

WEP (In)Security

Dominik Schürmann

English in Information and Communication Technology
Technische Universität Carolo-Wilhelmina zu Braunschweig

December 15, 2008



TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG

1 Overview

- Table of contents
- Introduction
- Facts
- Real world research

2 Technical background

- The WEP Protocol
- IV - Initialization Vector
- Basic flow

3 Breaking WEP

- History
- Weakness of WEP
- How To Crack
- Simplified process

4 Conclusion

- Conclusion
- Discussion

5 Resources

Introduction

WEP (Wired Equivalent Privacy)

- IEEE 802.11 wireless standard for data encryption and network authentication
- WEP got implemented into the IEEE 802.11 in the late 1990s
- only a few months later: the first research papers on WEP's poor implementation of the RC4 encryption keystream
- 2005: WEP protocol got officially declared "deprecated"

Introduction

WEP (Wired Equivalent Privacy)

- IEEE 802.11 wireless standard for data encryption and network authentication
- WEP got implemented into the IEEE 802.11 in the late 1990s
- only a few months later: the first research papers on WEP's poor implementation of the RC4 encryption keystream
- 2005: WEP protocol got officially declared "deprecated"

Introduction

WEP (Wired Equivalent Privacy)

- IEEE 802.11 wireless standard for data encryption and network authentication
- WEP got implemented into the IEEE 802.11 in the late 1990s
- **only a few months later: the first research papers on WEP's poor implementation of the RC4 encryption keystream**
- 2005: WEP protocol got officially declared "deprecated"

Introduction

WEP (Wired Equivalent Privacy)

- IEEE 802.11 wireless standard for data encryption and network authentication
- WEP got implemented into the IEEE 802.11 in the late 1990s
- only a few months later: the first research papers on WEP's poor implementation of the RC4 encryption keystream
- 2005: WEP protocol got officially declared "deprecated"

Facts

- With a basic knowledge of the Linux terminal and wireless networking anyone can gain unauthorized access
- Because WEP is depreciated and easy to crack one would assume the general population is not using it anymore
⇒ Sadly this is wrong

Facts

- With a basic knowledge of the Linux terminal and wireless networking anyone can gain unauthorized access
- Because WEP is depreciated and easy to crack one would assume the general population is not using it anymore
⇒ Sadly this is wrong

Facts

- With a basic knowledge of the Linux terminal and wireless networking anyone can gain unauthorized access
- Because WEP is depreciated and easy to crack one would assume the general population is not using it anymore
⇒ Sadly this is wrong

Real world research

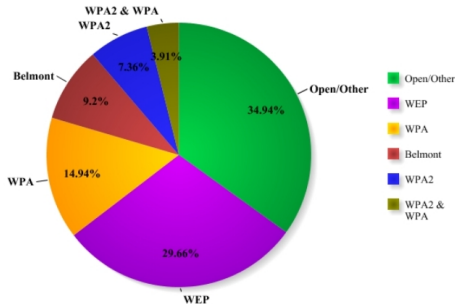


Figure: Pie Chart of Encryption Methods on Belmont's Campus

The WEP Protocol

- The protocol relies on a secret key, which is shared between the AP and all computers that want to access the WLAN
- Originally: 40-bit secret keys; Later: 104-bits
- Encryption based on RC4 algorithm
- Basically the RC4 algorithm creates a cipher-stream with a plaintext message to produce encrypted ciphertext

The WEP Protocol

- The protocol relies on a secret key, which is shared between the AP and all computers that want to access the WLAN
- Originally: 40-bit secret keys; Later: 104-bits
- Encryption based on RC4 algorithm
- Basically the RC4 algorithm creates a cipher-stream with a plaintext message to produce encrypted ciphertext

The WEP Protocol

- The protocol relies on a secret key, which is shared between the AP and all computers that want to access the WLAN
- Originally: 40-bit secret keys; Later: 104-bits
- Encryption based on RC4 algorithm
- Basically the RC4 algorithm creates a cipher-stream with a plaintext message to produce encrypted ciphertext

The WEP Protocol

- The protocol relies on a secret key, which is shared between the AP and all computers that want to access the WLAN
- Originally: 40-bit secret keys; Later: 104-bits
- Encryption based on RC4 algorithm
- Basically the RC4 algorithm creates a cipher-stream with a plaintext message to produce encrypted ciphertext

IV - Initialization Vector

- 40-bit key is known as 64-bit encryption and 104-bit key is known as 128-bit encryption
- Extra 24 bits: The Initialization Vector (IV)
- IV gets concatenated with the secret key to create the keystream
- Purpose of the IV: Avoid using the same keystream in two different ciphertexts

IV - Initialization Vector

- 40-bit key is known as 64-bit encryption and 104-bit key is known as 128-bit encryption
- Extra 24 bits: The Initialization Vector (IV)
- IV gets concatenated with the secret key to create the keystream
- Purpose of the IV: Avoid using the same keystream in two different ciphertexts

IV - Initialization Vector

- 40-bit key is known as 64-bit encryption and 104-bit key is known as 128-bit encryption
- Extra 24 bits: The Initialization Vector (IV)
- IV gets concatenated with the secret key to create the keystream
- Purpose of the IV: Avoid using the same keystream in two different ciphertexts

IV - Initialization Vector

- 40-bit key is known as 64-bit encryption and 104-bit key is known as 128-bit encryption
- Extra 24 bits: The Initialization Vector (IV)
- IV gets concatenated with the secret key to create the keystream
- Purpose of the IV: Avoid using the same keystream in two different ciphertexts

Basic flow

- 1 Every time the key is provided to the RC4 algorithm: a new IV is provided to augment this key and make it unique
- 2 Then the ciphertext is generated as a product of a unique keystream with the plaintext

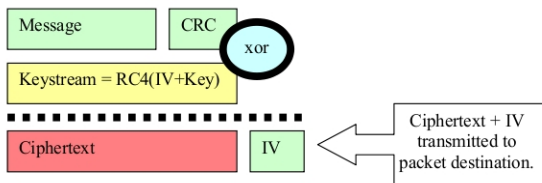


Figure: The basic flow of a encryption in WEP

Basic flow

- 1 Every time the key is provided to the RC4 algorithm: a new IV is provided to augment this key and make it unique
- 2 Then the ciphertext is generated as a product of a unique keystream with the plaintext

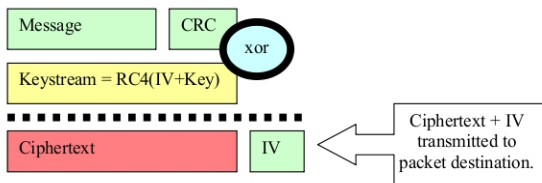


Figure: The basic flow of a encryption in WEP

Basic flow

- 1 Every time the key is provided to the RC4 algorithm: a new IV is provided to augment this key and make it unique
- 2 Then the ciphertext is generated as a product of a unique keystream with the plaintext

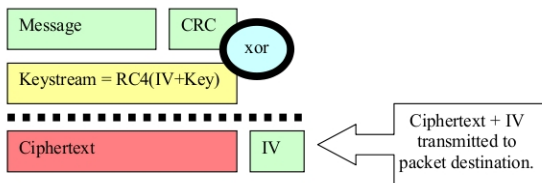


Figure: The basic flow of a encryption in WEP

History

- *2001:* Scott Fluhrer, Itsik Mantin and Adi Shamir released the foundational paper of WEP cracking
Secret key can be recovered from about 4,000,000 to 6,000,000 captured data packets
- *2004:* A hacker named KoReK improved the attack
The complexity of recovering a 104 bit secret key was reduced to 500,000 to 2,000,000 captured packets
- *2005:* Andreas Klein presented another analysis of the RC4 stream cipher
- *2007:* About 50% probability with 40,000 data packets
About 95% probability with 85,000 data packets

History

- *2001:* Scott Fluhrer, Itsik Mantin and Adi Shamir released the foundational paper of WEP cracking
Secret key can be recovered from about 4,000,000 to 6,000,000 captured data packets
- *2004:* A hacker named KoReK improved the attack
The complexity of recovering a 104 bit secret key was reduced to 500,000 to 2,000,000 captured packets
- *2005:* Andreas Klein presented another analysis of the RC4 stream cipher
- *2007:* About 50% probability with 40,000 data packets
About 95% probability with 85,000 data packets

History

- *2001*: Scott Fluhrer, Itsik Mantin and Adi Shamir released the foundational paper of WEP cracking
Secret key can be recovered from about 4,000,000 to 6,000,000 captured data packets
- *2004*: A hacker named KoReK improved the attack
The complexity of recovering a 104 bit secret key was reduced to 500,000 to 2,000,000 captured packets
- *2005*: Andreas Klein presented another analysis of the RC4 stream cipher
- *2007*: About 50% probability with 40,000 data packets
About 95% probability with 85,000 data packets

History

- *2001*: Scott Fluhrer, Itsik Mantin and Adi Shamir released the foundational paper of WEP cracking
Secret key can be recovered from about 4,000,000 to 6,000,000 captured data packets
- *2004*: A hacker named KoReK improved the attack
The complexity of recovering a 104 bit secret key was reduced to 500,000 to 2,000,000 captured packets
- *2005*: Andreas Klein presented another analysis of the RC4 stream cipher
- *2007*: About 50% probability with 40,000 data packets
About 95% probability with 85,000 data packets

Weakness of WEP

The problem with the IV

- **Problem No. 1:** 24-bits for unique IVs is not enough.
Possible IVs are recycled every few hours or less
- **Problem No. 2:** Many machines use a simple counter to generate IVs
- ⇒ With enough passive monitoring an attacker is able to collect packets with the same IV, leaving the WEP secret key vulnerable

Weakness of WEP

The problem with the IV

- **Problem No. 1:** 24-bits for unique IVs is not enough. Possible IVs are recycled every few hours or less
- **Problem No. 2:** Many machines use a simple counter to generate IVs
- ⇒ With enough passive monitoring an attacker is able to collect packets with the same IV, leaving the WEP secret key vulnerable

Weakness of WEP

The problem with the IV

- **Problem No. 1:** 24-bits for unique IVs is not enough. Possible IVs are recycled every few hours or less
- **Problem No. 2:** Many machines use a simple counter to generate IVs
- ⇒ With enough passive monitoring an attacker is able to collect packets with the same IV, leaving the WEP secret key vulnerable

How To Crack

Three simple steps to rule the WEP world

- 1 Generate large amounts of traffic in the target network with ARP
- 2 Collect the replies from the network
- 3 Run a statistical analysis crack on the collected packets to compute the secret WEP key

How To Crack

Three simple steps to rule the WEP world

- 1 Generate large amounts of traffic in the target network with ARP
- 2 Collect the replies from the network
- 3 Run a statistical analysis crack on the collected packets to compute the secret WEP key

How To Crack

Three simple steps to rule the WEP world

- 1 Generate large amounts of traffic in the target network with ARP
- 2 Collect the replies from the network
- 3 Run a statistical analysis crack on the collected packets to compute the secret WEP key

kismet (WLAN sniffer)

```

Network List (AutoFit)
-----
Name      T  M  Ch  Packts  Flags  IP Range  Info
-----
default   A  N  006   9  F      192.168.0.1  16
! iyonder.net  A  N  005  42  U4     10.254.178.254  Pkts/s
! iyonder.net  A  N  001  22  A3     10.254.178.0   228
! europot     A  N  001  19  U4     204.26.5.166   Cryptd
! NETGEAR     A  O  006   5      0.0.0.0        4
- europot     A  N  011  14      0.0.0.0        Weak
! beksin@dg   A  Y  011  17      0.0.0.0        0
! iyonder.net  A  N  011  16  A3     10.254.178.0   Noise
! tsunani     A  T  007  17      0.0.0.0        0
! -no ssid    A  O  003  11      0.0.0.0        Discrd
! Probe Networks  P  N  ---   3      0.0.0.0        0
! iyonder.net  A  N  008  35      0.0.0.0        Pkts/s
- -no ssid    A  T  011   5      0.0.0.0        8
NCID_NET     A  T  006   1      0.0.0.0
-no ssid     A  T  011   1      0.0.0.0
-----
Status
-----
Found new probed network "012:003:031:034:012:013:023:007:027:003:033:033:0
80:11:5D0:005:029:811:004:022:013:019:027:030:031:001:011:027:0C5:003:0
bssid:00:0A:8A:A2:C8:7F
Found IP 10.254.178.254 for iyonder.net.:00:50:8B:51:17:17 via UDP
Battery: AC 107%
    
```



airodump (collecting IVs)

```

CH 11 || Elapsed: 12 s || 00:00:00:00:00:00
-----
BSSID      PWR  RXP  Beacons  #Data, #S  CH  MB  ENC  CIPHER  AUTH  ESSID
-----
16:28:70:00:00:00  78  1  126      13  0  11  54  WEP  WEP      test_wep
-----
BSSID      STATION  PWR  Last  Packets  Probes
-----
16:28:70:00:00:00  00:CB:CA:00:00:00  63  0      19
    
```



aircrack (compute WEP key)

```

aircrack 2.0
-----
[00:00:02] Tested 2 keys (tot 207169 IVs)
-----
KB  depth  bits(vote)
-----
0  0/ 1  63( 61) A2( 12) 88( 12) 39( 8) FB( 5) 74( 5)
1  0/ 1  68( 95) E2( 15) 38( 13) 8A( 5) 44( 5) 8A( 5)
2  0/ 1  65( 43) F7( 8) 37( 8) 1D( 7) 6A( 5) 40( 3)
3  0/ 1  63( 98) 81( 15) 18( 12) 03( 5) BA( 5) 35( 5)
4  0/ 1  68( 58) 8C( 12) FE( 12) 4F( 9) 02( 8) 08( 2)
5  0/ 1  70( 76) F8( 12) DE( 8) 8B( 8) 17( 5) 58( 5)
6  0/ 1  61( 75) C3( 15) BE( 12) 9E( 10) 63( 10) 77( 8)
7  0/ 2  73( 34) 15( 26) 2D( 10) 72( 9) A7( 8) 9A( 6)
8  0/ 1  73( 87) E1( 15) B5( 12) B5( 10) DE( 10) ED( 10)
9  0/ 1  71( 89) 88( 12) 38( 13) 0A( 12) 52( 5) 11( FB( 10)
10 0/ 4  65( 22) 82( 13) F2( 13) 49( 13) DE( 10) 1A( 10)
11 0/ 1  72( 154) A9( 16) FB( 15) 73( 12) 5A( 11) C5( 10)
12 0/ 2  64( 30) BF( 25) DC( 10) 40( 10) 00( 10) 43( 10)
-----
KEY FOUND! [ 63:88:85:63:0B:70:61:73:73:77:6F:72:64 ] (checksum=0)
    
```

Conclusion

Results

- WEP doesn't meet the requirements of secure WLAN and is vulnerable to a number of exploits
- WEP is officially deprecated, so don't use it!
- Secure your wireless network with modern encryption algorithms like WPA or WPA2!

Conclusion

Results

- WEP doesn't meet the requirements of secure WLAN and is vulnerable to a number of exploits
- WEP is officially deprecated, so don't use it!
- Secure your wireless network with modern encryption algorithms like WPA or WPA2!

Conclusion

Results

- WEP doesn't meet the requirements of secure WLAN and is vulnerable to a number of exploits
- WEP is officially deprecated, so don't use it!
- Secure your wireless network with modern encryption algorithms like WPA or WPA2!

Discussion

Questions

Any Questions?

Resources



Ross Buffington and Will Proffitt; Faculty Advisor: Dr. William Hooper.
Wep (In)Security, 2008.
[Online; 8. Dezember 2008].