RESEARCH ARTICLE OPEN ACCESS

Secure Level Transmission in Wi-Fi Using Cryptography

K. Prasuna[1], M. Padmaja[2]
[1]Asst.Professor, Vijaya Institute of Technology for Women, Enikepadu, INDIA.
[2]Associate Professor,VR Siddhartha College of Engineering, INDIA

Abstract
Wi-Fi, is a mechanism that allows electronic devices to exchange data wirelessly over a computer network Wi-Fi suggests Wireless Fidelity, resembling the long-established audio-equipment classification term Hi-Fi or High Fidelity.This paper first gives some background information about WiFi system and security issues in ad hoc networks, then it concentrates on the specific security measures like hybrid encryption techniques using both AES and RSA algorithms and also the different standards. To provide the security for the data transmitted through WiFi ,it uses WEP algorithm,WEP64 and WEP128 and then it moves to WPA (Wi-Fi Protected Access) as the key is short in WEP.WPA use the TKIP and depends on RC4,which consist of 128 bit and 48 bit. The security comparisons show that WPA and TPIK is more advantageous than WEP and hence it is more preferable.

Keywords-Wi-Fi, WEP, WPA, TPIK

I. INTRODUCTION

Wi-Fi is a wireless technology that uses radio frequency to transmit data through the air. In Short called wireless fidelity and is meant to be used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, 802.11g, dual-band, etc.The 802.11 standard reserves the low levels of the OSI model for a wireless connection that uses electromagnetic waves.The physical layer , which offers three types of information encoding. The data link layer, comprised of two sub-layers:

Logical Link Control (or LLC) and Media Access Control (or MAC). The physical layer defines the radio wave modulation and signaling characteristics for data transmission, while the data link layer defines the interface between the machine's bus and the physical layer, in particular an access method close to the one used in the Ethernet standard and rules for communication between the stations of the network. The 802.11 standard actually has three physical layers, which define alternative modes of transmission:

Data Link Layer	Physical Layer
802.2	DSSS
802.11	FHSS,Infrared

II. THE VARIOUS WI-FI STANDARDS

The IEEE 802.11 standard is actually only the earliest standard, allowing 1-2 Mbps of bandwidth. Amendments have be made to the original standard in order to optimise bandwidth (these include the 802.11a, 802.11b and 802.11g standards, which are called 802.11 physical standards) or to better specify components in order to ensure improved security or compatibility. the various amendments to the 802.11 standard and their significance are given as

802.11a-Wifi5 : The 802.11a standard (called WiFi 5) allows higher bandwidth (54 Mbps maximum throughput, 30 Mbps in practice). The 802.11a standard provides 8 radio channels in the 5 GHz frequency band.

802.11b-WiFi: The 802.11b standard is currently the most widely used one. It offers a maximum thoroughput of 11 Mbps (6 Mbps in practice) and a reach of up to 300 metres in an open environment. It uses the 2.4 GHz frequency range, with 3 radio channels available.

802.11c-Bridging 802.11 and 802.1d: The 802.11c bridging standard is of no interest to the general public. It is only an amended version of the 802.1d standard that lets 802.1d bridge with 802.11-compatible devices (on the data link level).

802.11d-Internationalisation: The 802.11d standard is a supplement to the 802.11 standard which is meant to allow international use of local 802.11 networks. It lets different devices trade information on frequency ranges depending on what is permitted in the country where the device is from.

802.11e-Improving service quality: The 802.11e standard is meant to improve the quality of service at the level of the data link layer. The standard's goal is to define the requirements of different packets in terms of bandwidth and transmission delay so as to allow better transmission of voice and video.

802.11f-Roaming: The 802.11f is a recommendation for access point vendors that allows products to be more compatible. It uses the Inter-Access Point Roaming Protocol, which lets a roaming user transparently switch from one access point to another while moving around, no matter what brands of access points are used on the network infrastructure. This ability is also simply called roaming.

802.11g: The 802.11g standard offers high bandwidth (54 Mbps maximum throughput, 30 Mbps in practice) on the 2.4 GHz frequency range. The 802.11g standard is backwards-compatible with the 802.11b standard, meaning that devices that support the 802.11g standard can also work with 802.11b.

802.11h: The 802.11h standard is intended to bring together the 802.11 standard and the European standard (HiperLAN 2, hence the h in 802.11h) while conforming to European regulations related to frequency use and energy efficiency.

802.11i: The 802.11i standard is meant to improve the security of data transfers (by managing and distributing keys, and implementing encryption and authentication). This standard is based on the AES (Advanced Encryption Standard) and can encrypt transmissions that run on 802.11a, 802.11b and 802.11g technologies.

802.11Ir: The 802.11r stadard has been elaborated so that it may use infra-red signals. This standard has become technologically obsolete.

802.11j: The 802.11j standard is to Japanese regulation what the 802.11h is to European regulation.

The 802.11a, 802.11b and 802.11g standards, called "physical standards" are amendments to the 802.11 standard and offer different modes of operation, which lets them reach different data transfer speeds.

III. WEP

WEP known as Wired Equivalent Privacy.The main goal of WEP is to make Wi-Fi network at least as secure as wired LANand to encrpt data transmitted to prevent the attackers from getting the information.WEP offers services such as message confidentiality,message integrity and authencity and access control to the network.

WEP uses encryption algorithm called RC4.The key divided into two parts:IV(InitialVector) of 24 bits and Secret key of 40 bitsor 104 bits.There are two kinds of WEP-WEP64(40bit+24bit) and WEP 128(104bit+24bit).

This key is all-important to WEP in that it is also used in the encryption process to uniquely scramble each packet of information with a unique password. This ensures that if a hacker cracks one packets key,he won’t be able to view every packet’s information.WEP defines a method to create a unique secret key for each packet using the 5- or 13-characters of the pre-shared key and three more psuedo-randomly selected characters picked by the wireless hardware.

RC4 Algorithm

RC4 is the encryption algorithm used to cipher the data sent over the airwaves. It is important that data is scrambled; otherwise, anyone could “see” everything using a sniffer. This includes all e-mails, Web pages, documents, and more. RC4 is a very simple and fast method of encryption that scrambles each and every byte of data sent in a packet.It does this through a series of equations using the previously discussed secret key.RC4 actually consists of two parts: the Key Scheduling Algorithm and the Psuedo Random Generation Algorithm. Each part is responsible for a different part of the encryption process.

KSA (Key Scheduling Algorithm)

The Key Scheduling Algorithm is the first part of the encryption process. The following is the algorithm actually used in RC4.

```
1. Assume N = 256
2. K[] = Secrete Key array
3. Initialization:
4. For i = 0 to N – 1
5. S[i] = i
6. j = 0
7. Scrambling:
8. For i = 0 ... N – 1
9. j = j + S[i] + K[i]
10. Swap(S[i], S[j])
```

PRGA

The PRGA (Psuedo Random Generation Algorithm) is the part of the RC4 process that outputs a streaming key based on the KSA’s psuedo random state array. This streaming key is then merged with the plaintext data to create a stream of data that is encrypted.

```
1. Initialization:
2. i = 0
3. j = 0
4. Generation Loop:
5. i = i + 1
6. j = j + S[i]
7. Swap(S[i], S[j])
8. Output z = S[S[i] + S[j]]
9. Output XORed with data
```

The reason of transition to WPA.The same IV can be used more than once.The secret key is common in WEP.The key that WEP uses is short.Most users usually do not change their keys.

WPA:WPA known as Wi-Fi Protected Access.WPA use the TKIP and depends on RC4.The key in WPA consist of 128 bit and 48 bit for initial vector

TKIP:TKIP is a security protocol used in the IEEE 802.11 wireless networking standard.TKIP was a solution to replace WEP without requiring the replacement of legacy hardware..TKIP implement three new security features.TKIP implements a key mixing function.WPA implements a sequence counter to protect against replay attacks.Finally ,TKIP implements a 64-bit message integrity check named MICHAEL

	WEP	**WPA**	**WPA2**
Encryption	RC4	RC4	AES
Key rotation	None	Dynamic sessionkeys	Dynamic sessionkeys
Key distribution	Manually typed into each device	Automatic distribution	Automatic distribution

IV. CONCLUSIONS

As discussed above, security is not one time job. Security is constant vigilance against threats and attacks. We cannot eliminate hackers, pirates, thieves, etc. from the face of the earth. WPA (Wi-Fi Protected Access) is the next generation of wireless encryption technologies. It's far more secure and easier to configure than WEP. Almost all network devices support this. WPA replaces WEP with an improved encryption algorithm called Temporal Key Integrity Protocol (TKIP). TKIP supplies each client with a unique key and uses much longer keys that are rotated at a configurable interval. WPA also includes an encrypted message integrity check field in the packet to prevent denial-of-service and spoofing attacks, something that neither static for security. It can be used in Personal or Enterprise modes and has so far proven difficult to attack. It is recommended to use WPA or WPA2 encryption.

REFERENCES

[1] Arash Habibi Lashkari, F. Towhidi, R. S. Hoseini, "Wired EquivalentPrivacy(WEP)", ICFCC Kuala Lumpur Conference, Published byIEEE Computer Society, Indexed by THAMSON ISI, 2009

[2] Donggang Liu, P. N., "Security for Wireless Sensor Networks",Springer., November, 2006

[3] Garcia, R. H. a. M., "AN ANALYSIS OF WIRELESS SECURITY",CCSC: South Central Conference. 2006

[4] Kempf, J., "Wireless Internet Security: Architecture and Protocols",Cambridge University Press. October, 2008

[5] Hani Ragab Hassan, Yacine Challal, "Enhanced WEP: An efficientsolution to WEP threats", IEEE 2005

[6] Halil Ibrahim BULBUL, Ihsan BATMAZ, Mesut OZEL,"Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA(Wi-Fi Protected Access) and RSN (Robust Security Network)Security Protocols"; e-Forensics January 2008, Adelaide ,Australia.

[7] Gamal Selim, Hesham M. El Badawy, Mohamed Abdul Salam,"NEW PROTOCOL DESIGN FOR WIRELESS NETWORKSSECURITY", IEEE Explore

[8] Vebjørn Moen, H°avard Raddum, Kjell J. Hole, "Weaknesses in theTemporal Key Hash of WPA", University of Bergen,2005

[9] Arunesh Mishra, William, A. Arbaugh, "An Initial Security Analysisof the IEEE 802.1X Standard", University of Meryland, 2002

[10] Vebjørn Moen, H°avard Raddum, Kjell J. Hole; "Weaknesses in theTemporal Key Hash of WPA"; Mobile Computing andCommunications Review, 2005

[11] John L. MacMichael; "Auditing Wi-Fi Protected Access (WPA)Pre-Shared Key Mode"; Linux Journal, 2005.