Insecurity of 802.11
WEP Protocol

• **WEP** – Wired Equivalent Privacy
  - Wireless standard 802.11
  - Link layer

• Security goals:
WEP Protocol

- **WEP** – Wired Equivalent Privacy
  - Wireless standard 802.11
  - Link layer

- **Protocol goals:**
  - Confidentiality: prevent eavesdropping
  - Access control: prevent unauthorized access
  - Data integrity: prevent tampering of messages

- We show that none of the security goals are achieved
Network Model
WEP Algorithm Encryption

RC4: Rivest Cipher 4
Most widely used software stream cipher (used in SSL and WEP)
Designed by Ron Rivest of RSA Security in 1987
WEP Algorithm Decryption

IV \quad \text{Cipher} \quad \oplus \quad \text{RC4}(k,IV) \quad = \quad \text{Message} \quad \text{CRC}(M)
Confidentiality
Stream cipher properties

- Given two ciphers $C_1, C_2$ using the same $RC4(v,k)$, $C_1 \oplus C_2 = P_1 \oplus P_2$

- Two conditions required for this class of attacks to succeed:
Stream cipher properties

• Given two ciphers $C_1, C_2$ using the same $RC4(v,k)$, $C_1 \oplus C_2 = P_1 \oplus P_2$

• Two conditions required for this class of attacks to succeed:
  - Availability of ciphertexts where keystream is used more than once.
  - Partial knowledge of some of the plain texts.
Finding instances of keystream reuse

• Shared key $k$ changes rarely.
• Reuse of IV causes reuse of keystream.
• IV are public.
IV Usage

- **IV size is only 24 bits** \(\Rightarrow\) inherent limit
  - Busy access point of 5Mbps will exhaust available space in 11 hours.

- **Common practices make IV reuse more often**
  - Random IV selection
    - Birthday paradox: on random IV selection 5000 packets are needed to find a collision
  - Common PCMCIA cards set IV to zero and increment it by 1 for each packet \(\Rightarrow\) keystreams corresponding to low-valued IVs are reused many times
  - Standard only recommends but not requires change of IV on every packet
Exploiting keystream reuse

- Keystream reuse can lead to a number of attacks:
  - If plaintext of one message is known, the other is immediately obtainable.
  - In the general case, known techniques for breaking reused keystreams.
  - As the number of reused keystream increases breaking them becomes easier.
Exploiting keystream reuse

- Trial and errors
  - Many fields of IP traffic are predictable.
  - For example: login sequences.
- Send known text and sniff the encrypted text
- AP broadcast both encrypted and unencrypted form when subnet has both WEP and non-WEP clients
- As the number of reused keystream increases breaking them becomes easier.
Decryption dictionaries

• Once plaintext of encrypted message is obtained, keystream values stored in dictionary.
• Full table requires 24GB
• Size of dictionary does not depend on the size of key
Consequences of the Attack

• Compromise confidentiality of messages
• Compromise access control
• Compromise data integrity
Message Authentication

- Message modification
- Message injection
Message Modification

- Checksum used is CRC-32 which is a linear function of the message:

\[ \text{Checksum}(x \oplus y) = \text{Checksum}(x) \oplus \text{Checksum}(y) \]

- In other words, checksum distributes over the XOR operation.

- RC4 stream cipher also linear.
The attack

*Given C we would like to create C’ s.t. C’ decrypts to M’ instead of M.*

<table>
<thead>
<tr>
<th>Cipher</th>
<th>Δ</th>
<th>CRC(Δ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RC4(k,IV)</td>
<td>Δ</td>
<td>CRC(Δ)</td>
</tr>
<tr>
<td>Message</td>
<td>CRC(M)</td>
<td>CRC(M)</td>
</tr>
<tr>
<td>RC4(k,IV)</td>
<td>M’</td>
<td>CRC(M’)</td>
</tr>
</tbody>
</table>
Message Injection

- WEP checksum is an unkeyed function of the message.
- After knowing one keystream we can use it forever.

\[ C' = <M', CRC(M')> \otimes RC4(IV,k) \]

- It is possible to reuse old IV values without triggering any alarms at the receiver.
What are weaknesses of WEP?
Summary of Weakness

• **RC4 is efficient but not secure**
  - RC4 is linear
  - $C_1 \otimes C_2 = P_1 \otimes P_2 \Rightarrow$ Accurately inferring $P_1$ and $P_2$ allows you to get keystream

• **Frequent reuse of IV**
  - Inherent limit of 24-bit
  - Practical use: make reuse even more frequent

• **Poor key management**
  - Key is shared among many entities and rarely changes

• **All three security goals are violated**
  - Confidentiality
  - Access control
  - Data integrity
What are countermeasures?
Countermeasure

• Improve key management
  - Everyone has its own key
  - Prevent key reuse

• Use more secure cryptographic algorithms
• Use end-to-end security (e.g., VPN)
Conclusion

• Design of security protocols is difficult
  - Public review
• Combining several secure algorithms does not mean that the result is secure
• Engineering perspective dictated selection of cryptographic algorithms
802.11i (WPA)

Replacement of WEP

Properties
- Confidentiality
- Data origin authenticity
- Data integrity
- Replay protection
802.11i Components

Better encryption
- Temporal key integrity protocol (TKIP)
  - Changes temporal keys every packet
  - Still uses RC4 to perform encryption
  - Inter-operate with WEP
- Advanced encryption standard (AES)
  - Requires a coprocessor to operate ➔ new hardware
- Stronger message authentication code (MAC)

Key management
- Pre-shared key: easier to setup
- 802.1x
802.1x

- Provide authentication framework for WLANs
  - Client-only
  - Strong mutual authentication

- Use Extensible Authentication Protocol (EAP) to authenticate users
1: Association request
2: Association response
3: EAPOL-Start
4: Request/Identity
5: EAP-Response/Identity
6: EAP-Request
7: EAP-Response
8: EAP-Success
9: EAPOL-Key (WEP)

Authenticator
802.11

5: Radius-Access-Request
6: Radius-Access-Challenge
7: Radius-Access-Challenge
8: Radius-Access-Accept

Distribute dynamic key for WEP
Sharing Wireless Infrastructure

• Multi-provider access points can be shared among different service providers
  - Each network has its own SSID
  - 802.1x allows APs to implement different policies
Virtual Private Network (VPN)

• Even IEEE 802.11i and 802.11x are insufficient

• Only VPN technologies (IPSEC, TLS, SSL) can satisfy end-to-end security requirements in public domains

• VPN technologies might even be used in corporate networks