Clarkson
UNIVERSITY

Wireless Security

Course
Cryptography
Fall 2014

Virginia Weidhaas

Jihuang Hume

Alfredo Chapa

Supervisor:
Christino Tamon

December 11, 2014

Contents

1 Abstract

2 Introduction

3 WEP

3.1 How it works

3.2 Flaws

3.3 Attacks on WEP

3.3.1 FMS attack

FMS was released by Fluhrer, Mantin and Shamir in 2001 [1] and is a statistical attack on WEP. The assumption is, that the attacker knows the IV (three bytes of the per packet key) and it uses weaknesses in RC4. Therefore he can reconstruct the key from a number of unencrypted messages. The attack is used in tools such as AirSnort, webplab and aircrack with which it is possible to crack WEP networks.

3.4 ChopChop Attack

The ChopChop attack was created by the user KoreK (a user in the NetStumbler.org security forum). His attack is based on the FMS attack but lets the attacker find the key faster. In addition to that, he published another attack ”A-neg” allowing the attacker to reduce the keyspace, resulting in more speed, too.

The ChopChop attack addresses a design flaw in the WEP protocol itself, a weakness of CR32 checksum and the lack of protection of replay attacks. It is based on the check sum fact, that if one flips a bit in a given bitstring, it is possible with the checksum to detect which bit was flipped. The last byte of a packet is taken away and it is guessed which is the right value. This is possible by injecting the truncated packet back in the network-thus creating more traffic and creating more useful information. The packet will be invalid, since the Integrity Check Value (ICV) will be incorrect

3.4.1 Fragmentaion

3.4.2 plain text attack

RC4 is used to create a key stream that will be XORed with the plain text message to create the cipher text, such that cipher text = (plain text) XOR (key stream). If the attacker knows a plain text and the corresponding cipher text, he is able to reveal the key stream in the following way: Key stream = (cipher text) XOR (plain text) It is very easy to capture the cipher text by wireless sniffers like Wireshark, which are freely available. To get the plain text is more difficult, but it is still possible. For example, the attacker could trick someone to send a predictable message, e.g. a chat message or email. However, this is still difficult since packets contain not only the message, but different headers which obscure the original message. One could increase chances to obtain predictable data by sending an email with blank spaces or a long string of the same character, which is recognizable. Another way to obtain a plain text is to look for known communication headers (e.g., if hacker knows IP address of the AP or other information specified in the headers).

3.4.3 Attack provided by IV collisions

As described above, WEP uses initialization vectors(IV)to encrypt each packet with its own key. IVs have a long list of flaws. The IVs are too small and in clear text. It is only a 24 bit field which is sent in the cleartext field of a message, which is too small for cryptographic purposes. In addition to it, Ivs are static, if you reuse them it produces identical streams for the protection of data. However, because of the short length they will repeat after a while, in busy networks between 5 and 7 hours. The IV makes the key stream vulnerable, because it is not specified in 802.11 standard how IVs are changed or set. That means wireless adapters from the same vendors might generate the same IV sequence or even use a constant IV.

To decrypt a packet, the receiver must also know this IV to. Therefore the 3 byte IV is appended to the end of the encrypted packet A 24 bit IV allows only 224 (= 16.777.216) possible keys. Since the IV is a random number, it repeats after 5000 packets. That means if the attacker captures enough packets with IV, he can deduce the key streams. In practice, approximately 50k-100k packets are needed for 104bit WEP key and less than 50k packets are needed for 40bit WEP keys.

4 WPA

4.1 How it works

4.2 Flaws

4.3 Attacks on WEP

References

[1] Weaknesses in the Key Scheduling Algorithm of RC4.Shamir.

[2] Michael Zalewski. ”The Tangled Web: A Guide to Securing Modern Web Applications”, *No Starch Press*, 2011.

[3] http://eprint.iacr.org/2007/471.pdf