Flaws in WEP (Wired Equivalency Privacy) and Proposed Enhancements

112003151 - Adwait Vipra

112003158 - Shyam Aradhye

112007014 - Ved Bilaskar

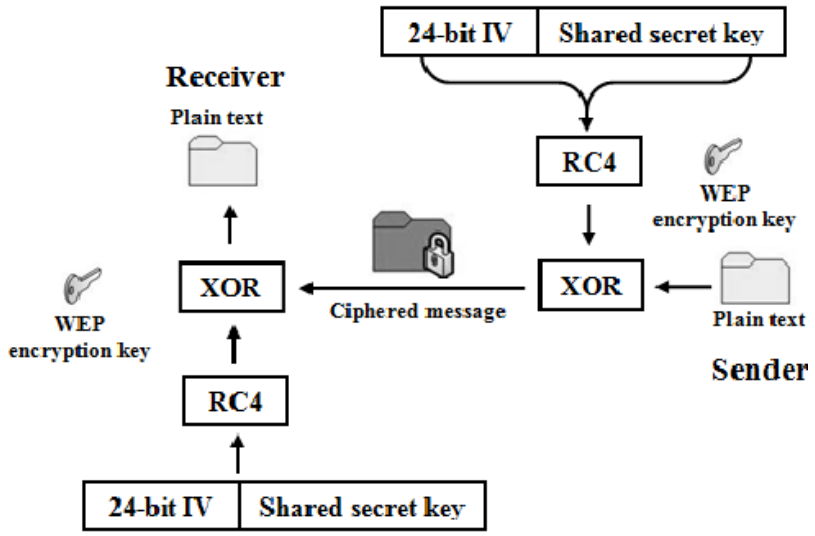
Abstract

Wireless Local Area Networks (WLANs) have become an integral part of modern connectivity, serving various environments such as colleges, cafes, offices, and more. Ensuring the privacy and security of data transmitted over WLANs is of paramount importance. However, WEP (Wired Equivalency Privacy), one of the earliest wireless security protocols, is known for its vulnerabilities. This paper aims to comprehensively analyze the flaws within WEP and propose enhancements to mitigate these vulnerabilities.

Introduction

Wireless Local Area Networks (WLANs) have proliferated across diverse settings due to their convenience and accessibility. In these environments, the protection of sensitive data is a critical concern. WEP was one of the pioneering security protocols designed to secure wireless communications and provide a level of security akin to that of wired networks. However, over time, several fundamental vulnerabilities have been exposed, rendering WEP ineffective for modern wireless networks. This paper undertakes a thorough examination of these vulnerabilities within WEP and presents a set of enhancements to bolster its security.

Working



- Key Setup:
  Shared Secret Key (K): The user or administrator provides a shared secret key, often referred to as the WEP key, which can be 40 or 104 bits in length.

- Generation of 24-bit IV:
  Initialization Vector (IV): A 24-bit random number that is generated for each packet. IVs are used to introduce randomness into the encryption process and prevent repetition.

- Key Expansion:
  RC4 Key Scheduling: The 24-bit IV is combined with the shared secret key (K) to create the RC4 encryption key.

  RC4_Key = IV || K (concatenation of IV and K)

- RC4 Encryption:
  RC4 Pseudo-Random Generation: RC4 is a stream cipher that generates a pseudo-random keystream based on the RC4_Key.

- XOR Operation:
  XOR with Plaintext: The plaintext (P) to be transmitted is XORed with the keystream generated by RC4.

  C = P XOR Keystream

  Where, C = Ciphertext , P = Plaintext

- Transmission:
  The resulting ciphertext (C) is sent over the wireless network along with the 24-bit IV.

- Receiver Side:
  At the receiver side, the 24-bit IV and the ciphertext (C) are received.

- Key Expansion (Receiver Side):
  The receiver knows the shared secret key (K) and uses the received IV to regenerate the RC4_Key.

  $$RC4\_Key = IV \,||\, K$$

- RC4 Decryption (Receiver Side):
  RC4 generates the same keystream on the receiver side using the regenerated RC4_Key.

- XOR Operation (Receiver Side):
  The receiver XORs the received ciphertext (C) with the regenerated keystream to recover the original plaintext (P).

  $$P = C \ XOR \ Keystream$$

  Where, C = Ciphertext , P = Plaintext

In summary, WEP encryption combines the 24-bit IV and the shared secret key (K) to create the RC4 encryption key. RC4 generates a keystream based on this key, which is XORed with the plaintext to produce ciphertext. At the receiver side, the same IV and shared secret key are used to regenerate the RC4 key and decrypt the ciphertext to recover the plaintext.

Flaws in WEP

WEP, initially designed to provide wireless networks with security comparable to that of wired networks, suffers from several significant vulnerabilities:

- Short IV Size and Reuse

One of WEP's primary vulnerabilities is its use of a short Initialization Vector (IV). The IV is only 24 bits long, which limits the number of unique IVs available. Consequently, IVs are reused within a relatively short timeframe, providing attackers with opportunities to exploit this weakness. By detecting IV collisions and leveraging them, attackers can deduce the keystream, a vital component of WEP's encryption.

- Weaknesses in RC4 Encryption

WEP relies on the RC4 stream cipher for encryption. While RC4 can be a robust encryption algorithm when implemented correctly, WEP's implementation introduces vulnerabilities. A critical issue is the use of weak keys. Frames encrypted with weak keys are substantially easier for attackers to decipher. Since WEP derives the first three bytes of the secret key from the IV, which is transmitted in plaintext, attackers can capture enough data to launch an attack within a relatively short timeframe, sometimes just a few hours.

- Lack of Frame Authentication

WEP lacks a mechanism to authenticate individual frames, rendering it vulnerable to frame spoofing and injection attacks. Attackers can introduce fraudulent frames into the network without detection, potentially compromising data integrity and overall network security.

- Vulnerability to Replay Attacks

WEP inadequately guards against replay attacks, wherein attackers intercept and retransmit previously captured network traffic. The absence of mechanisms to detect and prevent the replay of packets enables attackers to manipulate network communication.

- Limited Security of Data Integrity

WEP employs the Cyclic Redundancy Check (CRC) checksum for data integrity verification. While CRC can detect random errors in data transmission, it is ill-suited for safeguarding against intentional tampering by malicious actors. Attackers can modify ciphertext without affecting the CRC checksum, enabling them to inject forged or altered data packets into the network.

- IV Weaknesses

The IEEE 802.11 standard, encompassing WEP, lacks clear guidance on IV generation. This ambiguity leaves room for suboptimal IV generation practices, including the use of predictable IVs or commencing IVs from zero and incrementing them by one. Such weaknesses in IV management contribute significantly to WEP's susceptibility to attacks.

Methods to Improve WEP

To address the vulnerabilities inherent in WEP, several enhancement methods are proposed:

- Increase IV Size

One foundational enhancement is to increase the size of the Initialization Vector (IV). A larger IV space reduces the likelihood of IV collisions, making it more challenging for attackers to deduce the keystream. By extending the IV size beyond 24 bits, WEP can substantially improve its security.

- Hashed IV

Rather than transmitting the IV in plaintext, WEP can benefit from appending or prepending the hashed value of the IV to the ciphertext. This approach obscures the IV's value, making IV collisions less detectable by attackers.

- Stronger Data Integrity

WEP's reliance on CRC for data integrity can be replaced with more robust verification methods, such as cryptographic hash functions. These functions provide a higher level of assurance against tampering and data corruption.

- Dynamic Key Exchange

Enhancing security can be achieved by implementing dynamic key exchange mechanisms within WEP. Secure symmetric key distribution protocols can be employed to dynamically change shared keys, reducing the risks associated with prolonged use of a fixed key.

- Better Key Management

Effective key management practices can encourage regular key rotation. While manual administration of key changes may be challenging, automated systems can facilitate smoother transitions and reduce the likelihood of key compromise.

- Enhanced Authentication

Augmenting authentication mechanisms with robust protocols, such as the Extensible Authentication Protocol (EAP), can fortify WEP's security. EAP enhances protection against man-in-the-middle attacks during the authentication process.

These proposed enhancements aim to make WEP more resilient against known vulnerabilities and modern attack techniques. However, it is essential to recognize that while these improvements can bolster WEP's security, the protocol's fundamental design limitations may still render it less secure compared to more advanced alternatives such as WPA2 and WPA3.

Conclusion

In conclusion, the vulnerabilities within WEP have long been recognized, and this research paper has provided a comprehensive analysis of these flaws. Additionally, practical methods to enhance WEP's security have been proposed. While these improvements offer a step forward in securing WEP, it is important to acknowledge that the protocol is inherently limited. As such, modern security standards like WPA2 and WPA3 are recommended for robust wireless network protection.

Future Work

Future research endeavors should focus on the practical implementation and evaluation of the proposed enhancements to WEP. Real-world testing and deployment of these improvements will help determine their effectiveness in mitigating vulnerabilities. Additionally, exploring the adoption of more advanced wireless security standards, such as WPA3, should remain a key area of interest for enhancing network security further.

References:

- Jaspreet Kaur , “International Journal of Control Theory and Apllications” , ISSN : 0974-5572 , International Science Press
- Shivaputrappa Vibhuti , “IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability” , IEEE 802.11 San Jose State University, CA, USA