
# Wireless Security

**Course**
**Cryptography**
**Fall 2014**

Virginia Weidhaas

Jihuang Hume

Alfredo Chapa

Supervisor:
Christino Tamon

December 11, 2014

# Contents

**1 Abstract** **3**

**2 Common misbeliefs about Wifi-Security** **4**

**3 WEP** **6**
3.1 How it works . . . . . 6
3.2 Flaws . . . . . 6
3.3 Attacks on WEP . . . . . 6
3.3.1 FMS attack . . . . . 6
3.4 ChopChop Attack . . . . . 6
3.4.1 Fragmentaion . . . . . 6
3.4.2 plain text attack . . . . . 6
3.4.3 Attack provided by IV collisions . . . . . 7

**4 WPA** **8**
4.1 How it works . . . . . 8
4.2 Flaws . . . . . 8
4.3 Attacks on WEP . . . . . 8

**References** **9**

# 1 Abstract

This paper focuses on home WiFi security.

VW

# 2 Common misbeliefs about Wifi-Security

WiFis are common in nearly every household. They are very popular, it is very easy to connect all of your favourite devices at home, e.g. tablets, phones, computers and printers. With an increasing amount of attacks on Wifis, many users are concerned and want to take measurements to prevent intruding. However, most of these security measures are mostly meaningless and only decrease the comfort in your own home.

### Hiding your SSID

The idea behind this is, that a network which can't be seen can't be intruded. However, on some devices invisible networks can still be seen (even if there is no name visible yet).Usually, the Service Set Identifier (SSID) is broadcasted by the router in its beacon, so users can find and connect to the nework. The SSID was never meant to be hidden (specified in the protocol). The router still has to put that information in all of its data packets etc, even if it doesn't broadcast it in its beacons anymore. It is fairly easy with tools like Kismet to discover hidden WiFis, and besides, whenever a computer with a saved WiFi is turned on it is trying to find its hidden Wifi, revealing the information to everyone with a net work scanner nearby. Besides, having a hidden WiFi might even attract hackers because you might have sensitive data on it.

### Enabling MAC-filtering

A unique Media Access Control (MAC) identifies each device in a wireless network to send and receive packets. There is the possibility to add a white list of MAC Adresses to the router. Then every device has to be added to that list before it can access the network, even if it knows the key. However, it is very easy to scan the network traffic with a sniffer, determine a valid MAC address and simply spoof it. Having a MAC filter makes only using the network harder for legitimate users and doesn't provide much extra security, since a real hacker would use the tools anyway.

### Limit the router's IP address pool

Every decive in the network has a Internet Protocol (IP) address. The purpose to do this is to limit the range of available IPs which can be assignened and therefore the amount of devices which can join the network. However, as in the point mentioned before, with a network anaylzer (given the attacker is already in your network) you can analyze all the used IPs on a network, and assign one of them manually to his device. This security measure is meaningsless and makes it only harder for users which you actually want to have in your wifi, to connect to it.

### Disable your router's DHCP server

A router uses Dynamic Host Control Protocol (DHCP) to assign each device which joins the network dynamically an IP address. By disabling it, it should be reached that only

users who know the IP range and their address can join the network since each IP has to be assigned manually to the device (similiar to a table with MAC-addresses). However, like in the point above, a simple network scan (given the attacker is already in your network) will reveal the IP and the attacker can then just manually assign one of the used IPs to his devicer. Doing that, it makes it only harder to connect legitimate deviced to the network and does not increase security.

**Reducing your routers transmission power**
This has a very flawed logic, by reducing the transmission power it should be made harder to detect the network from outside of the home. However, if someone really wants to intrude he will use a special antenna which can detect even a bad signal, and in all other cases it will just be a struggle to work with your own wifi at home.

All in all, these ”protections” don't give any extra security, they make operating the WiFi only harder. But how can you protect your Wifi and make it really secure? The best way to do this is using a strong encryption, like WPA2 and a string password. However, many people still use WEP (although it was deprecated around 2003 as a security measure). In this paper, we will cover why still using WEP is a bad idea and which protocols are better for a safe WiFi.

# 3 WEP

## 3.1 How it works

## 3.2 Flaws

## 3.3 Attacks on WEP

VW

### 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.
*No Starch Press*, 2011.

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

[3] http://www.dummies.com/how-to/content/understanding-wep-weaknesses.html

[4] http://www.pcworld.com/article/2052158/5-wi-fi-security-myths-you-must-abandon-now.html