RESEARCH REVIEW JOURNALS
Volume-03
Issue-12
December -2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

A Study of Wireless Security & Risk Contentions

[1]Anoop Saxena and [2]Dr. Vijay Kumar Pandey

[1]*Research Scholar, Department of Computer Science& Engineering, Mewar University*
[2]*Professor, Noida Institute of Engineering and Technology*

ARTICLE DETAILS

Article History
Published Online: 10 December 2018

Keywords
WLAN Security, IEEE 802.11i, RSN, GSE, WEP, WPA, EAP, Wireless Intrusion Detection Systems.

ABSTRACT

Wireless local area networks (WLANs) based on the IEEE 802.11 standards are one of today's fastest growing technologies in businesses, schools, and homes, for good reasons. With the increase in deployment of WLAN, security challenges are also increased. Any technical lapse or any type of defect in software implementation may originate security risk. Standard Bodies and researchers have mainly used UML state machines to address the implementation issues. In this paper we have discussed various Wireless security issues and risks for the purpose of prevention of unauthorized access or damage to computers using wireless networks.

1. Introduction

The first wireless security solution for 802.11-based networks, the Wired Equivalent Privacy (WEP), received a great deal of coverage due to various technical failures in the protocol [1]. More time and money is being spend by the standard bodies and organization on developing and deploying next-generation solutions that address growing wireless network security problems. The IEEE 802.11i standard proposes a Robust Security Network (RSN) with much improved authentication, authorization, and encryption capabilities. The Wi-Fi Alliance, a wireless industry organization, has created the Wi-Fi Protected Access (WPA) standard, a subset of the 802.11i.

In comparison to the predecessors, these new standards are more complicated but are more scalable and secure than existing wireless networks. They also dramatically raise the bar for attackers and administrators. The new standards will employ a phased adoption process because of the large installed base of 802.11 devices. Proper migration to 802.11i and mitigating the legacy wireless risks will be a bumpy road. However, the end result will provide users a secure base for mobile distributed processing needs [2]. Nevertheless, the strong security mechanism can still be in vain if not implemented properly. Software Engineers must be able to correctly interpret and comprehend the standards. A naive implementation of the security protocol can lead to the same security breaches caused by technical flaws. In this regard, firstly, we have formulated a set of requirements for the RSN from the IEEE 802.11, 802.1X, and 802.11i standards. Next, we use the GSE methodology [3] to analyse these requirements for incompleteness, uncertainties, and inconsistencies. Thus identified ambiguities are resolved using appropriate domain expertise to derive at a complete and consistent set of requirements. Thereafter, new set of requirements may be used to build an implementation model for the RSN.

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Equivalent Privacy(WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device which encrypts the network with a 256 bit key; the longer key length improves security over WEP.

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues.[1]Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks.[2]As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources.[3]Wireless Intrusion Prevention Systems (WIPS)or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Hackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level.[4]Hacking methods have become much more sophisticated and innovative with wireless. Hacking has also become much easier and more accessible with easy-to- use Windows or Linux-based tools being made available on the web at no charge.

Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. In-Stat MDR and META Group have estimated that 95% of all corporate laptop computers that were planned to be purchased in 2005 were equipped with wireless. Issues can arise in a supposedly non- wireless organization when a wireless laptop is plugged into the corporate network. A hacker could sit out in the parking lot and gather info from it through laptops and/or other devices as handhelds, or even break in through this wireless card-equipped laptop and gain access to the wired network.

2. The Threat situation

Wireless security is just an aspect of computer security, however organizations may be particularly vulnerable to security breaches [5]caused by rogue access points. If an trusted entity brings in a wireless router and plugs it into an unsecured switch port, the entire network can be exposed to anyone within range of the signals. Similarly, if an employee adds a wireless interface to a networked computer via an open USB port, they may create a breach in network security that would allow access to confidential materials. However, there are effective counter measures that are available to protect both the network and the information it contains, but such countermeasures must be applied uniformly to all network devices.

3. Threats and Vulnerabilities in an industrial (M2M) context

Due to its availability and low cost, the use of wireless communication technologies increases in domains beyond the originally intended usage areas, e.g. M2M communication in industrial applications. Such industrial applications often have specific security requirements. Hence, it is important to understand the characteristics of such applications and evaluate the vulnerabilities bearing the highest risk in this context. An evaluation of these vulnerabilities and the resulting vulnerability catalogues in an industrial context when considering WLAN, NFC and ZigBee can be found here[6]

The Mobility Advantage

Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues.[1]Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks.[2]As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources.[3]Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

The Air interface and link corruption risk

There were relatively few dangers when wireless technology was first introduced, as the effort to maintain the communication was high and the effort to intrude is always higher. The variety of risks to users of wireless technology have increased as the service has become more popular and the technology more commonly available. Today there are a great number of security risks associated with the current wireless protocols and encryption methods, as a carelessness and ignorance exists at the user and corporate IT level.[4]Hacking methods have become much more sophisticated and innovative with wireless.

Accidental and Malicious association

Violation of the security perimeter of a corporate network can come from a number of different methods and intents. One of these methods is referred to as “accidental association”. When a user turns on a computer and it latches on to a wireless access point from a neighboring company’s overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network. Accidental association is a case of wireless vulnerability called as "miss-association".[7]Miss- association can be accidental, deliberate (for example, done to bypass corporate firewall) or it can result from deliberate attempts on wireless clients to lure them into connecting to attacker's APs. “Malicious associations” are when wireless devices can be actively made by attackers to connect to a company network through their laptop instead of a company access point (AP). These types of laptops are known as “soft APs” and are created when a cyber- criminal runs some software that makes his/her wireless network card look like a legitimate access point. Once the thief has gained access, he/she can steal passwords, launch attacks on the wired network, or plant Trojans. Since wireless networks operate at the Layer 2 level, Layer 3 protections such as network authentication and virtual private networks offer no barrier. Wireless 802.1x authentications do help with some protection but are still vulnerable to hacking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the criminal is just trying to take over the client at the Layer 2 level.

Identity theft (MAC spoofing)

Identity theft occurs when a hacker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to allow only authorized computers with specific MAC IDs to gain access and utilize the network. However, programs exist that have network “sniffing” capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the hacker desires,[8]and the hacker can easily get around that hurdle.

MAC filtering is effective only for small residential (SOHO) networks, since it provides protection only when the wireless device is "off the air". Any 802.11 device "on the air" freely transmits its unencrypted MAC address in its 802.11 headers, and it requires no special equipment or software to detect it. Anyone with an 802.11 receiver (laptop and wireless adapter) and a freeware wireless packet analyzer can obtain the MAC address of any transmitting 802.11 within range. In an organizational environment, where most wireless devices are "on the air" throughout the active working shift, MAC filtering provides only a false sense of security since it prevents only "casual" or unintended connections to the organizational infrastructure and does nothing to prevent a directed attack.

Man-in-the-Middle Attacks

Connections between authorized stations and access points are intercepted by inserting a malicious station between the victim’s station and the access point[13].

Session Hijack

A more advanced version of the above with the adversary gaining access to session information and intruding the network[13].

Denial of service

A Denial-of-Service attack occurs when an attacker continually bombards a targeted Access Point or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

The Do's attack in itself does little to expose organizational data to a malicious attacker, since the interruption of the network prevents the flow of data and actually indirectly protects data by preventing it from being transmitted. The usual reason for performing a Do's attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use various cracking tools to analyse security weaknesses and exploit them to gain unauthorized access to the system. This works best on weakly encrypted systems such as WEP, where there are a number of tools available which can launch a dictionary style attack of "possibly accepted" security keys based on the "model" security key captured during the network recovery.

Network injection

In a network injection attack, a hacker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as "Spanning Tree" (802.1D), OSPF, RIP, and HSRP. The hacker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices

Wireless intrusion prevention concepts

A Wireless Intrusion Prevention System is a concept for the most robust way to counteract wireless security risks.[11]However such WIPS does not exist as a ready designed solution to implement as a software package. A WIPS is typically implemented as an overlay to an existing Wireless LAN infrastructure, although it may be deployed standalone to enforce no-wireless policies within an organization. WIPS is considered so important to wireless security that in July 2009, the Council published wireless guidelines [12]for PCI DSS recommending the use of WIPS to automate wireless scanning and protection for large organizations.

4. There are three principal ways to secure a wireless network.

- For closed networks the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. Another option is to disable ESSID broadcasting, making the access point difficult for outsiders to detect. System scan be used to provide wireless LAN security in this network model.
- For commercial providers, hotspots, and large organizations, the preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN.
- Wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it is also often possible for remote intruders to gain access to the network through backdoors like Back Orifice. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

There is no ready designed system to prevent from fraudulent usage of wireless communication or to protect data and functions with wirelessly communicating computers and other entities. However there is a system of qualifying the taken measures as a whole according to a common understanding what shall be seen as state of the art. The system of qualifying is an international consensus as specified in ISO/IEC 15408.

Security measures

There are a range of wireless security measures, of varying effectiveness and practicality.

SSID hiding

A simple but ineffective method to attempt to secure a wireless network is to hide the Service Set Identifier.[13]

[14]this provides very little protection against anything but the most casual intrusion efforts.

MAC ID filtering

One of the simplest techniques is to only allow access from known, pre-approved MAC addresses. Most wireless access points contain some type of MAC ID filtering. However, an attacker can simply sniff the MAC address of an authorized client and spoof this addresses.

Static IP addressing

Typical wireless access points provide IP addresses to clients via DHCP. Requiring clients to set their own addresses makes it more difficult for a casual or unsophisticated intruder to log onto the network, but provides little protection against a sophisticated attacker.[14]

802.11 security

IEEE802.1X is the IEEE Standard authentication mechanisms to devices wishing to attach to a Wireless LAN.

WPAv1

The Wi-Fi Protected Access (WPA and WPA2) security protocols were later created to address the problems with WEP. If a weak password, such as a dictionary word or short character string is used, WPA and WPA2 can be cracked. Using a long enough random password or passphrase makes pre-shared key WPA virtually uncrack able. The second generation of the WPA security protocol (WPA2) is based

on the final IEEE802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance. With all those encryption schemes, any client in the network that knows the keys can read all the traffic.

TKIP

This stands for Temporal Key Integrity Protocol and the acronym is pronounced as tee-kip. This is part of the IEEE 802.11i standard. TKIP implements per-packet key mixing with a re-keying system and also provides a message integrity check. These avoid the problems of WEP.

LEAP

This stands for the Lightweight Extensible Authentication Protocol. This protocol is based on 802.1X and helps minimize the original security flaws by using WEP and a sophisticated key management system. This EAP-version is safer than EAP-MD5. This also uses MAC address authentication. LEAP is not secure; THC-Leap Cracker can be used to break Cisco's version of LEAP and be used against computers connected to an access point in the form of a dictionary attack. An wrap and asleep finally are other crackers capable of breaking LEAP.[20]

Restricted access networks

Solutions include a newer system for authentication, IEEE 802.1x, that promises to enhance security on both wired and wireless networks. Wireless access points that incorporate technologies like these often also have routers built in, thus becoming wireless gateways.

802.11i security

The newest and most rigorous security to implement into WLAN's today is the 802.11i RSN-standard. This full- fledged 802.11i standard however does require the newest hardware, thus potentially requiring the purchase of new equipment. This new hardware required may be either AES-WRAP or the newer and better AES-CCMP- equipment. One should make sure one needs WRAP or CCMP-equipment, as the 2 hardware standards are not compatible.

Smart cards, USB tokens, and software tokens

This is a very strong form of security. When combined with some server software, the hardware or software card or token will use its internal identity code combined with a user entered PIN to create a powerful algorithm that will very frequently generate a new encryption code. The server will be time synced to the card or token. This is a very secure way to conduct wireless transmissions. Companies in this area make USB tokens, software tokens, and smart cards. They even make hardware versions that double as an employee picture badge. Currently the safest security measures are the smart cards / USB tokens. However, these are expensive. The next safest methods are WPA2 or WPA with a RADIUS server. Any one of the three will provide a good base foundation for security. The third item on the list is to educate both employees and contractors on security risks and personal preventive measures. It is also its task to keep the company workers' knowledge base up- to-date on any new dangers that they should be cautious about. If the employees are educated, there will be a much lower chance that anyone will accidentally cause a breach in security by not locking down their laptop or bring in a wide open home access point to extend their mobile range. Employees need to be made aware that company laptop security extends to outside of their site walls as well. This includes places such as coffee houses where workers can be at their most vulnerable. The last item on the list deals with 24/7 active defines measures to ensure that the company network is secure and compliant. This can take the form of regularly looking at access point, server, and firewall logs to try to detect any unusual activity. For instance, if any large files went through an access point in the early hours of the morning, a serious investigation into the incident would be called for. There are a number of software and hardware devices that can be used to supplement the usual logs and usual other safety measures.

RF shielding

It's practical in some cases to apply specialized wall paint and window film to a room or building to significantly attenuate wireless signals, which keeps the signals from propagating outside a facility. This can significantly improve wireless security because it's difficult for hackers to receive the signals beyond the controlled area of an enterprise, such as within parking lots.[30]

Despite security measures as encryption, hackers may still be able to crack them. This is done using several techniques and tools. An overview of them can be found at the Network encryption cracking article, to understand what we are dealing with. Understanding the mind- set/techniques of the hacker allows one to better protect their system.

Mobile devices

With increasing number of mobile devices with 802.1x interfaces, security of such mobile devices becomes a concern. While open standards such as Kismet are targeted towards securing laptops, [31] access points solutions should extend towards covering mobile devices also. Host based solutions for mobile handsets and PDA's with 802.1x interface.

Security within mobile devices fall under three categories:

- Protecting against ad hoc networks
- Connecting to rogue access points Mutual authentication schemes such as WPA2 as described above
- Implementing network encryption

In order to implement 802.11i, one must first make sure both that the router/access point(s), as well as all client devices are indeed equipped to support the network encryption. If this is done, a server such as RADIUS, ADS, NDS, or LDAP needs to be integrated. This server can be a computer on the local network, an access point / router with integrated authentication server, or a remote server. AP's/routers with integrated authentication servers are often very expensive and specifically an option for commercial usage like hot spots. Hosted 802.1X servers via the Internet require a monthly fee; running a private server is free yet has the disadvantage that one must set it up and that the server needs to be on continuously.[34]

RADIUS

Remote Authentication Dial in User Service (RADIUS) is an AAA (authentication, authorization and accounting)protocol used for remote network access. RADIUS was originally proprietary but was later published under ISOC documents RFC 2138 and RFC 2139. The idea is to have an inside server act as a gatekeeper by verifying identities through a username and password that is already pre- determined by the user. A RADIUS server can also be configured to enforce user policies and restrictions as well as record accounting information such as connection time for purposes such as billing.

5. Conclusion

In this paper we have studied and analyzed various security attacks along with their impact over the systems. Inconsistencies between requirements and design models are a common problem faced by software engineers. Although the IEEE standards carry more technical details of the protocol, the fact is that the software engineers who implement the system have little or no domain knowledge in relevant fields. It is also identified that it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources.

References

1. "Network Security Tips". Cisco. Retrieved 2011- 04-19.
2. "The Hidden Downside Of Wireless Networking". Retrieved2010-10-28.
3. "How To: Define Wireless Network Security Policies". Retrieved2008-10-09.
4. "Wireless Security Primer (Part Ii)". Windowsecurity.Com. Retrieved2008-04-27.
5. "Fitting TheWlan Security Pieces Together". Pcworld.Com. Retrieved2008-10-30.
6. "Security Vulnerabilities And Risks In IndustrialUsage Of Wireless Communication". IeeeEtfa 2014 - 19th Ieee International Conference On Emerging Technology And Factory Automation. Retrieved2014-08-04.
7. "Top Reasons Why Corporate Wifi ClientsConnect To Unauthorized Networks". Infosecurity. Retrieved2010-03-22.
8. "Smac 2.0 Mac Address Changer". Klcconsulting.Com. Retrieved2008-03-17.
9. Lisa Phifer. "The Caffe Latte Attack: How It Works—And How To Block It". Wi-Fiplanet.Com. Retrieved2008-03-21.
10. "Caffé Latte With A Free Topping Of CrackedWep". Airtightnetworks.Com. Retrieved 2008-03- 21.
11. Pci Security StandardsCouncil
12. "PciDssWireless Guidelines". Retrieved 2009-07- 16.
13. "Simple Wireless Security For Home". Retrieved 2010-03-10.
14. "The Six Dumbest Ways To Secure A WirelessLan", George Ou, March 2005,Zdnet
15. "What Is A WepKey?"Lirent.Net. Retrieved 2008- 03-11.
16. “Weaknesses In The Key Scheduling Algorithm Of Rc4” By Fluhrer, Mantin AndShamir
17. "Fbi Teaches Lesson In How To Break Into Wi-Fi Networks",Informationweek.Com
18. "Analyzing The Tj Maxx Data Security Fiasco", New York State Society Of CpasPciDss1.2
19. Hacking Wireless Networks ForDummies
20. Robert Mcmillan. "Once Thought Safe, WpaWi-Fi Encryption Is Cracked". Idg. Retrieved 2008-11- 06.
21. Nate Anderson (2009). "One-Minute Wifi Crack Puts Further Pressure OnWpa". ArsTechnica. Retrieved2010-06-05.
22. Kevin Beaver, Peter T. Davis, Devin K. Akin. Hacking Wireless Networks For Dummies. Retrieved2009-02-09.
23. "Extensible authentication protocol verview". Microsoft Technet. Retrieved 2008-10- 02.
24. Joshua Bardwell; Devin Akin (2005). Cwna Official Study Guide (Third Ed.). Mcgraw-Hill. P. 435. Isbn0-07-225538-2.
25. George Ou. "Ultimate Wireless Security Guide: A Primer On Cisco Eap-Fast Authentication". Techrepublic. Archived From The Original On 2012-07-07. Retrieved2008-10-02.
26. "Wi-Fi Protected Access". Wi-Fi Alliance. Retrieved2008-02-06.
27. Wigle - Wireless Geographic Logging Engine - Stats
28. Http://Www.Airtightnetworks.Com/Wpa2-Hole196
29. "How To: Improve Wireless Security With Shielding". Retrieved2008-10-09.
30. "What Is Kismet?". Kismetwireless.Net. Retrieved 2008-02-06.
31. "End Point Wireless Security Solution Provides It Control With User Flexibility". Newsblaze.Com. Retrieved2008-03-03.
32. Khamish Malhotra, Stephen Gardner, Will Mepham. "A Novel Implementation Of Signature, Encryption And Authentication (Sea) Protocol On Mobile Patient Monitoring Devices".Ios Press. Retrieved2010-03-11.
33. Wireless Networks, Hacks And Mods For Dummies
34. Http://Netzpolitik.Org/2006/Offene-Netzwerke-Auch-Fuer-Deutschland/

