Network Security

COMP 435
Fall 2017
Prof. Cynthia Sturton

Challenges

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

Media Complexity

<table>
<thead>
<tr>
<th>Medium</th>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wire</td>
<td>Cheap</td>
<td>Signal emanation</td>
</tr>
<tr>
<td></td>
<td>Ubiquitous</td>
<td>Physical wiretapping</td>
</tr>
<tr>
<td>Optical Fiber</td>
<td>No emanation</td>
<td>Weak at connection points</td>
</tr>
<tr>
<td></td>
<td>No wiretapping</td>
<td></td>
</tr>
<tr>
<td>Microwave</td>
<td>Strong signal</td>
<td>Interception possible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Line of sight needed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Needs repeaters</td>
</tr>
<tr>
<td>Wireless</td>
<td>Ubiquitous</td>
<td>Interception possible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Short range</td>
</tr>
<tr>
<td>Satellite</td>
<td>Strong signal</td>
<td>Delay (long distance)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Interception possible</td>
</tr>
</tbody>
</table>
Security Perimeter

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

Interruption Threats

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

SYN
SYN + ACK
ACK

TCP Protocol

Smurf

SYN
SYN + ACK
ACK
SYN Flood: Attack on TCP Protocol

SYN RECV
SYN+ACK
SYN+ACK
...

Distributed Denial of Service

THE STRUCTURE OF A BOTNET

Blocking Access

- Ransomware
- DNS Spoofing
- DNS Cache Poisoning

Domain Name System (DNS)
Domain Name System (DNS)

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
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