Overview of 802.11 Security

Bingdong Li

Present for CPE 601

Sources: 1 Jesse Walker (Intel) & 2. WinLab
Agenda

- Introduction
- 802.11 Basic Security Mechanisms
- What’s Wrong?
- Major Risks
- Recommendations
- Improving in Progress
Introduction

• The nodes transmit over the air and hence anyone within the radio range can eavesdrop on the communication.

• Conventional security measures that apply to a wired network do not work in this case.

• The 802.11 security is notorious now,

Agenda

• Introduction

• 802.11 Basic Security Mechanisms

• What’s Wrong?

• Major Risks

• Recommendations

• Improving in Progress
802.11 Basic Security Mechanisms

• Service Set Identifier (SSID)
• MAC Address filtering
• A data encapsulation technique called Wired Equivalent Privacy (WEP)
• An authentication algorithm called Shared Key Authentication
Service Set Identifier (SSID)

• AP periodically broadcasts SSID in a beacon.
• Use of SSID – weak form of security as beacon management frames on 802.11 WLAN are always sent in the clear.
• A hacker can use analysis tools (eg. AirMagnet, Netstumbler, AiroPeek) to identify SSID.
• Some vendors use default SSIDs which are pretty well known (eg. CISCO uses tsunami)

2/9/2011

Sources: 1 Jesse Walker (Intel) & 2. WinLab
MAC Address Filtering

The system administrator can specify a list of MAC addresses that can communicate through an access point.

**Advantage:**
- Provides a little stronger security than SSID

**Disadvantages:**
- Increases Administrative overhead
- Reduces Scalability
- Determined hackers can still break it

Sources: 1. Jesse Walker (Intel) & 2. WinLab
WEP Overview

1. **Checksum**: For a message $M$, we calculate $c(M)$. The plaintext is $P = \{M, c(M)\}$

2. **Encryption**: The plaintext is encrypted using RC4. RC4 requires an initialization vector (IV) $v$, and the key $K$. Output is a stream of bits called the keystream. Encryption is XOR with $P$.

3. **Transmission**: The IV and the ciphertext $C$ are transmitted.

[Diagram of message, CRC, RC4($v,K$), and ciphertext with XOR symbol]
WEP Encapsulation Summary:

- Encryption Algorithm = RC4
- Per-packet encryption key = 24-bit IV concatenated to a pre-shared key
- WEP allows IV to be reused with any frame
- Data integrity provided by CRC-32 of the plaintext data (the “ICV”)
- Data and ICV are encrypted under the per-packet encryption key
WEP Authentication

802.11 Authentication Summary:

- Authentication key distributed out-of-band
- Access Point generates a “randomly generated” challenge
- Station encrypts challenge using pre-shared secret

Sources: 1 Jesse Walker (Intel) & 2. WinLab
Agenda

- Introduction
- 802.11 Basic Security Mechanisms
  - What’s Wrong?
- Major Risks
- Recommendations
- Improving in Progress
So What’s Wrong?

• Properties of Vernam Ciphers
• How to read WEP Encrypted Traffic
• How to authentication without the key
• Traffic modification
• Lessons
• Requirements for a networked data encapsulation scheme

2/9/2011

Sources: 1 Jesse Walker (Intel) & 2. WinLab
Properties of Vernam Ciphers (1)

The WEP encryption algorithm RC4 is a Vernam Cipher:

Encryption Key $K$ → Pseudo-random number generator

Random byte $b$ → Plaintext data byte $p$

$Ciphertext$ $data$ $byte$ $c$ $\oplus$ $Random$ $byte$ $b$

Decryption works the same way: $p = c \oplus b$
Properties of Vernam Ciphers (2)

- Vernam-style stream ciphers are susceptible to attacks when same IV and key are reused:
  \[ C_1 = P_1 \oplus RC4(v, K) \]
  \[ C_2 = P_2 \oplus RC4(v, K) \]
  \[ C_1 \oplus C_2 = P_1 \oplus RC4(v, K) \oplus P_2 \oplus RC4(v, K) \]
  \[ = P_1 \oplus P_2 \]

- Particularly weak to known plaintext attack: If \( P_1 \) is known, then \( P_2 \) is easy to find (as is \( RC4 \)).
  - This might occur when contextual information gives \( P_1 \) (e.g. application-level or network-level information reveals information)

- Even so, there are techniques to recover \( P_1 \) and \( P_2 \) when just \((P_1 \text{ XOR } P_2)\) is known (frequency analysis, crib dragging)
  - Example, look for two texts that XOR to same value
By the Birthday Paradox, probability $P_n$ two packets will share same IV after $n$ packets is $P_2 = 1/2^{24}$ after two frames and $P_n = P_{n-1} + (n-1)(1-P_{n-1})/2^{24}$ for $n > 2$.

- 50% chance of a collision exists already after only 4823 packets!!!
- Pattern recognition can disentangle the XOR’d recovered plaintext.
- Recovered ICV can tell you when you’ve disentangled plaintext correctly.
- After only a few hours of observation, you can recover all $2^{24}$ key streams.
How to Read WEP Encrypted Traffic (2)

• Ways to accelerate the process:
  – Send spam into the network: no pattern recognition required!
  – Get the victim to send e-mail to you
    • The AP creates the plaintext for you!
  – Decrypt packets from one Station to another via an Access Point
    • If you know the plaintext on one leg of the journey, you can recover the key stream immediately on the other
  – Etc., etc., etc.
How to Authenticate without the Key

With our background, an easy attack is obvious:

- Record one challenge/response with a sniffer
- Use the challenge to decrypt the response and recover the key stream
- Use the recovered key stream to encrypt any subsequent challenge

Sources: 1 Jesse Walker (Intel) & 2 WinLab
Vernam cipher thought experiment 2: how hard is it to change a genuine packet’s data, so ICV won’t detect the change?

Represent an n-bit plaintext as an n-th degree polynomial:

- \( p = p_nx^n + p_{n-1}x^{n-1} + \ldots + p_0x^0 \) \hspace{1cm} (each \( p_i = 0 \) or \( 1 \))

Then the plaintext with ICV can be represented as:

- \( px^{32} + ICV(p) = p_nx^{n+32} + p_{n-1}x^{n-31} + \ldots + p_0x^{32} + ICV(p) \)

If the n+32 bit RC4 key stream used to encrypt the body is represented by the n+32\(^{nd}\) degree polynomial \( b \), then the encrypted message body is

- \( px^{32} + ICV(p) + b \)
Traffic Modification (2)

But the ICV is linear, meaning for any polynomials $p$ and $q$

- $\text{IVC}(p+q) = \text{ICV}(p) + \text{ICV}(q)$

This means that if $q$ is an arbitrary $n$th degree polynomial, i.e., an arbitrary change in the underlying message data:

- $$(p+q)x^{32} + \text{ICV}(p+q) + b = px^{32} + qx^{32} + \text{ICV}(p) + \text{ICV}(q) + b$$
  $$= ((px^{32} + \text{ICV}(p)) + b) + (qx^{32} + \text{ICV}(q))$$

**Conclusion**: Anyone can alter an WEP encapsulated packet in arbitrary ways without detection (Spoofing and Injection).
Lessons

• Data encryption by itself offers no protection from attack
  – “It’s access control, stupid”
  – there is no meaningful privacy if the data authenticity problem is not solved

• It is profoundly easy to mis-use a cipher
  – “don’t try this at home”
  – Get any cryptographic scheme reviewed by professionals

Sources: 1 Jesse Walker (Intel) & 2. WinLab
Agenda

• Introduction
• 802.11 Basic Security Mechanisms
• What’s Wrong?
  • Major Risks
• Recommendations
• Improving in Progress
Major Risks

• Unauthorized Use of Service
• Insertion Attacks (Intrusions!)
• Interception and monitoring wireless traffic
• Misconfiguration
• Jamming
• Client to Client Attacks (Intrusions also!)

Sources: 1 Jesse Walker (Intel) & 2. WinLab
Agenda

• Introduction
• 802.11 Basic Security Mechanisms
• What’s Wrong?
• Major Risks
  • Recommendations
• Improving in Progress
Strengthen WLAN security

Recommendations

Wireless LAN related Configuration
- Enable WEP, use 128bit key*
- Using the encryption technologies
- Disable SSID Broadcasts
- Change default Access Point Name
- Choose complex admin password
- Apply Filtering
- Use MAC (hardware) address to restrict access
- The Use of 802.1x
- Enable firewall function

Sources: 1. Jesse Walker (Intel) & 2. WinLab
Agenda

• Introduction
• 802.11 Basic Security Mechanisms
• What’s Wrong?
• Major Risks
• Recommendations
  • Improving in Progress
Improving ...

- IEEE 802.11i: Enhanced security (2004) to enhance the MAC layer
- IEEE 802.11w: (or known as TGw) Protected Management Frames (2009) to protect management and broadcast frames.