WIRELESS NETWORK SECURITY

Lois Lo
WHAT IS WIRELESS SECURITY

• Protects a wireless network from unauthorized and malicious access attempts.
• Delivery of wireless security
• Importance:
  - Vulnerability of Wireless network:
  ➔ The broadcast nature of the wireless medium
  - Wireless vs Wired Networks
<table>
<thead>
<tr>
<th>Security Requirements</th>
<th>Specific Objectives to be Achieved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticity</td>
<td>Specified to differentiate authorized users from unauthorized users</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Specified to limit the confidential data access to intended users only</td>
</tr>
<tr>
<td>Integrity</td>
<td>Specified to guarantee the accuracy of the transmitted information without any falsification</td>
</tr>
<tr>
<td>Availability</td>
<td>Specified to make sure that the authorized users can access wireless network resources anytime and anywhere upon request</td>
</tr>
</tbody>
</table>
STRUCTURE OF THE WIRELESS ENVIRONMENT

- Wireless Client
- Wireless access point
- Transmission Medium
Adopts the open systems interconnection (OSI) protocol architecture

- Application layer
- Transport layer
- Network layer
- Medium access control layer (MAC)
- Physical layer
## PHY ATTACKS

### TABLE III

**Main Types of Wireless Attacks at the PHY Layer.**

<table>
<thead>
<tr>
<th>PHY Attacks</th>
<th>Characteristics and Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eavesdropping</td>
<td>Interception of confidential information [71]</td>
</tr>
<tr>
<td>Jamming</td>
<td>Interruption of legitimate transmission [72]</td>
</tr>
</tbody>
</table>
### MAC ATTACKS

**TABLE IV**

**Main Types of Wireless Attacks at the MAC Layer.**

<table>
<thead>
<tr>
<th>MAC Attacks</th>
<th>Characteristics and Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC spoofing</td>
<td>Falsification of MAC address [73]</td>
</tr>
<tr>
<td>Identity theft</td>
<td>Stealing of a legitimate user's MAC identity</td>
</tr>
<tr>
<td>MITM attack</td>
<td>Impersonation of a pair of communicating nodes [74]</td>
</tr>
<tr>
<td>Network injection</td>
<td>Injection of forged network commands and packets [75]</td>
</tr>
</tbody>
</table>
## NETWORK ATTACKS

### TABLE V

**Main Types of Wireless Attacks at the Network Layer.**

<table>
<thead>
<tr>
<th>Network Attacks</th>
<th>Characteristics and Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP spoofing</td>
<td>Falsification of IP address [76]</td>
</tr>
<tr>
<td>IP hijacking</td>
<td>Impersonation of a legitimate user’s IP address [77], [78]</td>
</tr>
<tr>
<td>Smurf attack</td>
<td>Paralyzation of a network by launching a huge number of ICMP requests [79]</td>
</tr>
</tbody>
</table>
### TABLE VI

**Main Types of Wireless Attacks at the Transport Layer.**

<table>
<thead>
<tr>
<th>Transport Attacks</th>
<th>Characteristics and Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP flooding</td>
<td>Sending a huge number of ping requests [80], [81]</td>
</tr>
<tr>
<td>UDP flooding</td>
<td>Launching an overwhelming number of UDP packets [82]</td>
</tr>
<tr>
<td>TCP sequence prediction attack</td>
<td>Fabrication of a legitimate user’s data packets using the predicted TCP sequence index</td>
</tr>
</tbody>
</table>
## TABLE VII
**Main Types of Wireless Attacks at the Application Layer.**

<table>
<thead>
<tr>
<th>Application Attacks</th>
<th>Characteristics and Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware attack</td>
<td>Malicious software in the form of code, scripts and active content programmed by attackers [85]</td>
</tr>
<tr>
<td>SQL injection</td>
<td>Inserting rogue SQL statements attempting to gain unauthorized access to legitimate websites</td>
</tr>
<tr>
<td>Cross-site scripting</td>
<td>Injecting client-side scripts into web pages for bypassing some of the access control measures</td>
</tr>
<tr>
<td>FTP bounce</td>
<td>Impersonating a legitimate user to gain unauthorized access [83]</td>
</tr>
<tr>
<td>SMTP attack</td>
<td>Malicious attacks in e-mail transferring between the SMTP servers and clients</td>
</tr>
</tbody>
</table>
Wireless Attacks

- Application attacks
- Transport attacks
- Network attacks
- MAC attacks
- PHY attacks

Comparison

- same
- different

Wired Attacks

- Application attacks
- Transport attacks
- Network attacks
- MAC attacks
- PHY attacks
EAVESDROPPING
WIRELESS JAMMING ATTACKS

• 1) constant jammer, where a jamming signal is continuously transmitted;
• 2) intermittent jammer, where a jamming signal is emitted from time to time;
• 3) reactive jammer, where a jamming signal is only imposed, when the legitimate transmission is detected to be active;
• 4) adaptive jammer, where a jamming signal is tailored to the level of received power at the legitimate receiver;
• 5) intelligent jammer, where weaknesses of the upper-layer protocols are exploited for blocking the legitimate transmission.
IMPLICATION OF JAMMING ATTACKS

• What are susceptible?
• Air traffic communication systems,
• Vehicle platoons,
• The satellite navigation
• The power market
THE BAKU-TBILISI-CEYHAN (BTC) PIPELINE CYBER-ATTACK

- Example of jamming attack
- Initial attack vector: IP-based camera system

Systems that might have been compromised
- Camera system and communication network
- Leak detection system
- Automated pressure reliefs
- Alarm server or input traffic from field devices
- Pipeline field devices found in valve or compression stations (e.g. RTUs & PLCs)
- Satellite terminals or the actual transmission of signals
CHALLENGES AHEAD

• Mixed wireless attacks
• Cross-layer wireless security design
• 5G physical-layer security
• Field experiments
REFERENCES

https://Classroom.Udacity.com
http://blog.ifac-control.org/2017/06/15/jamming-attacks/