International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Wi-Fi security using Elliptical Curve Cryptography

Karim Shahajhan Mulani[1], Nimbalkar Ravi Ramchandra[2]

[1, 2]Assistant Professor, Sahakar Maharshi Shankarrao Mohite Patil Institute of Technology and Research, Shankarnagar-Akluj, India

Abstract: ***The main purpose or aim of this topic is to help Wi-Fi network user to establish a secure network. For making your Wi-Fi network secure you have to take care of that network. In this paper I am analyzing some of the security issues as well as security techniques, for making a good secure Wi-Fi network. In this I am giving an overview of WEP, WPA, WPA2 and algorithms used for that security techniques. Also give the information about advantages and disadvantages of that technology and suggesting best one technology among those.***

Keywords: The key points of this topic are Wi-Fi network, information security & data encryption..

1. Introduction

Wi-Fi, which stands for Wireless Fidelity, is a radio technology that networks computers so they connect to each other and to the Internet without wires .Users can share documents and projects, as well as an Internet connection among various computer stations, and easily connect to a broadband Internet connection while traveling. By using a Wi-Fi network, individuals can network desktop computers, laptops and PDAs and share networked peripherals like servers and printers. A Wi-Fi network operates just like a wired network, without the restrictions imposed by wires. Not only does it enable users to move around be mobile at home and at work , it also provides easy connections to the Internet and business networks while traveling .The technologies used in this field are one of the best in the wireless space It is, therefore, important to provide appropriate security measures for wireless networks, which ensure the robustness of their operation even in case of malicious attacks. In this seminar, i focus on the security issues related to a particular wireless technology, namely Wi-Fi networks. We do not propose novel results here; our intention is rather to give a tutorial on existing solutions, and to summarize their strengths and weaknesses. In particular, we give an overview of WEP, WAP, and WAP2 & WPS.

2. Need of Wi-Fi Network Security

Wireless networking is inherently risky because you are transmitting information via radio waves. Data from your wireless network can be intercepted just like signals from your cellular or cordless phones. Whenever you use a wireless connection; you might want to ensure that your communications and files are private and protected.

In a home wireless network, you can use a variety of simple security procedures to protect your Wi-Fi connection. These include enabling Wi-Fi Protected Access, changing your password or network name (SSID) and closing your network. However, you can also employ additional, more sophisticated technologies and techniques to further secure your business network.

3. Security Issues of Wi-Fi Network

Here I am discussing some of the issues related with the Wi-Fi network information security.

3.1 Weakness of WEP Encryption Mechanism

Everyone who has ever site up wireless will know WEP. They will also likely know that WEP is a ‘bad thing’. Here we explain why WEP is now considered to be a very poor choice for wireless security and what was done to fix it. The original Wired Equivalent Privacy (WEP) algorithm was used to protect wireless communication from eavesdropping.

It uses predefined ‘WEP keys’ to encrypt the traffic using the RC4 encryption algorithm. It also ensures data integrity by using an "Integrity Check Value". This is 4 bytes and appended to the end of each packet. One of several security problems with WEP is that using a static, unchanging WEP key means that brute force efforts can be undertaken to ‘crack’ the key by capturing enough encrypted packets. WEP also uses an Initialization Vector (IV) which is used to ensure that text encrypted with the same encryption key translates to a different cipher text value. Unfortunately, IV is too small and is vulnerable to attacks that make the IV easy to determine. In addition, the size of the key – 40 bits – has been cited as a weakness of WEP. When the standard was written in 1997, 40-bit keys were considered reasonable for some applications. Since the goal was to protect against "casual eavesdropping" it seemed sufficient at the time. The U.S. did not tightly control exports of 40-bit encryption, and the IEEE wanted to ensure exportability of wireless devices. The WEP Integrity Check Value (a fancy name for a hash) is based on CRC-32, an algorithm for detecting noise and common errors in transmission. CRC-32 is an excellent checksum for detecting errors, but a poor choice for a cryptographic hash. Better-designed encryption systems use algorithms such as MD5 or SHA-1 for their Integrity Check Values. The CRC-32 Integrity Check Value has a weakness that allows an attacker to modify an encrypted message and easily fix the Integrity Check Value so the message appears authentic. So in relation to encryption and integrity, WEP fares rather badly. How does WEP fare in the areas of identification, authentication, authorization and accountability?

3.2 Searching For Wireless Signal

Search for wireless signal is also a method of attacking wireless networks; there are many identification and attack techniques and software for wireless networks. Nets tumbler software is software that is widely used to found a wireless network. Many wireless network is not using encryption, even if you use the encryption feature, if you did not turn off the AP broadcast message feature, AP Radio and still contains a lot of information can be used to infer the WEP key information in clear text, such as network name, SSID, and other conditions to hackers intrusions.

3.3 Wireless Network Eavesdrooping

This involves attack against the confidentiality of the data that is being transmitted across the network. By their nature, wireless LANs intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any wireless LAN installation. In the wireless network, eavesdropping by the third parties is the most significant threat because the attacker can intercept the transmission over the air from a distance, away from the premise of the company.

4. Wifi Network Information Security Technologies

For preventing your wireless network from unauthorized users and security threats we are employed some of the security techniques and that are discussed as follows.

4.1 Wireless Signal Spectrum Expansion Technology

Extended frequency technology is a technology used for secure transmission of data. Spread spectrum sent a very low power signal used in a very wide frequency range of launch, and narrow-band radio-on the contrary; it put all the energy into a single frequency. Some wireless LAN products in the ISM bands for transmit signals within the 2.4~2.483GHz, in the context of this can get 79 isolation of different channels; wireless signals are sent to a random sequence on each channel. Many of radio wave frequency transforms per second, in order to send the wireless signal on each channel, and stays fixed time on each channel, before converting to cover all channels. If you do not know the time spent on each channel and frequency hopping pattern site to receive and decode the data outside of the system is almost impossible. Using different frequency hopping pattern, dwell time and adjacent to the channel number can be no mutual interference between several wireless networks that do not intersect, so do not worry about data being intercepted by other users on the network.

4.2 WEP Data Encryption Technology

WEP is the most common security technology for IEEE 802.11 standards, that's main aim is to prevent the unauthorized users for gaining access to Wi-Fi network. Data encryption technology is the core with hardware or software, before the packet is sent encrypted, only the workstation has the correct key can decrypt and read the data. This technique is used when u use a small network or a home wireless network.

4.3 Network Resource Access Control Technology

For preventing the intruders from gaining access to network recourses one algorithm is used for that technique that is validation algorithm. In that algorithm the recourses or a wireless adaptor prove that the he knows the secret key. After proving that he knows key then and only then he gain the access of wireless network. in wireless network the port access technologies are used for increasing the network security. Every radio station gives an logical port for an AP, whenever AP opens that logical port then only users get the access of that network, otherwise users are not allowed to get access of wireless network. These techniques are ideal for smaller companies.

4.4 Enable WEP Encryption

In order to protect your data from snooping or prying eyes, you should encrypt, or scramble, it so that nobody else can read it. Most recent wireless equipment comes with WEP (wired equivalent privacy) encryption schemes that you can enable. So your wireless network is protected from unauthorized users. only the proper security key holders can access your wireless network.

4.5 Wireless Network Access Point's MAC Addresses Filtering

Most Wi-Fi access points and routers ship with a feature called hardware or MAC address filtering. This feature is normally turned "off" by the manufacturer, because it requires a bit of effort to set up properly. However, to improve the security of your Wi-Fi LAN (WLAN), strongly consider enabling and using MAC address filtering. Without MAC address filtering, any wireless client can join (authenticate with) a Wi-Fi network if they know the network name (also called the SSID) and perhaps a few other security parameters like encryption keys. When MAC address filtering is enabled, however, the access point or router performs an additional check on a different parameter. Obviously the more checks that are made, the greater the likelihood of preventing network break-ins. To set up MAC address filtering, you as a WLAN administrator must configure a list of clients that will be allowed to join the network. First, obtain the MAC addresses of each client from its operating system or configuration utility. Then, they enter those addresses into a configuration screen of the wireless access point or router. Finally, switch on the filtering option. Once enabled, whenever the wireless access point or router receives a request to join with the WLAN, it compares the MAC address of that client against the administrator's list. Clients on the list authenticate as normal; clients not on the list are denied any access to the WLAN.

4.6 Shield SSID Broadcast Information

One way to protect your network from unauthorized access is to hide the fact that you have a wireless network at all. By default, wireless network equipment typically broadcasts a beacon signal, announcing its presence to the world and providing key information necessary for devices to connect

to it, including the SSID. The SSID (service set identifier), or network name, of your wireless network is required for devices to connect to it. If you don't want random wireless devices to connect to your network, then you certainly don't want to announce your presence and include one of the key pieces of information they need to do so. By disabling the broadcasting of the SSID, or even the beacon signal itself, you can hide the presence of your wireless network or at least obscure the SSID itself which is critical for a device to connect to your network.

5. WEP (Wired Equivalent Privacy)

Security has been considered an important issue in Wi-Fi networks from the beginning. Consequently, early versions of the IEEE 802.11 wireless LAN standard [802.11] have already featured a security architecture, which is called WEP (Wired Equivalent Privacy).As its name indicates, the objective of WEP is to render wireless LANs at least as secures wired LANs (without particular security extensions). For instance, if an attacker wants to connect to a wired Ethernet network, (s)he needs physical access to the Ethernet hub. However, this is usually made difficult by placing the hub in a locked room. In case of an unprotected wireless LAN, the attacker has an easier job, because (s) he does not need to have physical access to any equipment in order to connect to the network. WEP is intended to transform this easy job into a difficult one. More precisely, WEP is intended to increase the level of difficulty of attacking wireless LANs such that it becomes comparable to the difficulty of attacking wired LANs (e.g., breaking into locked rooms). Unfortunately, WEP does not make attacks as difficult as its designers hoped. This would not have been a problem if the weaknesses had been discovered in due time. But things happened differently: WEP has already been deployed when cryptographers and IT security experts discovered its flaws [Walker00, Borisov+01, Arbaugh+02]. It became evident that WEP did not provide adequate protection, and following this discovery, tools that automate the cracking of WEP keys have soon appeared on the Web. In response to these developments, the IEEE came up with a new security architecture for Wi-Fi networks, which is described in an extension to the 802.11 standard. This extension is called 802.11i. We will discuss 802.11i in the next section, while in this section, we are concerned with WEP. The motivation of discussing WEP is that, despite its known weaknesses, many systems still support it (for backward compatibility), and thus, probably many people and organizations still use it. Those people and organizations should be aware of the limitations of WEP, and consider switching to WPA or RSN (WPA2).

5.1.1 WEP Encryption

WEP's encryption algorithm makes use of the RC4 pseudorandom number generation algorithm that was developed in 1987 and is licensed by RSA Data Security, Inc. The algorithm is classified as symmetric because the encryption and the decryption processes use the same key.

First, both the client devices and the AP must share a secret key, which is 40 bits in the original standard but extensions to the standard have provided support for 104-bit keys, which should, in theory, greatly increase the security of the encryption. The shared key is concatenated with the initialization vector (IV), which in 802.11b, is specified to be 24 bits. The resulting 64-bit string is then used to seed the pseudo-random number generator to produce a key sequence with a length equal to the number of data octets to be transmitted, along with four octets in order to transmit the integrity check value (ICV). The integrity check value, a measure meant to preserve the integrity of the transmitted data, is produced by performing the Cyclic Redundancy Check (CRC) algorithm on the plaintext block, resulting in a 32-bit ICV. The generated key sequence is XORed with the plaintext message and then concatenated with the ICV to produce the cipher text that will be transmitted. The IV used is concatenated to the beginning of this cipher text as clear text.

Once the entire packet reaches the receiver, the decryption is performed in a very similar manner. The clear text IV is concatenated with the shared secret key and used to generate the key sequence used to encrypt the data. XORing the cipher text and this key sequence yield the original plaintext and the ICV. The CRC-32 algorithm is executed again to recompute the ICV value. If the two ICVs do not match, then the packet is discarded, because an integrity violation has occurred and the data has been altered en route. The simple CRC is not as cryptographically secure as a hash or message authentication code.

5.1.2 Problems with WEP

24-bit IVs are too short, and this puts confidentiality at risk. The CRC checksum, called the Integrity Check Value (ICV), used by WEP for integrity protection is insecure, and does not prevent adversarial modification of intercepted packets.

WEP combines the IV with the key in a way that enables cryptanalytic attacks. As a result, passive eavesdroppers can learn the key after observing a few million encrypted packets.

6. WPA (Wi-Fi Protected Access)

Over the past year, the Wi-Fi Alliance has spearheaded an effort to bring to market a standards-based interoperable security specification that would greatly increase the level of data protection and access control for Wi-Fi wireless local area networks. That specification is Wi-Fi Protected Access (WPA). WPA addresses the flaws in Wired Equivalent Privacy (WEP), the original native security mechanism for WLANs that has been in place since the adoption of the Institute of Electrical and Electronics Engineers (IEEE)

802.11 standard in 1997. By 2001, WEP's cryptographic weaknesses had become well-known. A series of independent studies from various academic and commercial institutions had shown that an intruder equipped with the proper tools and a moderate amount of technical knowledge could gain unauthorized access to a WLAN even with WEP enabled. In spite of its flaws, WEP did provide a margin of security compared to no security at all. It remained useful for deflecting eavesdroppers in home and small office/home office (SOHO) environments where network traffic is light. However, it was not sufficient for enterprise use. Many large companies strengthened WEP by deploying it with other

third-party security solutions, including virtual private networks (VPNs), 802.1X authentication servers, and other proprietary technologies. WPA addresses Wi-Fi security with

a strong new encryption algorithm as well as user authentication, a feature that was largely missing in WEP. When properly installed, it provides a high level of assurance that user data will remain protected and that only authorized users may access the network. With WPA enabled, enterprises can offer employees the ease and flexibility of working wirelessly and securely without deploying add-on security solutions, such as VPNs.

7. WPA2 (Wi-Fi Protected Access2)

In April 2003, the Wi-Fi Alliance introduced an interoperable security protocol known as Wi-Fi Protected Access (WPA), based on draft 3 of the IEEE 802.11i amendment. WPA was designed to be a replacement for WEP networks without requiring hardware replacements, using a subset IEEE 802.11i amendment. Organizations who adopt WPA can take advantage of the following features:

(i) Strong cryptography support from the Temporal Key Integrity Protocol (TKIP), based on the RC4 cipher;
(ii) WPA-Enterprise, a mechanism for network authentication using IEEE 802.1x and a supported EAP type, one of EAP/TLS, TTLS or PEAP;
(iii) WPA-Personal, a mechanism for using TKIP without IEEE 802.1x authentication by using a shared passphrase, intended for consumer networks.

In July 2004, the IEEE approved the full IEEE 802.11i specification, which was quickly followed by a new interoperability testing certification from the Wi-Fi Alliance known as WPA2. WPA2 is based on the Robust Security Network (RSN) mechanism, which provided support for all of the mechanisms available in WPA, as well as:

a) Strong encryption and authentication support for infrastructure and ad-hoc networks (WPA is limited to infrastructure networks);
b) Reduced overhead in key derivation during the wireless LAN authentication exchange;
c) Support for opportunistic key caching to reduce the overhead in roaming between access points;
d) Support for pre-authentication, where a station completes the IEEE 802.1X authentication exchange before roaming;
e) Support for the CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) encryption mechanism based on the Advanced Encryption Standard (AES) cipher as an alternative to the TKIP protocol.

As of March 2006, the WPA2 certification became mandatory for all new equipment certified by the Wi-Fi Alliance, ensuring that any reasonably modern hardware will support both WPA and WPA2.

The WPA2 standard has two components, encryption and authentication which are crucial to a secure wireless LAN. The encryption piece of WPA2 mandates the use of AES (Advanced Encryption Standard) but TKIP (Temporal Key Integrity Protocol) is available for backward compatibility with existing WAP hardware. The authentication piece of WPA2 has two modes: Personal and Enterprise. The Personal mode requires the use of a PSK (Pre-Shared Key) and does not require users to be separately authenticated. The Enterprise mode, which requires the users to be separately authenticated based on the IEEE 802.1X authentication standard, uses the Extended EAP (Extensible Authentication Protocol) which offers five EAP standards to choose from:

EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), Protected EAP vo/EAPMicrosoft's Challenge Handshake Authentication Protocol

8. Proposed Algorithm For Encryption.

The above encryption algorithms such as RC4,TKIP,AES having some of the problems, due to that I am suggesting a new encryption algorithm which is used to minimize some of the pitfalls in current wireless security technologies.

Here I am presenting new encryption algorithm called Elliptical curve cryptography.

8.1 What Is ECC And Why Do We Need It?

RSA has been around for a long time and is well understood. Unfortunately, hackers (those nefarious rapscallions who wish to break the code and access the data) now have access to phenomenally powerful computers that can crack the smaller keys. Originally, 512-bit RSA keys were considered to be sufficient. Over time this was increased to 768 bits, then 1,024 bits, and then 2,048 bits. More recently, NIST recommended the combination of 128 bit AES keys with 3,072-bit RSA keys. Meanwhile, the Europeans are even more pessimistic, because they are recommending 128 bit AES keys with 6,000-bit RSA keys. The problem is the expensive computational requirements associated with using these large keys; moving from a 1,024-bit RSA key to a 2,048-bit key, for example, requires 8x the computations/processing. In the case of the hand-held product arena, personal digital assistant (PDA) and communication devices simply don't have the processing capability to use RSA keys of 3,072 bits and higher. The solution is to use ECC, which requires much less processing while – at the same time – being much harder to crack. For example, a 256-bit ECC key is as secure as a 3,072-bit RSA key. Similarly, the 521-bit ECC keys used in BlackBerry wireless handheld devices are equivalent to RSA keys with 15,000+ bits! As it happens, ECC was first introduced in 1985 by Neal Koblitz from the University of Washington and Victor Miller from IBM. So why has it taken so long to catch on? Well, when ECC was first presented it was not well-understood; also, RSA was (a) entrenched and (b) deemed to provide sufficient security to satisfy everyone's requirements at that time. Also, there is "inertia" to this sort of thing. Until recently, for example, you couldn't find support for ECC in operating systems. But now we're at a "tipping point" at which industry best practices are in the process of being re-defined.

8.2 Advantages of ECC

ECC is a public key cryptographic technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. The ECC can yield a level of security with a 164 –bit key that other systems require a 1024-bit hey to achieve, due to that ECC helps to establish equivalent security with lower computing power and battery resources.

Also ECC minimizes the CPU overhead and don't required to upgrade the hardware. ECC work on newer as well as older firmware.

9. Conclusion

After analysis of all wireless network information security issues, technologies and algorithms used I conclude that for securing a wireless network we need to establish a proper security technology and a better management of that .from this topic I found that the ECC algorithm is good for providing the better security with less resources and smaller computing time and also decrease the CPU overhead. That algorithm is better for his small key size and providing security equivalent to much larger key.ECC provide better efficiency and great security for Wi-Fi network by applying the much more higher key size.so much more work is needed to develop the security by using Elliptical curve cryptography.

References

[1] Review of wi-fi security techniques by promilla and Dr.R.S.Chhillar
[2] wi-fi security –WEP and 802.11i by lenvente buttyan and Leazlo Dora.
[3] wi-fi protected access –pre-shared key hybrid algorithm by Maricel O. Balitanas.
[4] An overview of technical aspects of wifi network technology by shailendra kaushik.
[5] Wireless security's future by Nancy R Mead.
[6] IEEE 802.11/Wi-Fi security ,Report om the final nail in WEP's Coffin by hyung-loon kim.
[7] Wi-Fi technology and development by Yang Haoyu.
[8] Wi-Fi technology research and application by chen wanghzhou.