH)	• Interface for applications to communicate over a network • Define an application level protocol such as HTTP
Transport (TCP, UDP)	• Process data transfer between two hosts • Adds a header to tell where the packet goes on a computer (includes source and destination port)
Network (IP)	• Routing of datagrams from source to destination • Adds a header to tell the packet where to go on a larger network (includes source and destination IP)
Data Link (Ethernet, 802.11n)	• Data transfer between neighboring network elements • Adds a header to tell the packet where to go on the local network (includes source and destination MAC address)
Physical	• Bits “on the wire”

Summing Up

- There are 5 main networking layers
  - Application
  - Transport
  - Network
  - Link
  - Physical

- Each layer has a specific function and faces security unique threats

Network Threats

Network Security

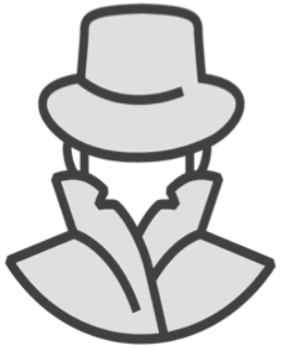
Network Security has two sides:

- **Protecting the network** from attack:
  - The network as the target of an attack
- **Protecting devices connected to the network** from being attacked
  - The network as the channel of attack
- Attacks could be:
  - Outbound
  - Inbound attacks (insider attack)

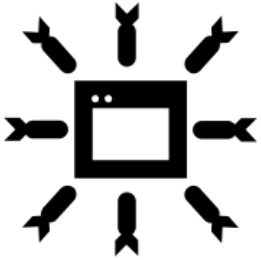
Key Network Attacks

Eavesdropping attacks
(intercept messages)

Masquerading attacks
e.g., fake (spoof) source address in packet



Man-in-the-middle attacks
(*Insert/update* messages into connection)



DoS / DDoS
(Flooding)

Hijacking: "take over" ongoing connection
(removing sender or receiver, inserting himself in place)

Eavesdropping example

screen dump of capture window after an FTP connection

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.46	192.168.1.1	DNS	Standard query A ftp.debian.org
2	0.156872	192.168.1.1	192.168.1.46	DNS	Standard query response A 128.101.240.212
3	0.203708	192.168.1.46	128.101.240.212	TCP	58408 > ftp [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1
4	0.311009	128.101.240.212	192.168.1.46	TCP	ftp > 58408 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 M
5	0.311128	192.168.1.46	128.101.240.212	TCP	58408 > ftp [ACK] Seq=1 Ack=1 Win=65535 Len=0 TSV=7
6	0.427572	128.101.240.212	192.168.1.46	FTP	Response: 220 saens.debian.org FTP server (vsftpd)
7	0.457218	192.168.1.46	128.101.240.212	TCP	58408 > ftp [ACK] Seq=1 Ack=43 Win=65535 Len=0 TSV=7
8	3.908879	192.168.1.46	128.101.240.212	FTP	Request: USER anonymous
9	3.995051	128.101.240.212	192.168.1.46	TCP	ftp > 58408 [ACK] Seq=43 Ack=17 Win=6144 Len=0 TSV=3
10	3.995621	128.101.240.212	192.168.1.46	FTP	Response: 331 Please specify the password.
11	4.058261	192.168.1.46	128.101.240.212	TCP	58408 > ftp [ACK] Seq=17 Ack=77 Win=65535 Len=0 TSV=
12	8.388059	192.168.1.46	128.101.240.212	FTP	Request: PASS ak@ak.org
13	8.473188	128.101.240.212	192.168.1.46	FTP	Response: 230-
14	8.473824	128.101.240.212	192.168.1.46	FTP	Response: 230-This site is just another one in a worldwid
15	8.659296	192.168.1.46	128.101.240.212	TCP	58408 > ftp [ACK] Seq=33 Ack=158 Win=65535 Len=0 TSV
16	8.751453	128.101.240.212	192.168.1.46	FTP	Response: 230-It is not the "primary Debian FTP site" – it
17	8.758911	192.168.1.46	128.101.240.212	FTP	Request: SYST

the three-way handshake

Observe the password and username

Main Treats Per Layer

- Threats at the Application Layer
  - Viruses, Spam, Malware, Ransomware
- Threats at the Network Layer
  - Ping of death
  - Traceroute misuse
- Threats at the Transport Layer
  - Denial of service
  - Port scanning
- Threats at the Data Link Layer
  - MAC Spoofing
  - ARP (Address Resolution Protocol) Poisoning
  - Man-in the-Middle (MITM) attacks

Wireless Communication Threats

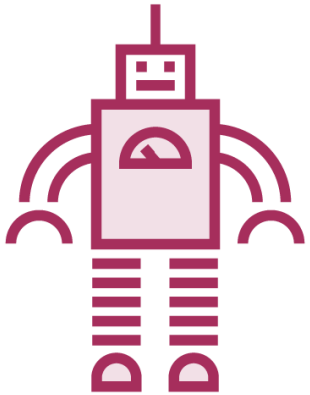
Interference (jamming)

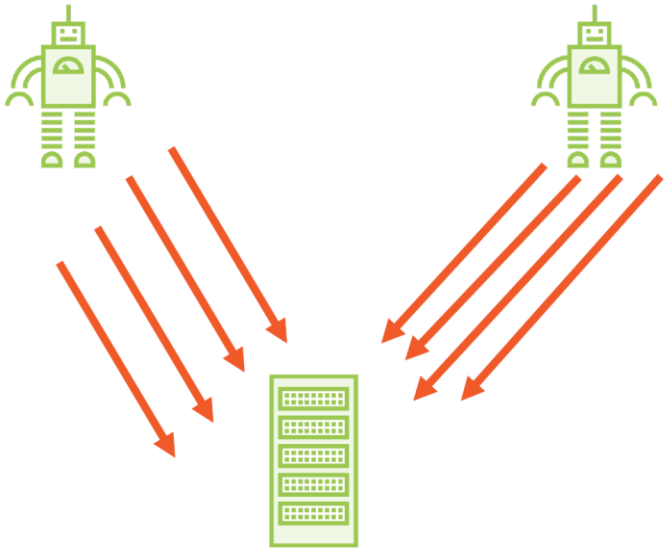
Flooding

Integrity

Authentication

Host Threats





- Remote unauthorized access
- Viruses
- Botnets
  - Robotically Controlled Networks
  - Command and Control
- Zombies
  - Can be used for DDoS

Attacks of Key Servers

- DNS Attacks
  - More details will be added
- Web Server Attacks
  - More details will be added

Countermeasures

Security goals of computer networks

- Counter various attacks
  - Confidentiality, Integrity, Availability
- Network security at different layers
  - Security measures at different layers
  - Many approaches rely heavily on crypto
  - See examples of what to do and what not to do…
  - It is not easy…

Controls

- Firewall
- IDS & IPS
- VPN
- Encryption (TLS)
- DDoS mitigation solutions
- Better administration
  - Backups
  - Change control
  - Patching

The Best Control Against Attacks

Education

Social Engineering awareness

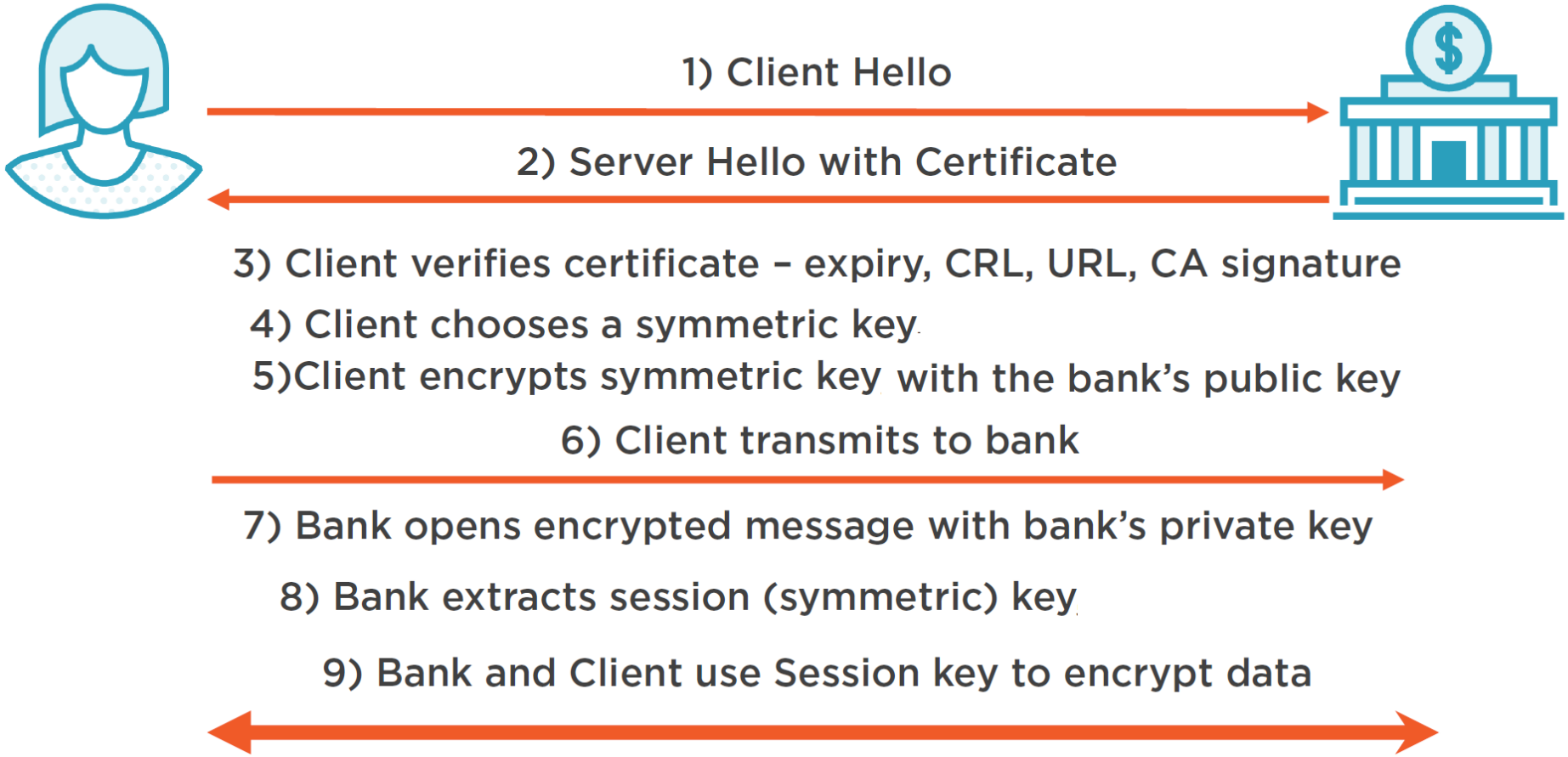
Knowledge of secure practices

Secure Network Communication

- Several means can be used to create secure connections
- Secure implementations require the use of valid protocols implemented correctly
- Secure implementations can provide trusted connections through less trusted environments

TLS

- Transport Layer Security is essential for ecommerce and trusted communications

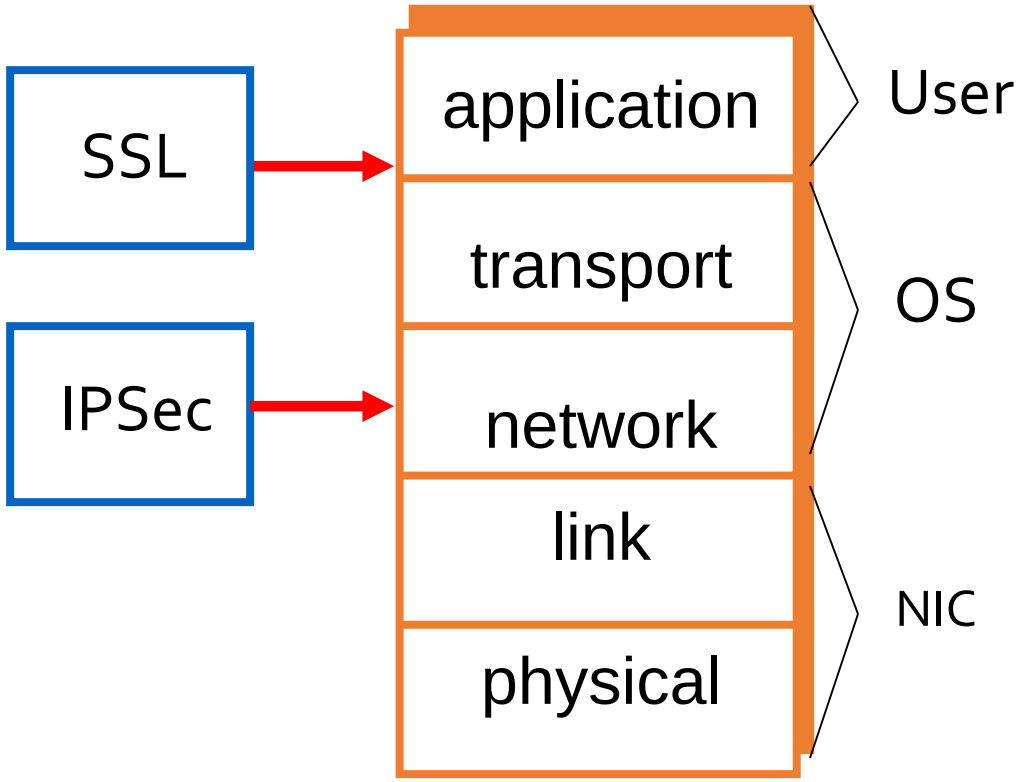


SSL vs IPSec

- SSL (and IEEE standard known as TLS)
  - Lives at socket layer (part of the app layer)
  - SSL: Apps must be aware, but not OS
  - Encryption, integrity, authentication, etc.
  - Relatively simple and elegant specification
- IPSec
  - Lives at the network layer (part of the OS)
  - IPSec often used in VPNs (secure tunnel)
  - Encryption, integrity, authentication, etc.
  - Is overly complex, has some security “issues”, hence not widely used

IPSec and SSL

- IPSec lives at the network layer
- IPSec is transparent to applications



Virtual Private Network (VPN)

- VPN extends a private network through (across) a public network
- Created by virtual point-to-point connection

- SSL/TLS

- IPSec: DataLink Layer Secure Communication

Key Points

- Attacker may:
  - Attack the network
  - Attack the devices connected to the network

- Networks must be protected at every layer
  - Do not expect a network layer control to effectively mitigate an application layer attack