IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability

By
Shivu Vibhuti
shivu.vibhuti@gmail.com
CS265 - Spring 2005

Advisor: Dr. Mark Stamp
stamp@cs.sjsu.edu
Agenda

- What is WEP?
- WEP Design objectives
- WEP Authentication
- WEP Encryption/Decryption
- WEP Vulnerability & attacks
- How to strengthen wireless security
- Q&A
What is WEP (Wired Equivalent Privacy)?

- Protection mechanism offered by the IEEE 802.11 standard
- Operates on the Media Access Control (MAC) layer
- Aim is to provide data privacy equivalent to the level of wired network
- WEP algorithm is used to protect wireless communication from eavesdropping
Design Objectives as per the IEEE 802.11 standard

- It is reasonably strong
- It is self-synchronizing
- It is efficient
- It may be exportable
- It is optional
WEP Design objectives

- It was not designed to be the ultimate "killer" security feature
- The intention was to make it hard to break-in
WEP Open Authentication

- Based on request and grant
- Essentially no authentication i.e. no client validation
WEP Shared Key Authentication

- Based on request, challenge, challenge-response, grant/deny
- Worse than open system authentication, exposes keystream
Shared Key Authentication Vulnerability

- Known keystream can be used to generate response
  - Response = (Challenge) XOR (known keystream for a particular IV)
Shared Key Authentication Vulnerability...

- Same shared key is used for both authentication and encryption
- Prone to man in the middle attack
WEP Encryption

- Based on symmetric shared key encryption, uses RC4 stream cipher
WEP Decryption

IV Ciphertext

Ciphertext

IV

Secret Key

Keystream

XOR

Plaintext CRC

Plaintext

CRC

CRC

Compare

Good Data

Bad Data
WEP Vulnerability

- IV mechanism has made the protocol vulnerable
- The IEEE 802.11 does not specify how to generate IV's
- Uses 40 or 104 bits key with 24 bits IV
- RC4 keystream repeats if IV's are repeated, major flaw in the WEP design/implementation
WEP Vulnerability

- Attacker can identify when IV collision occurs
- Attacker can pick two packets derived from the same key and obtain the unknown plaintext using $C_1 \text{ XOR } C_2 = P_1 \text{ XOR } P_2$
- Same IV can be used with every packet
- Cannot differentiate between forged packets and the original packets
WEP Vulnerability

- Difficult to keep secret, when the same key is shared among multiple users/devices
- Same key is used for a long time
- CRC checksum failed to protect data integrity
- Fluhrer, Mantin and Shamir discovered a flaw in the WEP key scheduling algorithm (IV weakness)
WEP attacks

- Known plaintext attack
- Reaction attack - Guess some of the bits in a message & determine the other bits
- Inductive attack - Trial and Error
WEP attacks

- Inductive attack – trial and error method
  - Obtain initial keystream K (length n)
  - Create ICMP ping or ARP request packet
  - Choose packet length to be “n+1”, attacker knows n bytes K, for n+1 th byte, try 256 different values
  - AP discards incorrect packet and responds to the correct packet, attacker now knows n+1 bytes of keystream
WEP cracking tools

- AirSnort
- WEPCrack
- Dweputils
Strengthening Wireless Security

- Choose bigger IV
- Use different mechanisms for the data integrity check
  For example: Hash functions
- keys can be assigned per user and configured to be changed based on time or packet limits
Strengthening Wireless Security

- Make wireless network invisible i.e. Dropping unencrypted packets/requests
- Use different authentication protocols e.g. EAP, LEAP, PEAP
- Use alternative protocols
  - IEEE 802.11i and TKIP, WPA, WPA in Pre-Shared Key (PSK) mode
Conclusion

- Don't just rely on WEP security, take additional measures at the higher layer
- WEP has many weaknesses due to the small IV space and poor selection of CRC32 for data integrity verification
- Another major issue with WEP is the key scheduling algorithm flaws discovered by Fluhrer, Mantin and Shamir
IEEE 802.11 WEP
(Wired Equivalent Privacy)
Concepts and Vulnerability

Q&A
Thank You!