Intercepting Mobile Communications: The Insecurity of 802.11

Nikita Borisov, Ian Goldberg, David Wagner
UC Berkeley
ACM SIGMOBILE 2001
Introduction

- 802.11 standard for wireless networks includes the Wired Equivalent Privacy (WEP) protocol to protect link layer communication from eavesdropping and other attacks
- WEP has serious security flaws
WEP

• Encrypting a frame:
  – Compute an integrity checksum on the message $M$
  – Concatenate $M$ and its checksum to get plaintext $P$
  – Encrypt plaintext using RC4
    • Choose initialization vector (IV) and key $K$
    • Generate keystream
    • XOR plaintext with keystream to get ciphertext
  – Transmit ciphertext and IV
WEP Goals

- Confidentiality
- Access Control
- Integrity
Breaking Confidentiality: Keystream Reuse

- WEP uses a stream cipher called RC4
- RC4 expands a secret key and a public initialization vector into a “keystream' of pseudorandom bits
- Encrypt plaintext by XORing it with the ciphertext
- Decrypt ciphertext by generating the keystream and XORing it with the ciphertext
Keystream Reuse

- Stream cipher pitfall: if two ciphertexts used the same IV and key, the two ciphertexts can be XORed together to generate the XOR of the plaintexts.
- If one plaintext is known, easy to get the others.
- Many other techniques to obtain or guess plaintexts.
- The more a keystream is reused the easier it is to guess plaintexts.
Finding Instances of Keystream Reuse

- Keystream reuse usually comes from reuse of the IV since shared keys are rarely changed.
- Improper IV management creates opportunity for attacks:
  - Ex: Poorly selected IV's
  - WEP standard size for IV field is 24 bits

  - Back of the envelope calculation: available space exhausted in half a day for AP sending 1500 byte packets with 5Mbps bandwidth.
Exploiting Keystream Reuse to Read Encrypted Traffic

- IV reuse discovered
- Next: obtain plaintext
- Methods:
  - Analyze traffic patterns and lengths
  - Send IP traffic to a mobile host from an Internet host under the attacker's control
  - Many others
Building Decryption Dictionaries

- IV reuse discovered, plaintext obtained
  - Keystream value can be discovered and used to decrypt any other message with the same IV
- Attacker can build a keystream table or decryption dictionary over time
Key Management

- 802.11 does not specify how to do key distribution
- Many installations use a single key for an entire network
  - Increases chances of IV collision
  - Difficult to replace compromised key
Breaking Integrity: Message Authentication

- WEP uses an integrity checksum (CRC-32) to ensure that packets are unchanged in transit
- Insufficient: messages can be:
  - 1. Modified
  - 2. Injected
  - 3. Spoofed
  - 4. Decrypted
Message Modification

• Checksumming distributes over the XOR operation
  – Can make modifications to ciphertext without disrupting the checksum in the WEP checksum
  – Attacker only needs to know original ciphertext and the desired plaintext difference
Message Injection

• Breaks goal of secure access control
• After obtaining full plaintext and ciphertext, the keystream can be calculated and used to create a new packet
• Although this means that the packet would use the same IV value as the old one (WEP standard specifies that each packet needs to have a different one) it is possible to reuse IV values without triggering alarms
  – How easy is this to do?
Authentication Spoofing

- WEP shared key authentication: access point sends a cleartext 128 byte random string (challenge)
- If the mobile station can respond with an encrypted challenge that the access point can decrypt it is allowed to associate with that access point
- Attacker can monitoring a legitimate authentication sequence and derive a keystream to use to respond to a new challenge
Message Decryption

• Trick the access point into decrypting ciphertext
• Two possible methods: IP redirection and reaction attacks
Message Decryption-IP Redirection

- Sniff encrypted packet off the air
- Change destination address of the packet (using message modification)
- Attacker reads the packet
- Ensure that checksum stays the same
  - Checksum is known—can change checksum to the correct value
  - Predict checksum
  - Compensate for change in destination field by change in another field
Message Decryption-Reaction Attacks

- Monitor reaction of recipient of TCP packet:
- Intercept a ciphertext C
- Invert some bits in C and adjust the checksum accordingly to get a new ciphertext with valid checksum
- Watch to see if recipient sends back TCP ACK to see if text passed checksum –can use this information to reveal plaintext
- Using recipient as an oracle to decrypt ciphertext
Countermeasures

- Put wireless network outside organization firewall
- Require that the same virtual private network be used to access internal network when connected over 802.11
- Improve key management: every host should have its own encryption key, change keys with high frequency
Conclusions

- WEP has major security flaws
- Need more precautions to provide security