Intercepting Mobile Communications: The Insecurity of 802.11

Nikita Borisov, Ian Goldberg, David Wagner

Presenter: Xin Li
Outline

- Overview of 802.11
- Introduction to WEP (Wired Equivalent Privacy)
- WEP Encryption/Decryption Algorithm
- Attacks
- Conclusion
802.11 Wireless Networks

Two modes of operation:

1) Independent Basic Service Set (IBSS), aka ad-hoc mode

1) Basic Service Set (BSS), aka infrastructure mode
Introduction to WEP

- 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
- Security “relies on the difficulty of discovering the secret key through a brute-force attack”
- We show that none of the security goals are attained
**WEP Encryption/Decryption Algorithm**

\[ \begin{align*}
&\text{P(Plaintext)} \\
&\text{IV} \quad \oplus \quad \text{Message} \quad \text{CRC(M)} \\
&\oplus \\
&\text{RC4(k,IV)} \\
&\oplus \\
&\text{IV} \quad \oplus \quad \text{Cipher} \\
&\text{CRC(M)} \quad \oplus \quad \text{Message}
\end{align*} \]

- \( K \) is secret key between communicating parties
- (standard: 40 bit, extended 104 bit)
- \( V \) is initialization vector (IV) for RC4 (24 bit)
- keystream is long sequence of pseudorandom bits
- checksum re-computed to ensure only frames with valid checksums are accepted
The Risks of keystream reuse

If and then

\[ C_1 = P_1 \oplus \text{RC4}(v, k) \]
\[ C_2 = P_2 \oplus \text{RC4}(v, k) \]

\[ C_1 \oplus C_2 = (P_1 \oplus \text{RC4}(v, k)) \oplus (P_2 \oplus \text{RC4}(v, k)) \]
\[ = P_1 \oplus P_2. \]

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.

Note: There are known technologies to recover \( P_1 \) and \( P_2 \) from \( P_1 \oplus P_2 \).

As the number of reused keystream increases breaking them becomes easier.
Finding instance of keystream reuse

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

- We call such a reuse of an IV value a “collision”
IV Usage

- Standard recommends (but not requires) change of IV.
- Common PCMCIA cards sets IV to zero and increment it by 1 for each packet.
- IV size is only 24 bits.
- Busy access point of 5Mbps will exhaust available space in 11 hours.
- Birthday paradox: on random IV selection 5000 packets are needed to find a collision.
Keystream obtaining

- Many field of IP traffic are predictable
  - Eg. Login sequence, shared library
- Transmitting known plaintext.
  - Sending IP traffic directly to a mobile host from an Internet host
- Decryption Dictionary
  - 1500 bytes for each of the $2^{24}$ possible IV (24 GB)
  - 40 bit v.s. 24 bit v.s. 104 bit
  - Shared key
Keystream obtaining example
Property: The WEP checksum is a linear function of the message.
\[ c(x \oplus y) = c(x) \oplus c(y) \]

\[ A \rightarrow (B) : <v, C> \]
\[ C = RC(v, k) \oplus <M, c(M)> \]

\[ (A) \rightarrow B: <v, C'> \]
\[ C' = C \oplus <\Delta, c(\Delta)> \]
\[ = RC4(v, k) \oplus <M, c(M)> \oplus <\Delta, c(\Delta)> \]
\[ = RC4(v, k) \oplus <M', c(M')> \]
Property: The Wep checksum is an unkeyed function of the message

\[ P \oplus C = P \oplus (P \oplus \text{RC4}(v,k)) = \text{RC4}(v,k). \]

\[(A) \rightarrow B: <v, C'> \]
\[ C' = <M', c(M')> \oplus \text{RC4}(v,k). \]

It is possible to reuse old IV values without triggering any alarms at the receiver.
Access Point

Client

128 bit random challenge $r$ (plaintext)

$<v, C> = <v, RC4(v, k) \oplus <r, c(r)>>$

Access Point

Attacker

128 bit random challenge $r'$ (plaintext)

$<v, C'> = <v, RC4(v, k) \oplus <r', c(r')>>$
Message Decryption

- Idea: Trick the access point into decrypting ciphertext for us.

- IP redirection

- Reaction attack
  - It is useful only against TCP traffic
  - Take the advantage of TCP checksum
The TCP checksum (CRC32) on a plaintext $P$ is valid only when $P \equiv 0 \pmod{2^{16} - 1}$

We let $C' = C \oplus \Delta$, where $\Delta$ which bits to flip. Pick $i$ arbitrarily, set bit positions $i$ and $i+16$ to one, and others to zeros, regarding $\Delta$.

$P \oplus \Delta \equiv P \pmod{2^{16} - 1}$, only when $P_i \oplus P_{i+16} = 1$

We can use ACK packets to give us one bit of information on the plaintext.
Conclusion

- WEP is not secure
- The use of stream ciphers is dangerous
- The importance of keyed integrity check
- Shared-key mechanism is insecure
- Public review is also of great importance
Thanks!