International Journal of Electronics and Communication Engineering (IJECE)
ISSN(P): 2278-9901; ISSN(E): 2278-991X
Vol. 5, Issue 5, Aug - Sep 2016; 15-22

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

DESIGN OF A CUSTOM ENCRYPTION KEY GENERATOR TO SECURE WIRELESS NETWORKS

HARINDER KAUR[1] & HARPREET KAUR[2]

[1]M.Tech. Student, Punjab Agricultural University, Ludhiana, India

[2]Assistant Professor, Punjab Agricultural University, Ludhiana, India

ABSTRACT

The wireless LANs have been deployed at many places, small or big, houses or commercial complexes mainly because of their ease of installation and use. The IEEE 802.11-based WLAN presents new challenges for network and information security administrators. Whereas the security requirements of wired Ethernet deployments are relatively simple, security of a WLAN is somewhat complex. 802.11-based WLANs broadcast radio-frequency data for the client stations to receive. Hence, there are complex security issues that involve augmenting the 802.11 standard. This work critically reviews main security flaws of Wired Equivalent Privacy and suggests a new approach of automatic key management and refresh of WEP key so that attacker could not get sufficient time to guess the key.

KEYWORDS: Access Point, Ethernet, IEEE 802.11, IEEE 802.11i, Key Management, Local Area Networks, Network Interface Card, Radio-Frequency, RC4, Transmitter, Wired Equivalent Privacy, Wireless Local Area Networks

I. INTRODUCTION

Wireless Local Area Network (WLAN) is a wireless network that uses radio frequency technology instead of traditional coaxial. It has many merits such as handiness, high efficiency and low cost. Therefore, WLAN is widely used, especially when traditional network is difficult to install. But, at the same time WLANs have to face certain security issues such as leaking of electromagnetic wave or eavesdropping of data because in WLAN, electromagnetic wave is used as media to transmit data. Therefore, the security of WLAN is very important. Compared with traditional wired network, there is always a security threat while transmitting data through WLAN. It can't prevent attacker from eavesdropping and modifying spitefully because the channel in WLAN is open. Also, electromagnetic wave is subject to attenuation when it is transmitted in air, hence the transmitted information may lose some data. Finally, it is easier that attackers conceal themselves as legit user because it is not necessary for users to connect network. Hence higher communication secrecy capability is needed when utilizing WLAN to communicate.

Unlike the wired Ethernet, with 802.11 based technologies, one needs to consider radio frequency related security issues, since the data carried by a WLAN is accessible to anyone within range of the transmitter device. In an effort to preserve security while using wireless networks, IEEE designed the Wired Equivalent Privacy (WEP) protocol in their 802.11 specifications to offer some wired security like services, such as data privacy, integrity and authentication. The WEP protocol acts as an authentication method assuming that only authorized mobile stations share the correct key with the communicating device. Unfortunately, the WEP protocol has some security deficiencies which allow an unauthorized third party to determine the WEP encryption. Meanwhile, Wi-Fi Protected Access (WPA) was proposed by the Wi-Fi Alliance Group and IEEE to address the known WEP issues. WPA introduced two modes of deployments: WPA

Enterprise and WPA Personal. Whereas the enterprise edition offers more advanced key distribution protocols relying upon a complex network structure, the personal mode, also called WPA-PSK (pre-shared key), come in the form of a shared secret similar to WEP that have to be configured manually in mobile stations and access points. However, recent attacks on WPA-PSK suffer from vulnerabilities due to the use of static shared key.

The deployment of pre-shared keys is still adopted, mainly because the installation of an alternative solution remains too complex, too expensive or even impossible for many individuals and organizations. It is easy to use and configure and does not require any hardware or infrastructure renewal/replacement. In fact, the great number of already installed wireless equipment supporting only WEP makes it hard to retro-fit security fixes. The new products/devices will not interoperate with the older ones. Furthermore, many individuals and organizations maintain the permanent fixed key that never changes for weeks; months and even years, since renewing the keys can be a cumbersome task and requires installing the new key manually at every station. Deploying the same key, coupled with the flaws in the protocols themselves, significantly heightens WLAN vulnerability to eavesdroppers.

Through literature study, research is done on available solutions in the field of key management and security of wireless networks. The drawbacks of the existing solutions are also presented, in order to demonstrate the need of an improvement in this domain. The theoretical background needed to understand basic 802.11 concepts and issues related to the deployment of pre-shared keys is described, so that possible fixes can be included in the requirements of the system. Using the theoretical background as guideline, an automated wireless key management system following cryptographic key management techniques that changes the pre-shared keys automatically and regularly could address the issues discussed.

II. BACKGROUND AND MOTIVATION

A wireless network is a local area network without wires. Wireless networks have been around for more than a decade, but are now just beginning to gain momentum because of falling costs and improved standards. Wireless networks transfer data using radio frequencies instead of cable. They can reach a radius of 150 meters indoors and 300 meters outdoors, and this area can be further broadened using antennas, transmitters and other access devices. There are many wireless standards available in the market today. The dominating technology today adheres to the IEEE 802.11 specifications. With 802.11 based WLANs, users can get Ethernet levels of performance, throughput and availability. WLAN has the advantage of simplicity and ease of installation. There is no need to pull cables through walls and ceilings. Basic components of WLAN are access points (APs) and Network interface cards (NICs)/client adapters.

In light of several security issues related to WEP and IEEE 802.11 security, a new task group, IEEE 802.11i, was formed to come up with better authentication and encryption algorithms for WLANs. The resulting IEEE 802.11i standard uses many components. For instance, 802.11i proposes encryption key management with stronger data confidentiality algorithms, namely TKIP (Temporal Key Integrity Protocol) and CCMP2 (Counter Mode CBC MAC Protocol). TKIP is supposed to be a short term fix for WEP, whereas CCMP is envisioned to be the long term WLAN security solution. Installing all the 802.11i components depends upon having an infrastructure supporting 802.1x and equipments supporting the new standards, which means major changes are needed: APs supporting 802.1x authentication, mobile stations that are 802.1x supplicants (for example Windows XP Professional), and additional server platform supporting RADIUS (Remote Authentication Dial In User Service). Moreover, all mobile stations need to upgrade their firmwares for the wireless LAN cards in order to support TKIP or CCMP. However, many wireless manufacturers have abandoned their equipment and no longer provide updated drivers/firmware upgrades, thus forcing WLAN users to buy new hardware in order to benefit from

the new standards. This can be very expensive for many individuals and organizations, which already have old hardware. Moreover, a RADIUS server requires additional management hassle for IT administrators. Also, 802.1x does not address peer-to-peer communications.

Another possible approach is to force all WLAN connections to use a Virtual Private Network (VPN), typically through a firewall. By implementing a VPN solution to secure wireless transmissions, the wireless network is treated as an untrusted zone. The VPN server acts as a gateway to the corporate network by providing authentication and full encryption over the wireless network. An encrypted VPN tunnel is then built from the mobile station and terminated at the VPN server. The most widely used protocol for creating VPN tunnels is IP-Security (IPsec). Additionally, user authentication can occur using a centralized authentication service such as RADIUS.

While this approach employs standard IT industry technology, it requires a huge capital investment and system administration efforts, since all the remote clients need to configure the right security parameters. To support a VPN solution, a VPN client software application must be deployed on all the mobile stations that will use the WLAN, which does have an associated cost since most VPN vendors charge the client software per user basis. Additionally, the secure tunnels between the client and the VPN gateway must be integrated with a firewall. Another disadvantage is the lack of consistent roaming, then a new VPN connection may need to be established each time the mobile station roams between the coverage areas of one AP to that of another. An additional issue is the likeliness that hackers will connect to the network regularly, although they will not stay for a long time due to the other layer of protection. Therefore, the WLAN will be listed on war driving websites like WIGLE and attract attention of other potential hackers. Further, The APs are under the threat of denial of service attacks, because they are placed in an open network without protection, as VPN protects down to the network layer and not down to the data link layer. Another issue with hackers is that they could even place their own access points in hope of stealing the VPN credentials.

Stenman et al. proposed a system which uses the Internet Key Exchange (IKE) protocol and public key encryption algorithms to first mutually authenticate mobile stations and APs and then to securely exchange sessions key used to encrypt subsequent packets. While this technique both authenticates the wireless clients and APs and cryptographically protects the transmitted packets, it involves installation and administration overhead. Also it requires a change in the APs firmwares since the authentication is done between the mobile stations and the base station. Further, the protocol consumes significant time and bandwidth for each connection, which is a significant drawback for roaming mobile stations. RSA Security, Inc. proposed modification to the present IEEE 802.11 standards to overcome the weaknesses in the WEP protocol, which Andersson summarized in a paper. This approach effectively uses an authentication protocol at the network layer level and a new algorithm to compute the key used for each packet transmitted.

Shared key authentication is based on a cryptographic key known as a Wired Equivalent Privacy (WEP) key which is shared by legitimate stations (STAs) and APs. Shared key authentication uses a simple challenge-response scheme based on whether the STA seeking WLAN access knows the WEP key. The STA initiates an Authentication Request with the AP, and the AP generates an 128-bit value randomly and sends it to the STA. Using the WEP key, the STA encrypts the value and returns the result to the AP. Then, the AP, using the same WEP key decrypts the result and allows the STA access only if the decrypted value matches with the value. The RC4 stream cipher algorithm is used for all the cryptographic computations involved, which generates a pseudo-random data sequence. This data sequence is then combined with data to encrypt or decrypt data.

Shared key authentication is still threat-prone because the AP is not authenticated to the STA, so there is no assurance that the STA is communicating with a legitimate AP. Another major problem with shared key authentication is that it requires all devices on a WLAN to use the same WEP key(s). This leads to reduced accountability and complicated troubleshooting. If the WEP key is compromised, it needs to be changed quickly. Unfortunately, IEEE 802.11 does not specify any support for key management. Further, generating and distributing a new key is a cumbersome process. The key needs to be replaced manually on all STAs and APs. WLAN administrators also need to implement methods for archiving old keys and auditing and destroying current keys. Key management problems often limit the scalability of IEEE 802.11 WLANs. In some implementations, poorly designed WEP keys are used, for example, trivial keys, such as all zeroes or all ones, which is very easy to guess. The key should be randomly generated so that it is not easily guessable. Once generated, they should be changed frequently to mitigate the impact of any key compromises.

However, the process of changing the keys is cumbersome and very time consuming because keys must be entered manually on all the mobile stations and access points; WEP does not specify a mechanism to centrally manage the keys and control user access into the WLAN. Key distribution and updates must be done in a secure medium outside of 802.11. The standard allows only for access points and network client adapters to hold four different WEP keys with four indexes, of which only one default key is active at a time and is used for transmission. A mobile station or AP can decrypt packets encrypted with any one of these four keys which still have to be entered manually. In a secure environment, cryptographic keys need to be automatically changed at periodic intervals or per session to limit the time any key is used. A transparent method for centrally managing and updating WEP keys is thus desirable.

III. OBJECTIVES

Because the 802.11 standard relies on an independent secure channel to generate and distribute the pre-shared keys (pre-shared keys refers to WEP static keys) to each station and does not specify key distribution services, most 802.11 WLAN deployments rely on manual key generation and distribution. This means that the pre-shared key remains the same unless the network administrator generates a new key and manually updates it on each access point and mobile station. Optionally, the keys could be distributed via email or fax to each user, who needs then to manually configure the new key, since the keys themselves are usually meaningless sequences of characters and digits, errors could occur when humans manually enter the key information. Administrators therefore tend to deploy easy to remember keys and thus easy to crack as well. Once the new key is updated at the access point, no user is able to connect to the WLAN until the key at the mobile station is updated to match the new key deployed at the access point. Obvious problems result from the fact that the keys are static in nature and the process of key management is manual as changing the keys on each station can be extremely time consuming, error prone and cumbersome, especially because of the mobility of WLAN users. If a mobile station is lost due to theft or accident, or if a mobile user needs to be revoked access to the WLAN, the process of updating new keys must then be repeated for each wireless station. If a key is static it simplifies the work of an attacker to crack it. He does not have to worry about a shortened period of time to capture network traffic in order to crack the key information before the key changes. In a secure environment, cryptographic keys are automatically changed at periodic intervals.

The research problem taken here is to design a system that mitigates the problems stated earlier by automatically managing the deployment of 802.11 pre-shared keys. The proposed system should provide a mechanism to automatically generate, distribute, synchronize and deploy pre-shared keys frequently at the base stations as well as at all authorized mobile stations, with minimal end user involvement. The current solution will allow wireless users to receive key securely

via the insecure wireless channel and allow installation of new keys, without any manual involvement of the user itself or the network administrator. The system will be useful for existing WLAN deployments that cannot afford to make use of the new 802.11 standards. Changing the key automatically and frequently helps to make sure that the wireless connections are at all times secure. It also helps reducing costs and management overhead of manually updating the keys on each station, without the need of an expensive complex infrastructure and/or change of the already installed wireless devices.

The objectives can be stated as follows:

- To improve the key management and security flaws of existing WEP standard with minimal interruption to existing system and user operation
- To improve the key generation technique on WEP by developing an algorithm to produce random keys to fight against hacking
- To demonstrate the need and effectiveness of an automated management system for 802.11 pre-shared keys

IV. RESEARCH METHODOLOGY

Cryptography has been an accepted method of protecting data for many years. It does this by enabling information to be shared only with individuals that hold the key to decipher the information. In cryptography, key are required for encryption and authentication. These procedures do not provide security when the keys have been handled incorrectly. How to initialize these keys and how to properly manage keys through the lifetime of a cryptographic system is the job of a key management scheme. Key management has to do with the effective generation, distribution, installation, storage, change, control and deletion of cryptographic keys. A key management system delivers the necessary keys to all the parties. Key management is actually the most important but also the hardest part of cryptography. From the moment it is generated until it is deleted, managing the life cycle of the key is very important to ensure that it is never exposed to misuse. Key Generation is the process of creating a key. Keys can be created using either manual or automatic generation. Key Distribution is the process of distributing newly created keys to all the users and processes. After keys are generated, they must be stored somewhere for a later use. Proper storage for both short and long periods of time is essential for good security. During the lifetime of a key, it may be stored in many different places such as in memory or on disk. And finally, the most challenging part of any key management system is ensuring that, once a key has been exposed, retired or the data media on which it was stored has been lost, stolen, or replaced, it can be deleted safely.

Generation of random WEP keys can be a tedious work - it's difficult to think up new ones. The keys must be changed regularly to prevent any security issues. The first option is to create a Custom WEP Key by entering a pass phrase. The pass phrase string is then separated into characters and an integer index number is returned. This number will be used by the second method when we convert string to HEX, and will be merged into one string that will be finally returned to the caller. The second option, probably the strongest, is to create a pseudo random WEP Key by selecting the corresponding length required by your hardware. It uses pretty much the same methods; the only thing is that Generate Strong Key now gives the pass phrase.

Software was designed to generate a random WEP encryption key. It will provide the equivalent HEX string which can be inserted directly into access point configuration. It inputs ***Port*** and ***Baud Rate*** to connect with the port. After

connection is established, it demands ***Key Type*** for specifying the length of key, i.e. whether 64-bit, 128-bit, 152-bit or 256-bit key to generate. And finally, ***Refresh key in*** specifies time to refresh key after. The encryption keys are generated likewise based on different values of inputs as shown in Figure 1. All the generated keys are displayed below as a grid. There is an option to ***Copy all Keys*** to copy all generated keys to the clipboard.

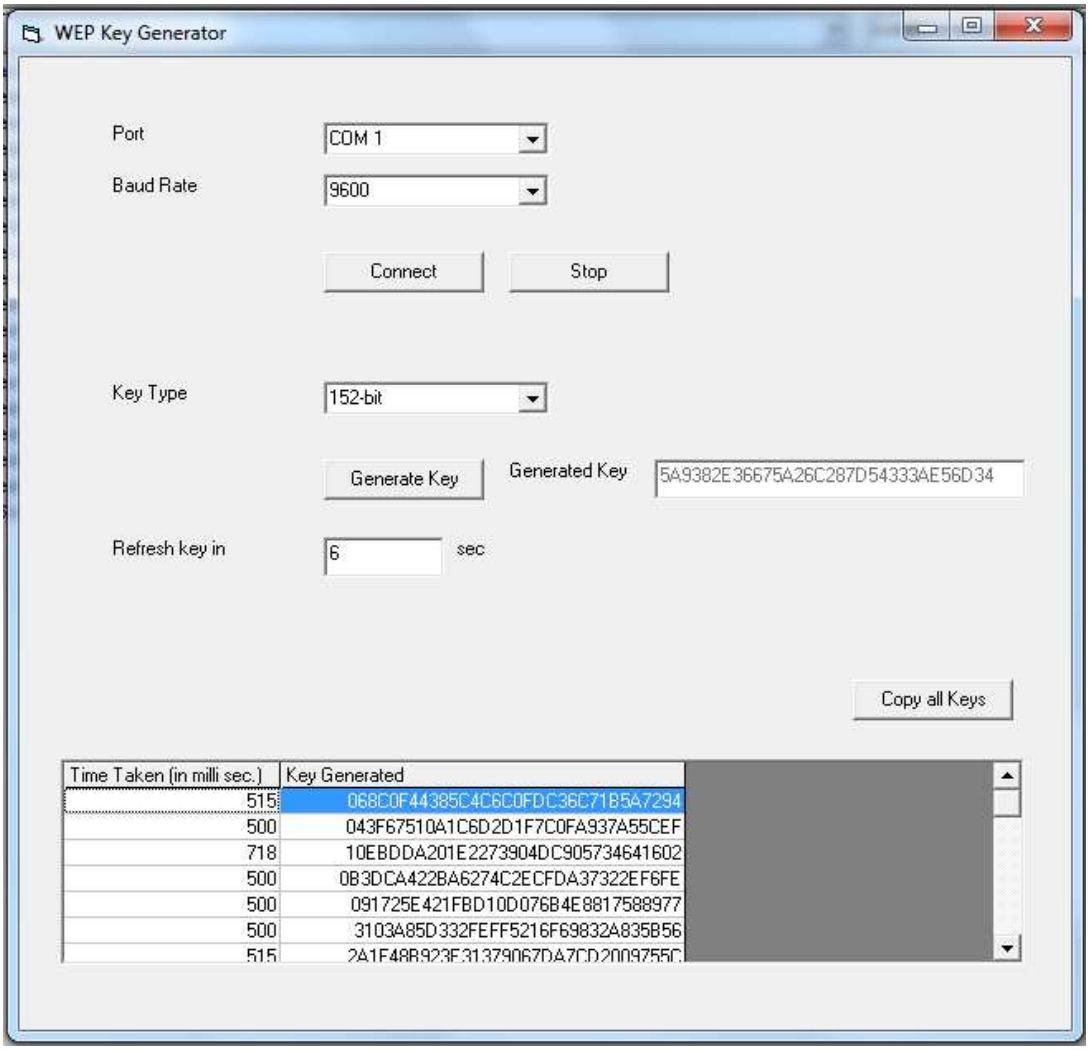

Figure 1: WEP Key Generator

V. CONCLUSIONS

While all the earlier methods discussed can effectively solve the network security issues but deployment of these solutions requires a new complex infrastructure, new hardware capabilities, radio drives and firmware. Therefore, they may not be compatible with existing mobile stations and access points. Furthermore, none of the approaches discussed above provide a way to distribute and manage WPA-PSK keys. Thus the solution adopted in this thesis, involves minimal changes to the existing infrastructure and does not require any hardware changes. And unlike other solutions, the presented approach can be applied to all kinds of WLANs.

This thesis focuses on the design of a system that complies with the 802.11 devices and infrastructures that support only the deployment of pre-shared keys, which means we do not solve the issues from which the 802.11 protocol themselves suffer but we mitigate the risks associated with such deployments by solving the key management issues.

Implementing a complete key management system is a time consuming task and was achieved to some extent. Future work can be done for its large scale deployment and to make it cheaper and user friendly.

REFERENCES

1. Anderson, Ross, and Markus Kuhn. "Tamper resistance-a cautionary note."*Proceedings of the second Usenix workshop on electronic commerce*. Vol. 2. 1996.
2. Andersson, Hakan. "Wireless LAN upper layer authentication and key negotiation." *RSA Security* 17 (2002).
3. Arbaugh, William A. *Real 802.11 security: Wi-Fi protected access and 802.11 i*. Addison-Wesley Longman Publishing Co., Inc., 2003.
4. Arbaugh, William A., et al. "Your 802.11 wireless network has no clothes."*Wireless Communications, IEEE* 9.6 (2002): 44-51.
5. Borisov, Nikita, Ian Goldberg, and David Wagner. "Intercepting mobile communications: the insecurity of 802.11." *Proceedings of the 7th annual international conference on Mobile computing and networking*. ACM, 2001.
6. Cam-Winget, Nancy, et al. "Security flaws in 802.11 data link protocols."*Communications of the ACM* 46.5 (2003): 35-39.
7. Chandran, Nishanth and Dhananjay Sampath. "Strengthening wep protocol for wireless networks using block chaining algorithm with variable encrypting function mechanism." *Advances in Wired and Wireless Communication, 2004 IEEE/Sarnoff Symposium on*. IEEE, 2004.
8. Earle, Aaron E. *Wireless security handbook*. CRC Press, 2005.
9. Elaine, Barker, et al. "Recommendation for key management–part 1: general." *NIST Special Publication* (2006): 800-57.
10. Fluhrer, Scott, Itsik Mantin and Adi Shamir. "Weaknesses in the key scheduling algorithm of RC4." *Selected areas in cryptography*. Springer Berlin Heidelberg, 2001.
11. Gast, M. "802.11 Wireless Networks The Definitive Guide O'Reilly and Associates." (2002).
12. Gutmann, P. "IEEE wireless LAN medium access control (mac) and physical layer (phy) specifications standard 802.11 c1997." *IEEE Computer Society LAN MAN Standards Committee* (1997).
13. Gutmann, P. "Software Generation of Practically Strong Random Numbers." *Usenix Security*. 1998.
14. Hollingshead, Tom. "802.11 Wireless Security vs. Basic Network Security Principles." *SANS Institute*, 2003.
15. IEEE 802.1 Standard Working Group. "IEEE standard for local and metropolitan area networks: port-based network access control." *IEEE Std*802.
16. IEEE Amendment 6: Medium Access Control (MAC) Security Enhancements. IEEE Standard 802.11i, 2004.
17. Knuth, Donald Ervin. *The art of computer programming: sorting and searching*. Vol. 3. Pearson Education, 1998.
18. Moskowitz, Robert. "WLAN Testing Reports." *PSK as the Key Establishment Method, ICSA Labs* (2003).

19. Park, Stephen K., and Keith W. Miller. "Random number generators: good ones are hard to find.

“Communications *of the ACM* 31.10 (1988): 1192-1201.

20. PUB, FIPS. *Security Requirements for Cryptographic Modules*. Diss. National Institute of Standards and Technology, 1999.

21. Rigney, C., et al. "Rfc 2865: Remote authentication dial in user service."*Internet Society (Jun. 2000)* (2000).

22. Schneier, Bruce. *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

23. Stenman, Jorma, Harri Hansen and Juha Salvela. "Key management methods for wireless LANs." U.S. Patent No. 7,028,186. 11 Apr. 2006.

24. Takahashi, Takehiro. "WPA passive dictionary attack overview." *Erhältlich unter:*

http://www.uninett.no/wlan/download/wlan-mac-spoof.pdf (2004).

25. Tipton, Harold F. and Micki Krause. *Information security management handbook*. CRC Press, 2003.

26. Walker, Jessie. "Unsafe at any key size; an analysis of the WEP encapsulation." *IEEE document* 802.00 (2000): 362.

27. "Wireless LAN” *wikipedia.com.* Retrieved Apr. 26, 2014, from https://en.wikipedia.org/wiki/Birthday_attack.

28. "Birthday attack” *wikipedia.com.* Retrieved Jul. 7, 2013, from https://en.wikipedia.org/wiki/Birthday_attack.