ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 3 March 2015, Page No. 10968-10971

A Survey: Wireless Lan Security Protocols

Anik Shah, Animesh Shah
12bce084
Computer science, Nirma university.
12BCE084@nirmauni.ac.in
12bce085
Computer science, Nirma university.
12BCE085@nirmauni.ac.in

Abstract— As we all know, Wireless Local Area Networks (WLANs), which is based on the IEEE 802.11 standards, is growing at a very considerable rate in the fields of business, schools and other organizations. As WLAN deployments increase, so does the challenge to provide these networks with security. Security can be needed either for the technical issues in the mechanisms, or due to software implementations. This survey paper proposes the use of GSE technique to analyze the shortcomings in the standards specified. After providing with the issues, we will switch focus to the Robust Security Network (RSN) which is proposed in the IEEE 802.11i standard using different GSE models.

Index Terms- WLAN Security, Robust Security Network (RSN), IEEE 802.11i, Security, Genetic Software Engineering (GSE), WPA (Wi-Fi Protected Access), Advanced Encryption Standard (AES).

I. INTRODUCTION

Wireless Local Area Networks or WLANs are expected to gain monopoly over all other wireless products in the market. WLANs facilitate us with ubiquitous communications and location-independent computing in restricted spatial domains such as offices, factories, hospitals etc. [1] WLANs is famous due to the following desirability : low cost, easy to install, flexibility, tether-less access to information infrastructure and support for ubiquitous computing through station mobility. It also provides advantage of quick installation in an ad-hoc configuration without a supporting backbone network.

The IEEE 802.11i standard proposes a robust security network (RSN) with much improved authentication, authorization and encryption capabilities. Though these new standards are more complicated than their antecedents, they are more secure than existing networks. [2]

In the infrastructure topology, wireless stations or STAs communicate wirelessly to a network access point (AP) which forms the WLAN. [3]

There are a lot of problems regarding the security of WLANs like using Radio Frequency as a medium of transmitting information and the fact that all messages are broadcasted to wherever the coverage of that WLAN can reach. [4] As the propagation of airwaves cannot be blocked or locked in a room, risk of man-in-the-middle-attacks exists.

Nevertheless, naïve implementation of the security protocol can lead to the same security issues of technical flaws. So, a set of requirements for the RSN from the IEEE 802.11i standards is formulated.

GSE technique [5] is used to analyze the requirements for shortcomings and thus identified ambiguities are resolved using appropriate domain expertise to derive at a complete set of requirements. GSE technique enables systematic modeling of complex systems with good traceability, control and accommodation of change. [6]

We provide with the requirements, analyses and modeling details of the WLAN security further in this paper.

II. WLAN SECURITY CHARACTERISTICS

In this subsection we will discuss the WLAN characteristics those are pertinent to security protocols design.

- Roaming: It is the ability to deliver services to wireless stations outside of the basic service area. When a wireless station is roaming, new authentication through the wireless medium must be performed to ensure the new origination of

communication and the new session key from unauthorized access and use.

- Reduce power Consumption: Since the WLANs are intended for portable battery operated wireless stations, low power consumption is a very important factor to be taken into consideration. Therefore, the security mechanisms developed should use relatively low complex cryptographic algorithms.

- Limited Bandwidth: The limited ISM frequency band allocated by the FCC and the requirement to use spread spectrum communication limit the data rate. This characteristic will require security protocol design that reduces the number of messages exchanged over the wireless medium.

- Noisy Channel: In WLANs, the bit error rate is high relatively to wired transmission medium. This characteristic will describe security protocols that incorporate appropriate provisions for erroneous messages and retransmission procedures.

III. WLAN SECURITY STANDARDS

The evolution of today's WLAN security standards begins with 802.11. This standard helped launch practical WLANs that were ideal for the home and most small offices, but lacking in features required by the large enterprise. Authentication was essentially ignored by the standard.

The data privacy solution was WEP. It is an implementation of the RC4 algorithm. The RC4 encryption technique is strong enough, but a weak implementation in 802.11 meant it was only strong enough to protect against casual eavesdropping. In addition, the proliferation of readily available hacking tools led to WEP being generally discredited for enterprise wide distributed processing environments [7].

IEEE 802.11i and WPA2 are future WLAN standards introduced by the IEEE and Wi-Fi Alliance respectively. The new features in 802.11i/WPA2 are AES (Advanced Encryption Standard), message integrity, and fast-roaming support (pre-authentication). Vendor interoperability, as well as forward and backward compatibility, has been consistent themes for the IEEE and Wi-Fi Alliance as WLAN standards have evolved [8].

Because of the shortcoming of security technologies in IEEE802.11, Wi-Fi Alliance released a new security standard for the industry called "Wi-Fi Protected Access" (WPA). WPA added two more technologies, namely, IEEE802.1x to improve authentication and TKIP for privacy and integrity of information.

Recently IEEE published a new security standard for WLANs, the new standard is IEEE802.11i [9], the new standard provides enhancements of the security shortcomings of WEP and it comprises all security technologies in WPA.
In addition to that, IEEE802.11i adopts recently certified encryption algorithm called the "Advanced Encryption Standard" (AES).

The usage of security technologies to discover and fix security holes and to maintain security in a WLAN environment has to be compatible with a security policy issued by the organization's management to achieve best results. The security policy defines who are alleged wireless users, wireless user's responsibilities, network security administrator's responsibilities, what to be done in the case of security violations and general guidelines in implementing and maintaining WLAN security. Such security policies are to be adhered and enforced in order to be effective.

IV. WLAN SECURITY ATTACKS

Data transfer through WLANs can be affected adversely by many security threats and attacks. They can be broadly divided into two types: Logical attacks and Physical attacks.

Logical Attacks:

- Attacks on WEP: Web Equivalent Privacy (WEP) is a protocol based on encryption algorithm known as RC4. It aims to provide security to the WLAN similar to the one provided in wired LAN. [4] It still has major drawbacks as the encrypted messages can be easily retrieved using publicly available tools.

- MAC Address Spoofing: MAC addresses are sent in the clear when communication between STAs and AP takes place with integrity. Integrity means to preserve the accuracy of information transmitted between STAs and AP [10]. Since addresses are sent in the clear, an attacker can obtain the address of authorized station by sniffing airwaves using tools like ethereal and kismet and can thus spoof them. [11] This is a major security violation.

- Denial of Service Attack: DoS is a serious threat on both kinds of networks, which aims to disable the availability of the network and its services. [10] Little is done so far to counteract DoS attacks.

- Man-in-the-Middle Attack: This is a famous attack in both wired and wireless networks. An illicit STA intercepts the communication between legitimate STAs and the AP. The illegal STA fools the AP and pretends to be a legitimate STA; on the other hand, it also fools the other end STA and pretends to be trusted AP. Using techniques like IEEE802.1x to achieve mutual authentication between APs and STAs as well as adopting an intelligent wireless Intrusion Detection System can help in preventing such attacks.

- Bad Network Design: WLANs function as an extension to the wired LAN and hence the security of the LAN depends highly on the security of the WLAN. The vulnerability of WLANs means that the wired LAN is directly on risk. Also dedicating specific subnets for WLAN than the once used for wired LAN could help in limiting security breaches. Careful wired and wireless LAN network design plays an important role to secure access to the WLAN.

- Default AP configuration: Service Set Identifier (SSID) is the name given to a certain WLAN and it is announced by the AP, the knowledge of SSID is important and works like the first security defense.

Some APs don't disable SSID request, in fact the SSID request is enabled but the SSID name itself is broadcasted in the air. This is another security problem because it advertises the existence of the WLAN.

Physical Attacks:

- Rogue Access Points: The APs which are also known as "Rogue APs" are installed without IT center's awareness and they form a security hole in the network. [12] Network security administrators can discover Rogue APs by using wireless analyzing tools to search and audit this network.

	WEP	**WPA**	**WPA2**
Purpose	Provide security comparable to wired networks	Overcome the flaws of WEP without requiring new hardware, Implements majority of IEEE 802.11i standard	Implements completely IEEE 802.11i standard and an enhancement over WPA
Data Privacy (Encryption)	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Counter Mode with Cipher block Chaining Message Authentication Code Protocol (CCMP) using block cipher Advanced Encryption Standard (AES)
Authentication	WEP-Open and WEPShared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise
Data Integrity Code	CRC-32	Michael (generates Message Integrity (MIC))	Cipher block chaining message authentication code (CBC-MAC)
Key Management	Lack of key management	Provides robust key management and keys are generated through four way Handshake	Provides robust key management and keys are generated through four way handshake
Hardware Compatibility	Works on existing hardware	Works on existing hardware through firmware upgrades on NIC	Supported in Wi-Fi devices certified since 2006, Does not work with older NIC
Deployment complexity	Easy to setup and configure	Complicated setup required for WPAenterprise	Complicated setup required for WPA2-Enterprise

- Physical placement of APs: The installation location of APs is another security issue because placing APs inappropriately will expose it to physical attacks. Attackers can easily reset the APs once found causing the AP to switch to its default settings which is totally insecure. It is very important for network security administrators to carefully choose appropriate places to mount APs.

- AP's coverage: The signals broadcasted by the AP can propagate outside the perimeter of a room or a building, where an AP is placed, which allows users who are not physically in the building to gain access to the network remotely. Attackers use special equipments and sniffing tools to find available WLANs and eavesdrop live communications while driving a car or roaming around CBD areas. Because RF signals obey no boundaries, attackers outside a building can receive such signals and launch attacks on the WLAN. This kind of attack is known as "war driving" [13].

V. SUMMARY

First of all, this survey paper gives us a brief introduction about the WLAN network and the security threats imposed on it while transferring data. After giving the central idea, we explain the WLAN Security characteristics in short. Further, we describe the WLAN security standards through different references. Finally, we discuss the different types of attacks and their possible solutions.

VI. ACKNOWLEDGEMENT

This survey paper wouldn't have been produced without the mentorship and guidance of Prof. Pushpak Raval.

References:

[1] Borisov, N. Goldberg, I. Wagner, D. "Intercepting Mobile Communications: The Insecurity of 802.11", ACM SOGMOBILE, Vol. 7, Jan. 2001, pp. 180-188.

[2] Mead, N.R. McGraw, G. "Wireless Security Future", IEEE Security & Privacy, July/Aug. 2003, pp. 68-72.

[3] IEEE Standard for local and metropolitan area networks, "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications", ANSI/IEEE Std 802.11, 1999 Edition (R2003).

[4] Shin, M.; Ma, J.; Mishra, A.; Arbaugh, W.A., "Wirelessnetwork security and interworking", Proceedings of IEEE, Volume 94, Issue 2, pp 455 – 466, February 2006.

[5] Dromey, R.G. From Requirements to Design: formalizing the key steps, Proc. 1st International Conference on Software Engineering and formal methods, Sep. 2003, Brisbane, Australia, pp. 2-11.

[6] Sithirasenan, E. Muthukkumarasamy, V. "A Model for Object Based Distributed Processing Using Behavior Trees: Proceedings of the Eighth IASTED International Conference on Software Engineering and Applications, Nov. 2004, Cambridge MA, USA, pp 477-482.

[7] Stubblefield, A. Ioannidis, J, Rubin, A.D. A key recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)", ACM Transactions on Information and System Security, Vol. 7, No. 2, May 2004, pp. 319-332.

[8] Wi-Fi Alliance. "Wi-Fi Protected Access (WPA)", Version 2.0, April 2003.

[9] IEEE Standard for local and metropolitan area networks, "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications, Medium Access Control (MAC) Security Enhancements". ANSI/IEEE Std 802.11i, 2004 Edition.

[10] William Stallings, Cryptography and Network Security Principles and Practices, 3rd Edition, Prentice Hall 2003.

[11] Joon S.Park and Derrick Dicoi, "WLAN Security: Current and Future". IEEE Computer Society, October 2003.

[12] Joel W. Branch, Nick L.Petroni JR, Leendert Van Doorn and David Safford, "Autonomic 802.11 Wireless LAN Security Auditing". IEEE Security & Privacy, 2004.

[13] War driving website, http://www.wardriving.com/

[14] IEEE 802.11 Wireless LAN Security Overview
Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen
IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, May 2006

[15] Wireless Network Security Protocols A Comparative Study
Swati Sukhija, Shilpi Gupta
International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 1, January 2012)

[16] IEEE 802.11i WLAN Security Protocol – A Software Engineer's Model
AusCERT2005: Refereed R&D Stream