

WEP Flaws and Implementation Flaws of Authentication Protocols

By: Levi Portillo, Zhan Liu

Course: ELEN 689

Texas A&M University

April 6, 2006

Outline

- **Introduction**
- **WEP Overview**
- **WEP Implementation Problems**
- **WEP Vulnerabilities and Possible Attacks**
- **Solutions and Countermeasures**
- **Q&A's**

Introduction

- **IEEE 802.11 standard defines the Wired Equivalent Privacy (WEP) for encapsulation of 802.11 data frames.**
- **Main goal of WEP is to provide data privacy to the level of a wired network.**
- **WEP uses the RC4 algorithm for encryption purposes.**

WEP Overview

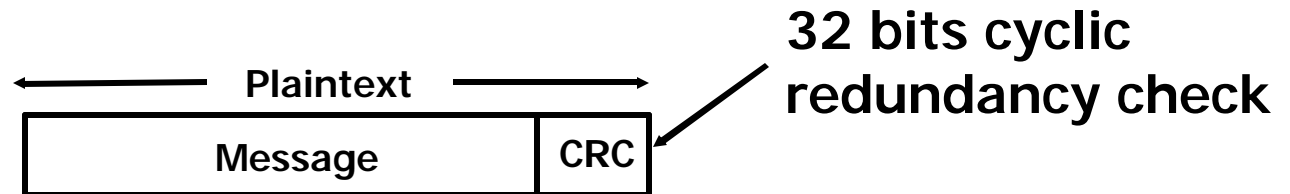
WEP relies on:

- **A key shared between all the communicating parties**
- **An encryption algorithm (RC4 – which also works as the decryption algorithm)**
- **A 24-bit initialization vector (IV)**
- **A CRC of the frame payload**

WEP Overview

How the encryption works:

- **Checksumming:** we compute an integrity checksum on the message. The checksum is then concatenated to the end of the plaintext message



WEP Overview

How the encryption works:

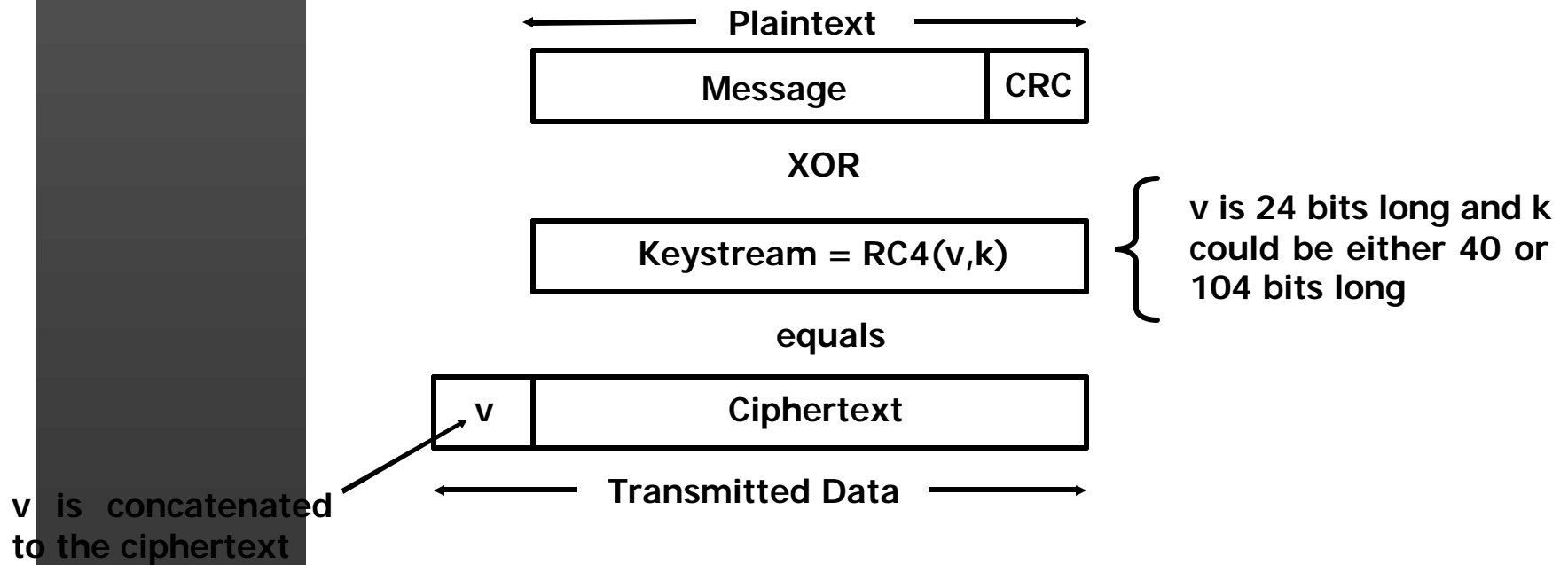
Encryption (RC4):

We encrypt the plaintext using RC4.

- An initialization vector (IV) v is chosen.
- RC4 generates a keystream (sequence of pseudorandom bytes) as a function of v and the key k .
- The keystream is XORed with the plaintext to generate the ciphertext

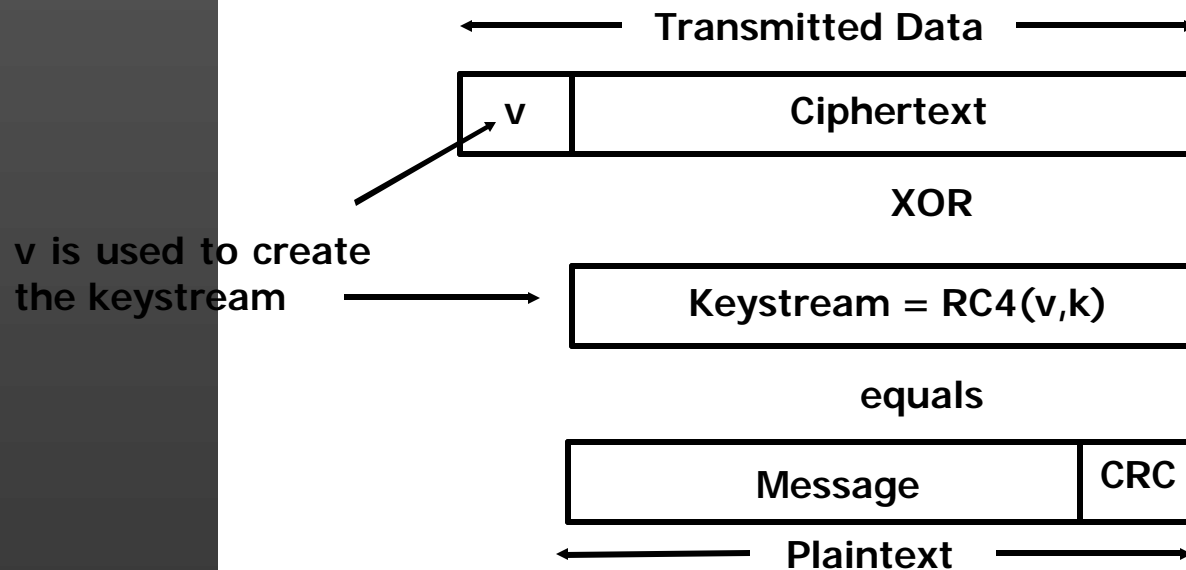
WEP Overview

How the encryption works:



WEP Overview

How the decryption works:



WEP Overview

Main Security Goals of WEP:

- **Confidentiality:** prevent eavesdropping so that the content of your traffic remains private
- **Access Control:** to discard all network packets that are not encrypted using WEP
- **Data Integrity:** prevent network traffic from being modified or corrupted. This is the main reason why the CRC has been included

WEP Overview

Major Attacks to WEP:

- **Passive attack: an attack in which an “unauthorized party gains access to the wireless network but does not modify its content or engage in communication with any node in the network”[1]. For example:**
 - 1. Eavesdropping**
 - 2. Traffic analysis by decrypting every packet that is sent over the wireless link**

This is commonly achieved using WLAN tools to recover encryption keys such as Aircrack-ng and a wireless NIC capable of working under RF monitor mode.

WEP Overview

Major Attacks to WEP:

- **Active attack: an attack in which an “unauthorized party makes modifications to a message, data stream or file”[1]. For example:**
 1. Masquerading
 2. Message modification
 3. Denial of service

This is the most dangerous kind of attack but not the most popular since they require more technical knowledge and there is greater risk of getting caught.

WEP Implementation Problems

Key Management:

- The 802.11 standard does not address the issue of key management (how keys are to be distributed)
- The standard relies on an external mechanism to populate a globally-shared array of 4 keys
- Usually, only one key is used for an entire network
- Since everybody is using the same key, once a key is compromised for one session, the same key can be used to decrypt any other session

WEP Implementation Problems

Key Management:

- It is also difficult (if not impossible) to replace a compromised key. To achieve this, every single user would have to reconfigure their wireless network driver
- Reusing a single key also increases chances of identifying a reused IV (v)
- Usually, only one key is used for a entire network
- What happens if someone who was using the key decides to share it with somebody else or has a laptop stolen?

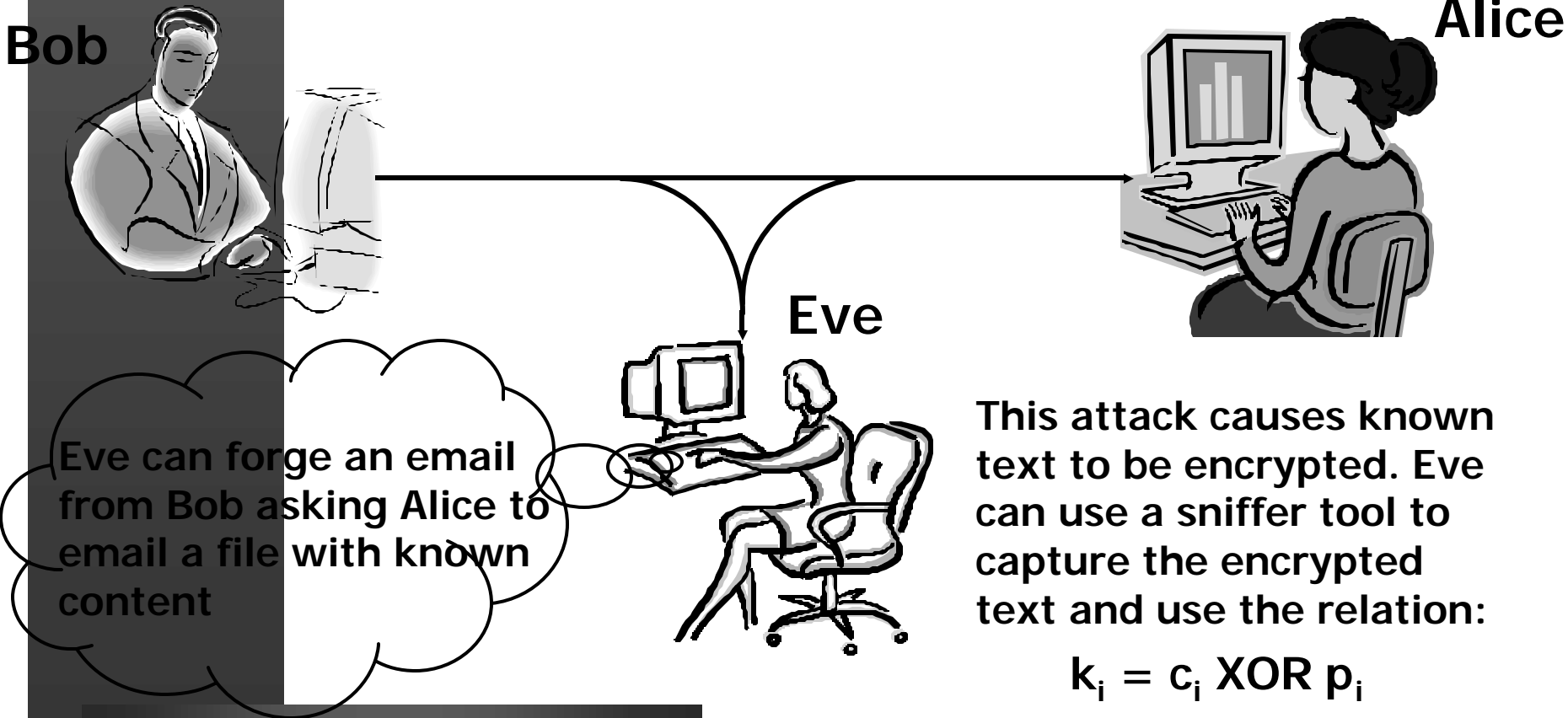
WEP Implementation Problems

Problems with using RC4 Cipher:

- The 802.11 protocol did not define how to implement IVs. The IV space takes 2^{24} possible values which means that the secret share key should be changed as soon as all possible IVs have been consumed. WEP defines no practical way to accomplish this
- WEP's initialization vector duplication: the combination of a shared secret key (k) and the repeated IV (v) results in a repeated keystream. Remember that IV is sent in clear text

WEP Vulnerabilities and Possible Attacks

A possible attack:



WEP Vulnerabilities and Possible Attacks

Illustration for keystream attack:

Plaintext ¹ : 11010011	Plaintext ² : 00101101
Keystream ³ : \oplus 10100110	Keystream ³ : \oplus 10100110
Ciphertext ¹ : 01110101	Ciphertext ² : 10001011

Ciphertext ¹ : 01110101	Plaintext ¹ : 11010011
Ciphertext ² : \oplus 10001011	Plaintext ² : \oplus 00101101
11111110	11111110

If both cipher texts are known and one plain text is known, the second plaintext can be derived

WEP Vulnerabilities and Possible Attacks

Other possible attacks:

- When two ciphertexts (generated using the same IV) are XORed one recovers the XOR of the two plaintexts. We could look for two English texts with the same XOR, or even better, for n ciphertexts with the same keystream (and for a large enough n) it is possible to use frequency analysis
- It is also possible to obtain candidates for the plaintext since many fields of IP traffic are predictable (e.g. well-defined and predictable structures in messages such as a login sequence)
- In conclusion, to exploit keystream reuse we need two conditions:
 1. Ciphertexts in which keystream has been reused
 2. Partial knowledge of some of the plaintext

WEP Vulnerabilities and Possible Attacks

Message Injection:

- WEP's checksum is an unkeyed function of the message. It can be computed by the attacker once he knows an entire plaintext corresponding to some transmitted frame
- XORing the plaintext P and the ciphertext C an attacker can obtain the keystream $RC4(v,k)$. He can then use the keystream and his own plaintext to forge a new ciphertext

WEP Vulnerabilities and Possible Attacks

Authentication used by WEP:

The access point will use the following mechanism before allowing a client to form an association:

- The client requests a shared-key authentication
- The access points sends a challenge (128-byte string) in cleartext.
- The client then responds with the same challenge encrypted using WEP
- Authentication is successful if the decryption of the response calculated at the access point matches the challenge

WEP Vulnerabilities and Possible Attacks

Authentication Spoofing:

- One of the main of flaws of the previously described authentication is that the challenge text is always 128 bytes.
- Let us remember that IVs can be repeated and reused.
- Then, by monitoring the negotiation process of a legitimate authentication sequence, an attacker could learn both the challenge sent by the AP and the encrypted version sent by the client
- The attacker can then derive the keystream and use it to create a proper response for a new challenge (using the message injection technique)
- No knowledge of the WEP key is needed for this kind of attack

WEP Vulnerabilities and Possible Attacks

Table-based attack:

- Since there are 2^{24} possible IVs, an attacker could build a decryption table (with a space requirement of about 24GB) like this:

IV_1	Cipherstream ₁ (K_1)
IV_2	Cipherstream ₂ (K_2)
.....
IV_x	Cipherstream _x (K_x)
.....
$IV_{2^{24}}$	Cipherstream _{2^{24}}} ($K_{2^{24}}$)

- Once this table is available and the attacker learns the plaintext for some packet, he can get the keystream and decrypt each subsequent ciphertext almost in real time.

WEP Vulnerabilities and Possible Attacks

Some Facts:

- **An Access Point sending 1500 byte packets at an average of 11Mbps will run out of the available IV space (224) in about 5 hours**
- **Some wireless network cards reset the IV to zero each time they are initialized, incrementing the IV by one for each packet transmitted.**
- **Programs such as Aircrack-ng and WEPCrack exploit some of WEP's weaknesses to crack WEP keys by analyzing from totally passive data captures.**

Solutions and Countermeasures

- **Increasing the IV size (to 48 bits for example) and using a 104 secret key would decrease the likelihood of key stream reuse significantly, making it harder for an attacker to solve for the key using clues**
- **Improving key management by allowing every host, if possible, to have its own encryption key, changing keys with high frequency.**
- **Making the secret k dynamic so that it is changed before an attacker has time to gather information to break the key**
- **Place the wireless network outside the organization firewall (considering the wireless network as much of a threat as any other internet host)**

Q&A's



References

- [1] Simcoe E., Goldberg H. and Ucal M. "An Examination of Security Algorithm Flaws in Wireless Networks".
- [2] Barken Lee. "How secure is your wireless network?", Prentice Hall PTR, 2004.
- [3] Borisov N., Goldberg I. and Wagner D. Intercepting Mobile Communications: The Insecurity of 802.11"
- [4] Giller R. and Bulliard A., "Security Protocols and Applications 2004: Wired Equivalent Privacy", Swiss Institute of Technology, Lausanne, Mar. 3, 2004
- [5] Boland H. and Mousavi H., "Security Issues of the IEEE 802.11B Wireless LAN", CCGEI 2004, Niagara Falls, May 2004
- [6] Walker J., "Unsafe at any key size; An analysis of the WEP encapsulation, Intel Corporation, Oct. 2000