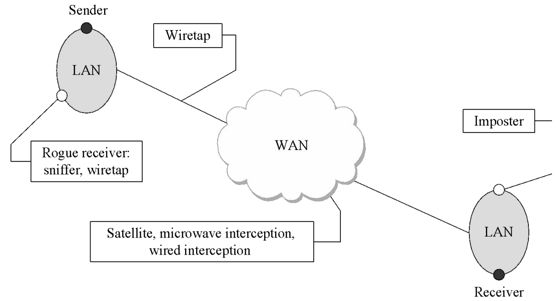
Network Security

COMP 435
Fall 2017
Prof. Cynthia Sturton


Sender
Wiretap
LAN
WAN
Imposter
Rogue receiver: sniffer, wiretap
Satellite, microwave interception, wired interception
LAN
Receiver

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Challenges

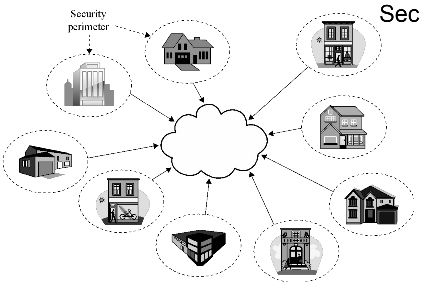
- Anonymity
- Many points of attack
- Sharing
- Complexity
- Unknown perimeter
- Unknown path

Media Complexity

Medium	**Strengths**	**Weaknesses**
Wire	● Cheap ● Ubiquitous	● Signal emanation ● Physical wiretapping
Optical Fiber	● No emanation ● No wiretapping	● Weak at connection points
Microwave	● Strong signal	● Interception possible ● Line of sight needed ● Needs repeaters
Wireless	● Ubiquitous	● Interception possible ● Short range
Satellite	● Strong signal	● Delay (long distance) ● Interception possible

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Security Perimeter



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Threats

- Interception
- Modification
- Fabrication
- Interruption

Dolev-Yao Model

Active Attacker:

- Can obtain any message on the network
- Is a legitimate user of the network
- Can be a receiver to any user

Dolev-Yao Model: Attacker carries the message

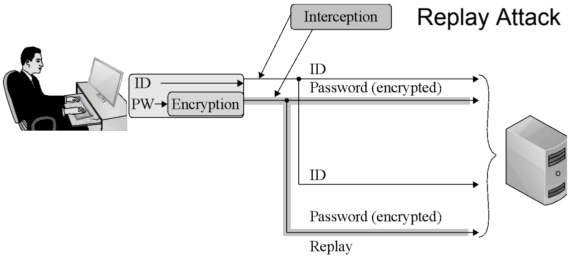
Interception Threats

- Wiretapping
- Eavesdropping

Modification & Fabrication Threats

- Data corruption
- Sequencing
- Substitution
- Insertion
- Replay

Replay Attack



From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Interruption Threats

- Excessive demain (Denial of Service attack)
- Routing failures
- Component failures

Denial of Service

Denial of Service

- Attack on availability
- Motivations
- Consequences

DoS Strategies

- Overload capacity
- Block access ransomware
- Component failure

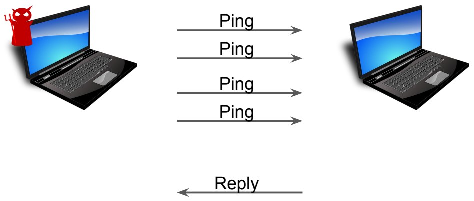
Overloading Capacity

- Ping of Death
- Smurf
- SYN Flood
- DDOS

Ping

- Internet Control Message Protocol (ICMP)
- Send & Reply
- Tests reachability and availability of destination

Ping of Death



Ping

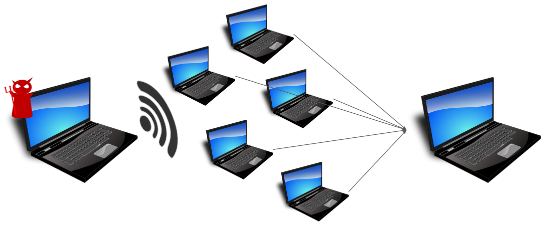
Ping

Ping

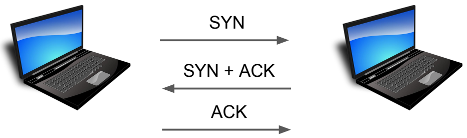
Ping

Reply

Smurf



TCP Protocol

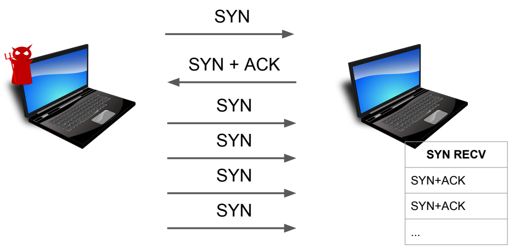


SYN

SYN + ACK

ACK

SYN Flood: Attack on TCP Protocol



SYN

SYN + ACK

SYN

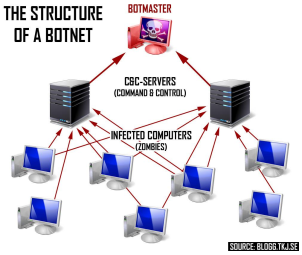
SYN

SYN

SYN

SYN RECV
SYN+ACK
SYN+ACK
...

Distributed Denial of Service

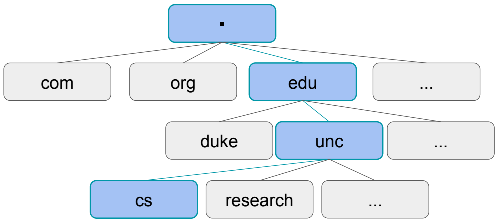


SOURCE: BLOGG.TKJ.SE

Blocking Access

- Ransomware
- DNS Spoofing
- DNS Cache Poisoning

Domain Name System (DNS)



.

com

org

edu

...

duke

unc

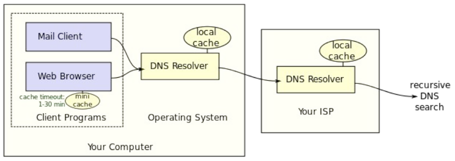
...

cs

research

...

Domain Name System (DNS)



By Lion Kimbro - Own work, Public Domain, https://commons.wikimedia.org/w/index.php?curid=386501

DNS Spoofing

Attacker responds to a DNS query with incorrect mapping

DNS Cache Poisoning

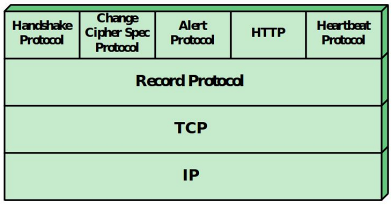
Incorrect name-to-address translation is stored in the translation cache

Ransomware

- Resource held for ransom
- Motivation
- Consequences
- Countermeasures

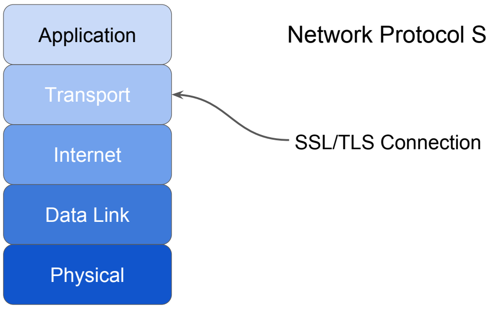
TLS & SSL

SSL and TLS

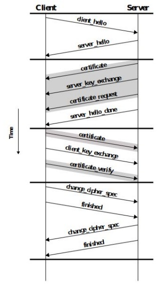


Computer Security: principles and practice, 3rd edition. Stallings and Brown

Network Protocol Stack



TLS Handshake

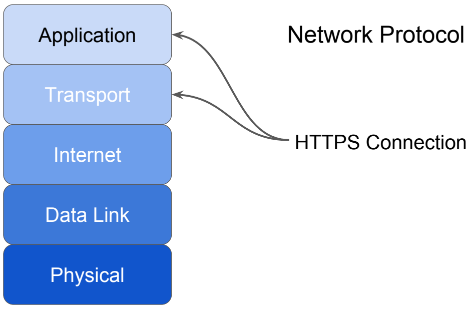


Computer Security: principles and practice, 3rd edition. Stallings and Brown

HTTPS: TLS over HTTP

- Secure communication between browser and server
- Authenticates the server
- Built into all modern browsers

Network Protocol Stack



Attacks on TLS

- Downgrade
- Heartbleed