Wireless Security

Course
Cryptography
Fall 2014

Virginia Weidhaas

Jihuang Hume

Alfredo Chapa

Supervisor:
Christino Tamon

December 11, 2014

Contents

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 Security Attacks against wireless networks

The main difference between wired and wireless networks is the medium it transfers its data through. This difference made the burden of securing the network heavier. The broadcast nature of wireless networks makes it easy for everyone to attack the network if not secured, due to the absence of physical barriers, where the range of wireless transmission ranges from 300 ft. to half a mile

*Arbaugh*2003

.

Below is a list of the most common attack types known in both wired and wireless networks. Most of the security attacks and threats are listed under the following categories:

Traffic Analysis
In this type of attacks the attacker uses the statistics of network connectivity and activity to find information about the attacked network. Information includes: AP location, AP SSID and the type of protocol used by the analysis of size and types of packets

*Welch*2003

.

Passive Eavesdropping
Attackers in this type set themselves in sniffing mode, where they listen to all the network traffic hoping to extract information from it. This type of attack is only useful with unencrypted networks and stream cipher encrypted ones.

Active Eavesdropping
Similar to passive eavesdropping but the attacker tries to change the data on the packet, or to inject a complete packet in the stream of data.

Unauthorized Access
This type of attack is also known by many other names, such as war driving, war walking, and war flying

*Earle*2005

. This is the most common attack type where the attacker tries to get access to a network that she is not authorized to access. Mainly the reason behind such attacks is just to get Internet access for free

*Potter*2003

.

Man-in-the-middle Attacks
In this attack, the attacker gets the packets before the intended receiver does. This allows her to change the content of the message. One of the most known subset of this attack is called ARP (Address Resolution Protocol) attacks, where the attacker redirects network traffic to pass through her device

*Welch*2003

.

Session Hijacking
The attacker attacks the integrity of the session by trying to hijack an authorized session from an authorized user.

Replay Attacks
In this type of attack the attacker uses the information from previous authenticated sessions to gain access to the network.

Rouge AP
Some of the devices allow the user to declare itself as an AP. This will make people confused and sometimes they may connect to this false AP exposing their information to it. This can be solved by imposing mutual authentication between AP and network devices.

DoS Attacks
DoS (Denial of Service) attacks are the hardest type of attacks to overcome. Attackers use frequency devices to send continuous noise on a specific channel to ruin network connectivity. It is known in the wireless world as RF Jamming

*Welch*2003

.

There are many other threats that can be placed under one of the categories above. These different types of attacks make it harder for the standard regulators to find the best way to come up with the best solutions to the security hazards without sacrificing network usability or speed. In this section we discussed the common concepts in security, the wireless world and the common security attacks against networks in both wired and wireless networks. This section should have provided enough information to go through the following sections.

3.2 Wired Equivalent Privacy (WEP)

Wep is the original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks.

However, WEP has many well-known security flaws, is difficult to configure, and is easily broken.

WEP's Major Weakness

WEP's major weakness is its use of static encryption keys. When you set up a router with a WEP encryption key, that one key is used by every device on your network to encrypt every packet that's transmitted. But the fact that packets are encrypted doesn't prevent them from being intercepted, and due to some esoteric technical flaws it's entirely possible for an eavesdropper to intercept enough WEP-encrypted packets to eventually deduce what the key is. This problem used to be something you could mitigate by periodically changing the WEP key (which is why routers generally allow you to store up to four keys). But few bother to do this because changing WEP keys is inconvenient and time-consuming because it has to be done not just on the router, but on every device that connects to it. As a result, most people just set up a single key and then continue using it ad infinitum. Even worse, for those that do change the WEP key, new research and developments reinforce how even changing WEP keys frequently is no longer sufficient to protect a WLAN. The process of 'cracking' a WEP key used to require that a malicious hacker intercept millions of packets plus spend a fair amount of time and computing power. Researchers in the computer science department of a German university recently demonstrated the capability to compromise a WEP-protected network very quickly. After spending less than a minute intercepting data (fewer than 100,000 packets in all) they were able to compromise a WEP key in just three seconds.

The Widespread Use of WEP

Widespread use of WEP is almost understandable given that to the layperson, the similar abbreviations WEP and WPA don't convey any meaningful difference between the two security methods (and they may even imply equivalence) Plus, WEP is almost always presented first by the security interface of most broadband routers since WEP comes before WPA both historically and alphabetically).

Security Issues with WEP (Wired Equivalent Privacy) was proven to be full of flaws back in 2001. WEP protocol itself has some weaknesses that allows the attackers to crack them in no time. Probably, the biggest flaw in a WEP key is that it supports only 40bit encryption. This means that there are only 16million possibilities.

3.3 Attacks of WEP

Fluhrer, Mantin, and Shamir

2002

present several weaknesses in the key scheduling algorithm of RC4, and describe their cryptanalytic significance. They identify a large number of weak keys, in which knowledge of a small number of key bits suffices to determine many state and output bits

with non-negligible probability. They use these weak keys to construct new distinguishers for RC4, and to mount related key attacks with practical complexities. They show that RC4 is completely insecure in a common mode of operation which is used in the widely deployed Wired Equivalent Privacy protocol (WEP, which is part of the 802.11 standard), in which a fixed secret key is concatenated with known IV modifiers in order to encrypt different messages. Our new passive ciphertext-only attack on this mode can recover an arbitrarily long key in a negligible amount of time which grows only linearly with its size, both for 24 and 128 bit IV modifiers.

Adam Stubblefield et al. implemented Fluhrer, Mantin, and Shamir's attack

*FMS*2002

against WEP, the link-layer security protocol for 802.11 networks. They were able to recover the 128 bit secret key used with a passive attack. The WEP standard uses RC4 IVs improperly, and the attack exploits this design failure. They make some optimizations to make the attack more efficient, conclude that 802.11 WEP is totally insecure.

Itsik Mantin revisit a known but ignored weakness of the RC4 keystream generator, where secret state info leaks to the generated keystream, and show that this leakage, also known as Jenkins' correlation or the RC4 glimpse, can be used to attack RC4 in several modes. Their main result is a practical key recovery attack on RC4 when an IV modifier is concatenated to the beginning of a secret root key to generate a session key. As opposed to the WEP attack from

*FMS*2002

the new attack is applicable even in the case where the first 256 bytes of the keystream are thrown and its complexity grows only linearly with the length of the key. In an exemplifying parameter setting the attack recovers a 16-byte key in 248 steps using 217 short keystreams generated from different chosen IVs. A second attacked mode is when the IV succeeds the secret root key. They mount a key recovery attack that recovers the secret root key by analyzing a single word from 222 keystreams generated from different IVs, improving the attack from

*FMS*2002

on this mode. A third result is an attack on RC4 that is applicable when the attacker can inject faults to the execution of RC4. The attacker derives the internal state and the secret key by analyzing 214 faulted keystreams generated from this key.

Tews

2007

demonstrated an active attack on the WEP protocol that is able to recover a 104-bit WEP key using less than 40,000 frames with a success probability of 50%. In order to succeed in 95% of all cases, 85,000 packets are needed. The IV of these packets can be randomly chosen. This is an improvement in the number of required frames by more

than an order of magnitude over the best known key-recovery attacks for WEP. On an IEEE 802.11g network, the number of frames required can be obtained by re-injection in less than a minute. The required computational effort is approximately 220 RC4 key setups, which on current desktop and laptop CPUs is negligible.

3.4 How it works

3.5 Flaws

3.6 Attacks on WEP

3.6.1 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.

Due to weakness in the PRNG used to genereate the keystream, the attacker knowing the first byte of the keystream and the first m bytes of the key can derive (m+1) byte of key. That only works with certain IV. The reason is,the first byte of the plaintext comes from the WEP SNAP header, an attacker can assume he can derive the first byte of the keystream from B XOR 0xAA. From there, he only needs an IV in the form (a + 3, n - 1, x) for a key index a origin 0, element value space n (256 since 8 bits make a byte), and any X. To start, the attacker needs IVs of (3, 255, x). WEP uses 24-bit IVs, making each value one byte long.[5]

3.7 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.

3.7.1 Fragmentaion

3.7.2 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).

3.7.3 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 Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) is a security standard for Wi-Fi wireless connection. WPA is an improvement and a replacement of the original Wi-Fi security standard, Wired Equivalent Privacy or WEP.

WPA was developed when it became evident that WEP was not as secure as originally hoped. WPA provides more sophisticated data encryption than WEP and provides a user authentication (WEP's user authentication is considered insufficient).

WPA also addresses most of the known WEP vulnerabilities and is primarily intended for wireless infrastructure networks. This infrastructure includes stations, access points, and authentication servers (typically remote authentication dial-in user service servers, called RADIUS servers). The RADIUS server holds user credentials and authenticates wireless users before they gain access to the network.

WPA, like its predecessor WEP, has been shown via both proof-of-concept and applied public demonstrations to be vulnerable to intrusion. The process by which WPA is usually breached is not a direct attack on the WPA algorithm but by attacks on a supplementary system that was rolled out with WPA, Wi-Fi Protected Setup (WPS), designed to make it easy to link devices to modern access points.

4.0.4 Temporal Key Integrity Protocol

This security standard encryption method is the Temporal Key Integrity Protocol or TKIP. TKIP addresses the weaknesses of WEP by including a per-packet mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism. WPA provides "strong" user authentication based on 802.1X and the Extensible Authentication Protocol (EAP). WPA also depends on a central authentication server such as RADIUS to authenticate each user.

TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as a solution to replace WEP without requiring the replacement of legacy hardware. This was necessary because the breaking of WEP had left WiFi networks without viable link-layer security, and a solution was required for already deployed hardware. TKIP is not an encryption algorithm, but it's used to make sure that every data packet is sent with a unique encryption key.

TKIP implements a more sophisticated key mixing function for mixing a session key with an initialization vector for each packet. This prevents all currently known related key attacks because every byte of the per packet key depends on every byte of the session key and the initialization vector. Additionally, a 64 bit Message Integrity Check (MIC) named MICHAEL is included in every packet to prevent attacks on the weak CRC32 integrity protection mechanism known from WEP. To prevent simple replay attacks, a sequence counter (TSC) is used which allows packets only to arrive in order at the receiver.

There are two attacks known against TKIP: 1. Beck-Tews attack 2. Ohigashi-Morii attack (which is an improvement on the Beck-Tews attack)

Both of these attacks only could decrypt small portions of data, compromising confidentiality. What they can't give you is access to the network. To give you an idea of how much data can be recovered, a single ARP frame would take around 14-17 minutes to get the plain text. Getting useful information with this type of attack is very improbable but not impossible considering the rate of recovery.

The only attack known, besides flaws in firmware of some routers is brute forcing the WPA key. Generally the key is generated as follows:

Key = PBKDF2(HMAC-SHA1,passphrase, ssid, 4096, 256)

The algorithm takes the type of HMAC to be used, the passphrase, the ssid as salt, the amount of iterations the password will be hashed and the final length of the generated hash. Considering this algorithm is meant to prevent hashed passwords from being broken it can take a huge amount of time. The only reasonable attack would be to use a dictionary attack. Also you need to change your SSID to something random.

5 WPA2

Wi-Fi Protected Access 2, the follow on security method to WPA for wireless networks, provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks.

WPA2 is based on the IEEE 802.11i standard; it also provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1X based authentication.

One of the most significant changes between WPA and WPA2 was the mandatory use of AES (Advanced Encryption Standard) algorithms and the introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a replacement for TKIP (still preserved in WPA2 as a fallback system and for interoperability with WPA). This is the main reason why WPA2 is more secure than WPA.

CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES standard. This is used to replace TKIP for message confidentiality and fixes the security issues which were identified in WPA.

Both WPA and WPA2 let you choose your authentication modes and both let you choose between TKIP and AES encryption mode. A WPA compliant device however can implement AES optionally whereas WPA2 compliant devices must be capable of both though you're not required to use AES. The only other thing that WPA2 adds is pre-authentication and PMK (Pairwise Master Key) caching which improves seamless roaming of clients between access points but has nothing to do with security.

5.1 WPA and WPA2 Security Issues

In 2008 researchers succeeded in cracking WPA's TKIP key, but they haven't been able to actually decrypt the individual keys generated by the TKIP, which are used to encrypt the data packets sent between a computer and the router.

Later in 2009 they developed a way to break the WPA encryption system used in wireless routers in about one minute. The attack gives you a way to read encrypted traffic sent between computers and certain types of routers that use the WPA (Wi-Fi Protected Access) encryption system.

This attacks work only on WPA systems that use the Temporal Key Integrity Protocol (TKIP) algorithm. They do not work on newer WPA 2 devices or on WPA systems that use the stronger Advanced Encryption Standard (AES) algorithm. While TKIP & Michael significantly improve WEP security, design limitations result in cryptographic weaknesses.

In the other hand, the primary security vulnerability to the actual WPA2 system requires the attacker to already have access to the secured Wi-Fi network in order to gain access to certain keys and then perpetuate an attack against other devices on the network. As such, the security implications of the known WPA2 vulnerabilities are limited almost entirely to enterprise level networks and deserve little to no practical consideration in regard to home network security.

Unfortunately, the same vulnerability that is the biggest hole in the WPA armor, the attack vector through the Wi-Fi Protected Setup (WPS), remains in modern WPA2-capable access points. Although breaking into a WPA/WPA2 secured network using this vulnerability requires anywhere from 2-14 hours of sustained effort with a modern computer, it is still a legitimate security concern and WPS should be disabled and, if possible, the firmware of the access point should be flashed to a distribution that doesn't even support WPS so the attack vector is entirely removed.

*Arbaugh*2003

"Wireless security is different," Computer Volume 36, Issue 8, Aug. 2003 Page(s):99 - 101

*Welch*2003

"Wireless security threat taxonomy," Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society 18-20 June 2003 Page(s):76 - 83

*Earle*2005

"Wireless Security Handbook," Auerbach Publications 2005

*Potter*2003

"Wireless security's future," Security & Privacy Magazine, IEEE Volume 1, Issue 4, July-Aug. 2003 Page(s):68 – 72

*FMS*2002

Scott R. Fluhrer, Itsik Mantin and Adi Shamir: Weaknesses in the Key Scheduling Algorithm of RC4. Selected Areas in Cryptography 2001: 1-24

*Tews*2007

E Tews, RP Weinmann, A Pyshkin: Breaking 104 bit WEP in less than 60 seconds - Information Security Applications, 2007 - Springer

References

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

[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

[5] http://en.wikipedia.org/wiki/Fluhrer,_Mantin_and_Shamir_attack

[6] http://www.howtogeek.com/howto/28653/debunking-myths-is-hiding-your-wireless-ssid-really-more-secure/