Wireless Security
COMP 435
Fall 2017
Prof. Cynthia Sturton

Administrative
- Course Evaluations close Wednesday 12/6
- Final Exam Saturday 12/9, 4-7PM, SN 014
- Poster Session Wednesday 12/4, 3:35-4:50, SN 014 & Lobby

Wireless Security
Access Point
Client
Transmission Medium

Wireless Security
Access Point
Client
NIC
**Network Interface Card (NIC)**

- Communicates radio signals with the Access Point (AP)
- Identified by MAC address
  - Medium Access Control
  - 48- or 64-bit
  - Ideally, fixed and unique

**Threats to Wireless Security**

- Association
- MAC Spoofing
- MITM
- Network Injection

---

**802.11 Protocol Stack**

- Physical
- Medium Access Control
- Logical Link Control
802.11 Protocol Stack

- Logical Link Control
- Medium Access Control
- Physical

Logical Link Control optionally does some book-keeping.

2.4 GHz radio signal band

802.11 Protocol Stack

- Logical Link Control
- Medium Access Control
- Physical

Creates WiFi Frames

WiFi Frames

- Header
- Data
- Frame Control
- Frame Type
- Sequencing
- Direction
- WEP
- Dest. MAC
- Src MAC
Management Frames

- Beacon
  - Advertises a network accepting connections
  - Service Set ID (SSID)
- Authentication
  - NIC's request to an AP
- Association
  - Follows authentication
  - Encryption agreed on

SSID

- 32-bit character
- Broadcast in Beacon Frame
- Included in ongoing communication

WiFi Protocol

- Beacon: SSID
- Authentication
- Accepts
- Association

Client Authentication

- Open Mode:
  - AP broadcasts beacon
  - Any client can request a connection
- Client authentication:
  - MAC addresses
- Attacks:
  - Inauthentic MACs
  - MAC spoofing
Server Authentication

- Closed Mode:
  - Client broadcasts connection request
  - Any AP can reply
- Server Authentication:
  - SSID
- Attacks:
  - Promiscuous AP
  - Leveraging preferred associations

Threat: Stealing the Association

WEP: Wired Equivalent Privacy

Authentication Request

Challenge

\[ \text{Enc}_K(\text{Challenge}) \]

Accept/Deny

WEP: Wired Equivalent Privacy

\[
\begin{align*}
\text{IV + key} & \quad \rightarrow \quad \text{RC4} \\
& \quad \rightarrow \quad \text{keystream} \\
& \quad \rightarrow \quad \text{1100} \\
& \quad \rightarrow \quad \text{1001} \\
& \quad \rightarrow \quad \text{Cipher text}
\end{align*}
\]
WEP Insecurity

- 40 or 104-bit key
- Users have to enter key
  - HEX strings
    0xb0fa93ad712df8321ac39decbd
  - ASCII strings
    s8j3ls.pc9gl5
- Keys are not chosen uniformly at random from key space

WEP Insecurity: Weak Encryption Algorithm

IV + key → seed → RC4 → keystream

\[
\begin{array}{c}
0 & 1 & 0 & 1 \\
\oplus
\end{array}
\begin{array}{c}
1 & 1 & 0 & 0 \\
\oplus
\end{array}
\begin{array}{c}
1 & 0 & 0 & 1 \\
\end{array}
\]

Plain text → Cipher text

WEP Insecurity

- Key changes infrequently
- Susceptible to brute force

WEP Insecurity

- SSIDs are known identities
- MACs are spoofable
- Key is shared by all on the network
WiFi Protected Access (WPA)

- Changing keys
- Authentication
- AES
- Stronger, encrypted integrity check

Attack on WPA: MITM

Attack on WPA: Malicious AP

Mobile Device Security
Threats to Mobile Devices

- Lack of physical control
- Personal devices (BYOD)
- 3rd party apps
- Auto-synching
- QR codes
- Location services

Buffer Overflow: a brief review

Compromised Stack

```plaintext
Procedure p1
{
    ...
    call p2;
    ...
}
```