Wireless Security 2
--WLAN and WSN
Outline

- Introduction to WLAN
- Security mechanisms in IEEE 802.11
- Attacks on IEEE 802.11
- Measures to strengthen WLAN security
- Conclusions
Introduction to WLAN

- WLANs are becoming increasingly popular, and promise to be the platform for many future applications:
  - Home entertainment networking

- Typical WLAN/WPAN technologies:
  - IEEE 802.11 & Bluetooth

WLAN End User Forecast (millions)
Introduction to WLAN
Introduction to WLAN

- Transmission range \( \leq 300 \text{ meters} \)
- High bandwidth
  - 802.11b up to 11Mbps
  - 802.11a/g up to 54Mbps
  - 802.11n \( \geq 100 \text{Mbps} \)
- Shared wireless channel
- IEEE 802.11 MAC protocols
  - Distributed Coordination Function (DCF)
  - Point Coordination Function (PCF)
- Infrastructure vs. ad hoc mode
Introduction to WLAN

Ad hoc mode

Client A

Client B

Client C
Introduction to WLAN

Infrastructure mode

Client A

Access point

Client B

Infrastructure mode
WLAN Security – Problem!!!

- Wireless networking is just radio communications
  - Hence anyone with a radio can eavesdrop and inject traffic
A Few Dumbest Ways to Secure a WLAN: Overview

- MAC “authentication”
- Disabling DHCP
- SSID “hiding”
- Antenna placement and signal suppression
MAC “Authentication”

- Use of the word “authentication” is laughable, all that’s happening is MAC address filtering
- MAC addresses are transmitted in clear text
- Extremely easy to capture
- Extremely easy to clone and defeat
- Extremely difficult to manage MAC filtering
Disabling DHCP

- Disabling DHCP and forcing the use of Static IP addresses is another common myth.
- IP schemes are easy to figure out since the IP addresses are sent over the air in clear text.
- Takes less than a minute to figure out an IP scheme and statically enter an IP address.
SSID “Hiding”

- No such thing as “hiding” an SSID, all that’s happening is Access Point beacon suppression
- Four other SSID broadcasts not suppressed
  - Probe requests/Probe responses
  - Association requests/Re-association requests
- SSIDs must be transmitted in clear text, otherwise 802.11 cannot function
Antenna Placement and Signal Suppression

- The hacker’s antenna is bigger than yours
- Directional high-gain antennas can pick up a weak signal from several kilometers away
- Lowering the signal hurts legitimate users a lot more than it hurts the hackers
IEEE 802.11 Security Mechanisms

- Service Set Identifier (SSID)
- MAC address filtering
- Wired Equivalent Privacy (WEP) protocol

802.11 products are shipped by the vendors with all security mechanisms disabled!!
SSID & Limitations

- A SSID is the unique name of a WLAN
- All packets on a WLAN should carry its SSID
- An extremely weak form of security - limit the network access to only the clients with knowledge of the SSID
  - Beacon frames containing SSID are always sent in the clear
  - A hacker can use analysis tools (e.g., AiroPeek) to identify SSID
  - Some vendors use default SSIDs which are pretty well known (e.g., CISCO uses tsunami)
  - Changes in SSID require communicating it to all legitimate mobile clients
MAC Address Filtering

- Control access by allowing only valid MAC addresses to access the network
- Pros
  - Provides a little stronger security than SSID
- Cons
  - Increases administrative overhead
  - Reduces scalability
  - Determined hackers can still break it by spoofing MAC addresses with software
Wired Equivalent Privacy (WEP)

- The industry’s solution: WEP (Wired Equivalent Privacy)
  - Share a single cryptographic key among all devices
  - Encrypt all packets sent over the air, using the shared key
  - Use a checksum to prevent injection of spoofed packets

(encrypted traffic)
WEP Security Requirements

- WEP had three main security goals
  - Confidentiality: To prevent casual eavesdropping
  - Access control: To prevent illegal access to a wireless network infrastructure
  - Data integrity: To prevent tampering with transmitted messages

- None of the three security goals are attained!!!
How WEP Works

IV → RC4

key

original unencrypted packet → checksum

encrypted packet

IV
WEP Access Control

- Before association, the STA (station) needs to authenticate itself to the AP (Access Point)
- Authentication is based on a simple challenge-response protocol:
WEP Integrity

- WEP integrity protection is based on an encrypted CRC value

- Operation
  - ICV (integrity check value) is computed and appended to the message
  - The message and the ICV are encrypted together
WEP Confidentiality

- WEP encryption is based on RC4 Algorithm
- For each message to be sent
  - Shared secret key between STA and AP is the same for each message
  - 24-bit IV changes for every message
  - RC4 produces a pseudo-random stream, which is XORed to the message
WEP Encryption

IV: Initial Vector
K: pseudo-random keystream
ICV: Integrity check value
WEP Blocks
RC4 Algorithm

- Developed by Ron Rivest, RSA labs, called Ron’s Code 4 (RC4)
- Symmetric: Same key is used in encryption and decryption
- Stream Cipher: Data is encrypted one byte at a time
- Synchronous: Key stream is generated separately from the plaintext
RC4 Algorithm (Two Elements)

- **Key Scheduling Algorithm (KSA):** Generates a random 256-value state array $S$, based on the secret key - $K$ (length $l \text{ bytes}$)
- **Pseudo-Random Generation Algorithm (PRGA):** Outputs a stream based on the KSA array $S$
Key Scheduling Algorithm (KSA)

- Input is key
- Output a random 256-value state array $S$

```plaintext
KSA(key)
for i from 0 to 255
    S[i] := i
Endfor

j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap(S[i], S[j])
endfor
```
The Pseudo-random Generation Algorithm (PRGA)

- Outputs a Pseudo-random stream

PRGA()

\[ i := 0 \]
\[ j := 0 \]

while GeneratingOutput:

\[ i := (i + 1) \mod 256 \]
\[ j := (j + S[i]) \mod 256 \]
\[ \text{swap}(S[i],S[j]) \]
\[ \text{output } S[(S[i] + S[j]) \mod 256] \]

endif
WEP Problems

- **Access Control**
  - Authentication is one-way only, AP is not authenticated to STA, STA is at risk to associate to a rogue AP
  - The same shared secret key is used for authentication and encryption

- **Integrity**
  - Possible for an attacker to flip selected bits of the message, and still have the message pass the ICV test

- **Confidentiality**
  - RC4 is always used in software implementation
  - IV reuse and weak key
A Property of RC4

- Keystream leaks, under known-plaintext attack
  - Suppose we intercept a ciphertext $C$, and suppose we can guess the corresponding plaintext $P$
  - Let $Z = \text{RC4}(\text{key, IV})$ be the RC4 keystream
  - Since $C = P \oplus Z$, we can derive the RC4 keystream $Z$:
    \[ P \oplus C = P \oplus (P \oplus Z) = (P \oplus P) \oplus Z = 0 \oplus Z = Z \]
- This is not a problem ... unless keystream is reused!
WEP Problems (Cont.): IV Reuse

- IVs are only 24 bits, so there are only $2^{24}$ unique IVs. After around 17 million messages, IVs are reused.

- This seemingly large IV space can be depleted quickly. On average reuse occurs after

$$2^{24} \text{ packets} \times \frac{1500 \text{ bytes}}{\text{packet}} \times \frac{8\text{ bits}}{1\text{ byte}} / 11\text{ Mbps} = 18,300 \text{ s} = 5\text{ hrs}$$

- Collisions occur when an IV is reused and so the same RC4 key stream is used to encrypt the data.

\[
c_1 = p_1 \oplus k \\
c_2 = p_2 \oplus k \\
c_1 \oplus c_2 = (p_1 \oplus k) \oplus (p_2 \oplus k) = p_1 \oplus p_2
\]
WEP Problems (Cont.): IV Reuse

- If IV’s repeat, confidentiality is at risk
  - If we send two ciphertexts \((C, C')\) using the same IV, then the xor of plaintexts leaks \((P \oplus P' = C \oplus C')\)
  - If we can guess one plaintext, the other is leaked
  - Lesson: If RC4 isn’t used carefully, it becomes insecure
WEP Problems (Cont.): IV Reuse

An example in binary:

- 01011010101 \text{ Plaintext 1}
- 10111100000 \text{ XOR Keystream}
- 11100100101 \text{ Ciphertext 1}

- 11100101010 \text{ Plaintext 2}
- 10111100000 \text{ XOR Keystream}
- 01011011010 \text{ Cipher Text 2}

- 11100100101 \text{ Cipher Text 1}
- 01011011010 \text{ Cipher Text 2}
- 10111111111 \text{ result of ciphertexts}

- 10111111111 \text{ result}
- 01011010101 \text{ XOR Plaintext 1}
- 11100101010 \text{ Plaintext 2}
WEP Problems (Cont.): Weak Key

- For some seed values (called weak key), the beginning of the RC4 output is not really random
- If a weak key is used, the first few bytes of the output reveals a lot of information about the key, so breaking the key is made easier
- Knowing plaintext before it is encrypted allows attackers to exploit the weak IVs and gain knowledge of the shared key
- WEP encryption can be broken by capturing a few million messages!
Some Facts

- 802.11 WEP standard released (1997)
- Simon, Aboba, Moore: some weaknesses (Mar 2000)
- Walker: Unsafe at any key size (Oct 2000)
- Borisov, Goldberg, Wagner: 7 serious attacks on WEP (Jan 30, 2001)
- NY Times, WSJ break the story (Feb 5, 2001)
Attack #1: Keystream Reuse

- WEP didn’t use RC4 carefully
- The problem: IV’s frequently repeat
  - The IV is often a 24-bit counter that starts at zero
  - Hence, rebooting causes IV reuse
  - Also, there are only 17 million possible IV’s, so after intercepting enough packets, there are sure to be repeats
- Implications: can eavesdrop on 802.11 traffic
  - An eavesdropper can decrypt intercepted ciphertexts even without knowing the key
Attack #2: Dictionary Attack

- Send IP traffic to a mobile client from an Internet host under the attacker’s control
- Intercept the ciphertext to obtain $RC4(K, IV)$
- Repeat until all the keystreams $RC4(K, IV)$s are known
- Be able to decrypt any intercepted packet using the correct $RC4(K, IV)$

Credits: Arbaugh, et al.
Attack #3: Packet Modification

- CRC is linear
  \[ \Rightarrow \text{CRC}(P \oplus \Delta) = \text{CRC}(P) \oplus \text{CRC}(\Delta) \]
  \[ \Rightarrow \text{the modified packet } (P \oplus \Delta) \text{ has a valid checksum} \]
- Attacker can tamper with packet \((P)\) without breaking RC4 and fear of detection

\[(P, \text{CRC}(P)) \oplus \text{RC4}(K) \oplus (\Delta, \text{CRC}(\Delta))\]
**Attack #4: Spoofed Packets**

- Attackers can inject forged 802.11 traffic
  - Learn $Z = RC4(K, IV)$ using Attack #2
  - Since the CRC checksum is unkeyed, you can then create valid ciphertexts that will be accepted by the receiver
- Attackers can bypass 802.11 access control
  - All computers attached to wireless net are exposed

$IV, (P, CRC(P)) \oplus Z$
Attack #5: Authentication Spoofing

- Shared-key authentication
  - The AP sends the mobile client a challenge which is a 128-byte random string in plaintext
  - The client responds with the same challenge encrypted using WEP
  - The authentication succeeds if the decryption of the response at the AP matches with the challenge

- It is easy to derive the keystream used to encrypt the response, which can then be used to create a proper response for a new challenge.
**Attack #6: IP Redirection**

- This attack works when the AP acts as an IP router with Internet connectivity
  - The attacker sniffs an encrypted packet off the air and modifies the IP destination address to be one controlled by the attacker using Attack #3
  - The AP will then decrypt the packet and sends it to the new destination
  - Thus the attacker can let the AP decrypt any packet he would like to know
Attack #7: Cracking the Key

- Some available tools
  - AirSnort: http://airsnort.shmoo.com/
  - WEPCrack: http://wepcrack.sourceforge.net/
  - WepLab: http://weplab.sourceforge.net/
  - dwepcrack: http://www.dachb0den.com/projects/dwepcrack.html
  - aircrack: http://www.cr0.net:8040/code/network/
Possible Improvements

- **IV Reuse**
  - Use longer IV space
  - Hash IV and shared key combination before sending through RC4

- **Weak Key**
  - Weak IVs can be filtered out
  - Discard first 256 outputs of RC4 algorithm to reduce correlation between input and output

- **Have additional protection:** Firewalls, Virtual Private Networks (VPNs)
War Driving/Walking

If the distance from the Access Point to the street outside is 1500 feet or less, then an Intruder could also get access – while sitting outside.
War-driving Expeditions

In one 30-minute journey using the Pringles can antenna, witnessed by BBC News Online, the security company I-SEC managed to find and gain information about almost 60 wireless networks.
War Chalking

- Practice of marking a series of symbols on sidewalks and walls to indicate nearby wireless access. That way, other computer users can pop open their laptops and connect to the Internet wirelessly.
Packet Sniffing

```
Packet Sniffing

```

```
<table>
<thead>
<tr>
<th>Packet</th>
<th>Source</th>
<th>Destination</th>
<th>BSSID</th>
<th>Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>00:A0:F8:0E:67:80</td>
<td>Broadcast</td>
<td>Broadcast</td>
<td>1.0</td>
</tr>
<tr>
<td>9</td>
<td>00:A0:F8:0E:67:80</td>
<td>Broadcast</td>
<td>Broadcast</td>
<td>1.0</td>
</tr>
<tr>
<td>10</td>
<td>00:60:1D:23:1D:5D</td>
<td>00:A0:F8:0E:67:80</td>
<td>00:60:1D:23:1D:5D</td>
<td>2.0</td>
</tr>
<tr>
<td>11</td>
<td>00:60:1D:23:1D:5D</td>
<td>00:A0:F8:0E:67:80</td>
<td>00:60:1D:23:1D:5D</td>
<td>2.0</td>
</tr>
<tr>
<td>12</td>
<td>00:60:1D:23:1D:5D</td>
<td>00:A0:F8:0E:67:80</td>
<td>00:60:1D:23:1D:5D</td>
<td>2.0</td>
</tr>
<tr>
<td>13</td>
<td>00:A0:F8:0E:67:80</td>
<td>Broadcast</td>
<td>Broadcast</td>
<td>1.0</td>
</tr>
<tr>
<td>14</td>
<td>00:60:1D:23:1D:5D</td>
<td>00:A0:F8:0E:67:80</td>
<td>00:60:1D:23:1D:5D</td>
<td>2.0</td>
</tr>
<tr>
<td>15</td>
<td>00:60:1D:23:1D:5D</td>
<td>00:A0:F8:0E:67:80</td>
<td>00:60:1D:23:1D:5D</td>
<td>2.0</td>
</tr>
<tr>
<td>16</td>
<td>00:A0:F8:0E:67:80</td>
<td>00:60:1D:23:1D:5D</td>
<td>00:60:1D:23:1D:5D</td>
<td>1.0</td>
</tr>
</tbody>
</table>
```

```
802.11 MAC Header

```
```
Jamming (Denial-of-Service)

- Broadcast radio signals at the same frequency as the wireless Ethernet transmitters - 2.4 GHz
- To jam, you just need to broadcast a radio signal at the same frequency but at a higher power.
- Waveform Generators
- Microwave
Replay Attack

Good guy Alice

Authorized WEP Communications

Eavesdrop and Record

Bad guy Eve

Good guy Bob

Play back selections
An Exercise in Wireless Insecurity

- Tools used:
  - Laptop with 802.11a/b/g card
  - Netstumbler
  - Aircrack (or any WEP cracking tool)
  - Ethereal
  - GPS
  - The car of your choice

From B. Lee et. al.
Step 1: Find Networks to Attack

- An attacker would first use Netstumbler to drive around and map out active wireless networks.
- Using Netstumbler, the attacker locates a strong signal on the target WLAN.
- Netstumbler not only has the ability to monitor all active networks in the area, but it also integrates with a GPS to map AP’s location.
WarDriving

WarDriving / Access Point Mapping

468 WEP
1,265 Clear
1,733 Total
Step 2: Choose the Network to Attack

- At this point, the attacker has chosen his target, most likely a business.
- Netstumbler can tell you whether or not the network is encrypted.
- Also, start Ethereal to look for additional information.
Step 3: Analyzing the Network

- Netstumbler tells me that SSID is ITwireless
- Multiple access points
- Many active users
- Open authentication method
- WLAN is encrypted with WEP
Step 4: Cracking the WEP key

- Attacker sets NIC drivers to Monitor Mode
- Begins capturing packets with Airodump
- Airodump quickly lists the available network with SSID and starts capturing packets
- After a few hours of airodump session, launch aircrack to start cracking!
- WEP key for ITwireless is revealed!
Step 5: Sniffing the Network

- Once the WEP key is cracked and the NIC is configured appropriately, the attacker is assigned an IP, and can access the WLAN
- Attacker begins listening to traffic with Ethereal
- Sniffing a WLAN is very fruitful because everyone on the WLAN is a peer, therefore you can sniff every wireless client
- Listening to connections with plain text protocols (in this case FTP and Telnet) to servers on the wired LAN yielded usable logins
Security Evaluations of WEP

- **WEP cannot be trusted for security**
  - Attackers can eavesdrop and spoof wireless traffic
  - Also can break the key with a few minutes of traffic
- **Attacks are serious in practice**
  - Attack tools are easily retrievable on the Internet
  - Hackers sitting in a van in your parking lot may be able to watch all your wireless data, despite the encryption
- **WEP is often not used anyway**
  - High administrative costs
  - WEP is turned off by default
Conclusion

- The bad news: 802.11 cannot be trusted for security
  - 802.11 encryption is readily breakable, and 50-70% of networks never even turn on encryption
  - Hackers are exploiting these weakness in the field

- The good news
  - Fixes (WPA, 802.11i) are on the way!

- Suggestions for securing your home 802.11
  - Use encryption
  - Don’t announce yourself
  - Limit access to your access point
More and Better Schemes

- **802.11i (WPA-2)**
  - Will require hardware upgrade
  - Uses new cipher (AES)
  - Provides final 802.11i standard
  - Offers forward compatibility with WPA

- **802.11 + WPA**
  - Uses today’s hardware
  - Replaces WEP (but not the cipher)
  - Incorporates key features of 802.11i
  - Includes firmware upgrade

- **802.11 + 802.1x**
  - Uses today’s hardware
  - Adds authentication through software upgrade
  - Leverages a RADIUS server with EAP

- **802.11 (WEP)**
  - Uses today’s hardware
  - Offers sufficient security for home use
  - Can use proprietary WEP enhancements
  - Can be augmented with VPN in enterprise and high-traffic environments
Access Point Setup

![Image of Linksys Wireless-G Broadband Router setup page]

Security Modes: You may choose from Disable, WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, RADIUS, WEP. All devices on your network must use the same security mode in order to communicate.

More...
Measures to Strengthen WLAN Security

- WPA: Wi-Fi Protected Access
  - An interim solution with backward compatibilities
  - Started in Apr. 2003 and becoming mandatory in Nov. 2003
- WPA enhances WEP in three ways
  - A message integrity code (MIC), in place of CRC to defeat message forgeries
  - A packet sequencing method to defeat replay attacks
  - Per-packet WEP encryption keys
- Installation of WPA include a firmware update and a driver upgrade
Measures to Strengthen WLAN Security

- IEEE 802.11i
  - The long-term solution towards 802.11 security
  - Ratified in June 2004

- Unique features
  - Use a single key to provide confidentiality and integrity to reduce key management overhead
  - Replace RC4 with AES as the encryption algorithm
  - Use counter mode for encryption
  - Use the Cipher Block Chaining Message Authentication Code (CBC-MAC) for integrity protection
  - Address all known WEP deficiencies, but require brand-new wireless cards and APs
History Repeats Itself...

Cell phones

1980 analog cellphones: AMPS

1990 digital: TDMA, GSM
- TDMA eavesdropping [Bar]
- more TDMA flaws [WSK]
- GSM cloneable [BGW]
- GSM eavesdropping [BSW,BGW]

2000 Future: 3rd gen.: 3GPP, ...

wireless networks

1999 802.11, WEP

2000 WEP broken [BGW]

2001 WEP badly broken [FMS]
- attacks pervasive

2002 WPA

2003 Future: 802.11i

wireless security: not just 802.11
Further Reading

- [http://www.cs.berkeley.edu/~daw/research/wireless.html](http://www.cs.berkeley.edu/~daw/research/wireless.html)
Wireless Sensor Network Security
Wireless Sensor Networks

- A wireless sensor network (WSN) is composed of a large number of low-cost sensor nodes randomly deployed to monitor the field of interest.

- **Sensor nodes**
  - Limited in energy, computation, and storage
  - Sense/monitor their local environment
  - Perform limited data processing
  - Communicate untethered over short distances

- **Sink**
  - Gather data from sensor nodes and connect the WSN to the outside world
Wireless Sensor Networks

sink
Wireless Sensor Networks

- Applications
  - Physical security for military operations
  - Indoor/outdoor environmental monitoring
  - Seismic and structural monitoring
  - Industrial automation
  - Bio-medical applications
  - Health and wellness monitoring
  - Inventory location awareness
  - Future consumer applications, e.g., smart homes
  - …
Security Requirements

- Message confidentiality
- Message authenticity & integrity
- Node mutual authentication
- More …
Design Challenges

- Shared wireless channel
  - Facilitate message eavesdropping & injection

- Resource constraints of sensor nodes
  - Battery, memory, computation, communication …

- Very large network scale (n*100 or n*1000)
  - Impossible to monitor each individual node
  - Nodes are subject to attacks such as captures

- Vulnerable protocol design
  - Security is often overlooked
#1 Sybil Attack

- A malicious node claims multiple identities
  - Severely interrupt routing, fair resource allocation, distributed storage, misbehavior detection …
  - Douceur (IPTPS’02), Newsome et al. (IPSN’04)
#2 Node Duplication Attack

- The attacker put clones of a captured node at random or strategic locations in the network
  - Parno et al. (SP’05)
#3 Random Walk Attack

- The attacker uses secret information of a captured node to roam in the network
#4 Sinkhole Attack

- Compromised node attracts traffic in a particular area by making itself attractive in terms of routing metric
- Then attacker can further the attack by selective forwarding, modifying, and dropping packets intended for the destination
#5 Wormhole Attack

- Attackers tunnel packets received at one location to another distant network location
  - Hu et al. (INFOCOM’03), Karlof et al. (SNPA’03)
- Allowing the attacker to
  - Disrupt routing, selectively drop packets, …
  - Build sinkhole based on wormhole
#6 Data Injection Attack

- The attacker continuously injects bogus data into the network via a captured node
  - Ye et al. (INFOCOM’04), Zhu et al. (SP’04)
- Allowing the attacker to
  - Deplete scarce energy of sensor nodes
  - Cause network congestion & false alarms
Neighbor-to-Neighbor Authentication

- Two neighboring nodes verify that the other party is who it claims to be
  - Chan et al. (SP’03)
- Otherwise, attackers can
  - Inject false data reports via good nodes
  - Distribute wrong routing information
  - Impersonate good nodes to misbehave

“A” → “Show me why you are B”
“Show me why you are A” → “B”
Key Agreement

- Two neighboring nodes establish a shared secret key known only to themselves
  - Eschenauer and Gligor (CCS’03), Chan et al. (SP’03), Liu and Ning (CCS’03), …
- The shared key is a prerequisite for
  - Message encryption/decryption
  - Message authentication

A → B
encrypt/ authenticate

encrypted message

secret key
Other Defense Techniques

- Secure location discovery
- Broadcast authentication
- Secure data aggregation
- Secure clock synchronization
- Secure routing and MAC protocols
- Intrusion detection
- ...
Security is a journey, not a destination!