An Overview of Wireless Network Security

Alireza Kavianpour, Ph.D.
College of Engineering and Information Sciences
DeVry University
901 Corporate Center Dr. Pomona, CA. 91768-2642
akavianpour@devry.edu

Michael C Anderson, BSEET
Resource & Project Support Group
Westinghouse Electric Company
980 Waltz Mill Rd. Madison, PA. 15663
andersmc@westinghouse.com

***Abstract* - While assuming the role of Chief Security Officer, Network Security Designer, and Network Security Administrator, the intention of this research was to identify principle elements related to network security and provide an overview of potential threats, vulnerabilities, and countermeasures associated with technology designed to the IEEE 802.11 wireless LAN standard. In addition, fundamental security requirements are discussed and access control principles were included to address future trends in wireless network security.**

Index Terms* - Ad hoc networks, Network security *Wireless LAN, Wireless networks

I. Introduction

Just as technology continues to advance, devices are exceedingly trending towards mobile and wireless connectivity. This new era of technological flexibility can also provide an open invitation for network security threats not only in the corporate world, but also the privacy of users at home. Our ability to remain equally as knowledgeable and vigilant as newer technologies emerge, will have a significant impact on how we design and plan network defense strategy against unauthorized intrusions of the future.

II. Adopting Security Principles

In order to protect proprietary information, intellectual property, financial or any other private information contained within a network of a system, Confidentiality, Integrity, and Availability are three principle security control measures that should be implemented with the IEEE 802.11 standard. Including the CIA Triad method is necessary to ensure the awareness of threats and effectively manage risks. As vastly different as they may seem, there is little difference between the overall objective of wireless and wired network security. Both require resolute confidentiality with no violations to system integrity, while continuing to sustain access to information and related systems for authorized users.

III. Weighing pros and cons

At a slight additional cost wireless installation may be easier to install, however it also offers opportunities for network interference which may contributes to its overall reliability and performance. When the decision is made to transition from a physically connected architecture to wireless LAN technology, component accessibility and signal propagation provide convenient opportunities for unauthorized users to introduce malicious activities, intercept data transmission, or passively eavesdrop upon the infrastructure of a system. [2] Some of these vulnerabilities include access points, radio NIC, routers, repeaters, and antennas.

IV. Network Security Professionals

Corporations and small businesses have become savvy to the benefits of robust security platform in order to remain competitive and sustainable. Intellectual property and proprietary information is an extremely valuable asset to these companies. [5] Trusting individuals to protect their business interests is often critical and greatly impact their decision to hire or assign various network security personnel that may even include a high level executive type as a Chief Security Officer (CISO/CSO) [2] Besides approving policies specific to the network security program, many of these responsibilities include interfacing with a CIO to develop strategy and budgets, prioritize projects, make employment decisions, and even act the spokesperson when necessary. Reporting to the appointed CSO is typically a Network Security Engineer regarded as the subject matter expert on network security solutions and is able to design, implement, optimize, and troubleshoot the system and control safeguard information. Security related software and firewall installation is the responsibility to a Network Security Analyst whom also monitors the network, responds to system threats, and communicates related issues to security and management. [4] Following up on these issues to ensuring that security is properly implemented to the system design is typically the role of Certified Network Administrator.

V. Incorporating OSI Model

To adequately secure the integrity of a network, administrators require standards of the framework to implement various protocols. In order to replace TCP/IP and satisfy this prerequisite, the Open System Interconnection (OSI) model was introduced as network reference model for analyzing data communication between hardware and software in a seven layer system. [6] These seven layers of OSI model are each designated a specific protocol and unique standards they are responsible for. While performing very distinctive functions, each layer is also assigned to support the layer above and provide service to the one below it respectively. Layers 1-4 are assigned the lower layers of the protocol stacks and media layers responsible for transferring and moving data.

978-1-5090-6644-5/17 $31.00 © 2017 IEEE
DOI 10.1109/CSCloud.2017.45

Layers 5-7 are considered to be the upper host layers of the system and are associated with application level data. [7]

VI. OSI LAYERS

The Physical (Layer 1) is located at the bottom of that stack and it refers to the physical topology and components of the network associated electrical mechanical hardware required to transmit and receive communications. [8]The specific wire, line, and cable requirements such as Ethernet, Fiber-optic, RS232, T1, 802.x, RJ45, and various others make up the physical layer. The data at this layer is characterized as binary and is referred as bits as it sends likes to the layer2.

The Data Link Layer (Layer 2) is made up of the Logical Link Control (LLC) and Media Access Control (MAC) layer that was implemented by IEEE to detect and segregate the individual responsibilities carried out at this level. [8]The importance of this layer is the link system functionality provided by the LLC between the physical layer and the layers above so they can effectively communicate with each other. The MAC sublayer is responsible for providing the system with a unique identifier (MAC address) allowing the network to distinguish between computers associated across the network. [6] The Network Layer (Layer 3) handles routing independent "packets" of information from source to destination using associated IP addresses. Routers are most commonly recognized as being a component that represents this layer. These packets of data being transferred across the network can be observed and identified using software such as the WireShark applications.

The Transport Layer (Layer 4) focuses on quality of the service provided as well as providing host-to-host transportation. Additionally, these packets of information are known as "segments." Protocols associated with this layer are connection based like TCP and ACK, with the exception of UDP by which ACK isn't necessary. The Sessions Layer (Layer 5) manages and controls the connection between network applications. Protocols of this layer include NFS, SQL, and ISO session.

The Presentation Layer (Layer 6) or "Syntax layer" as it is commonly referred to provide encryption, reformats data from lower stacks to make it presentable in the application layer above it. Coding schemes such as HTML and ASCII as well as file extensions like .PNG, .JPG, and .gif are prepared at this level. The Application Layer (7) being at the top is applies to the end user interactions and processes. User authentication takes places as this level and as well as any process that is related to a user interfacing with computer applications. These activities include creating files, email, transferring documents or files, even browsing the internet. [7]

TABLE I
OSI MODEL: SEVEN LAYER ARCHITECTURE

	OSI Model : 7 Layers & Architecture			
	Assigned Layer Number	***Data units type***	***OSI model layer***	***Layer function***
Host Layers	**7**	Data	Application	• Applications interface • Interpreting program requests & info requirements.
	6	Data	Presentation	• Data compression • Data representation • Encryption.
	5	Data	Session	• Communications of interhost
Media Layers	**4**	Segments	Transport	• End-to-end connections • Properly sequence of packets
	3	Packets / datagram	Network	• Establish network connection • Translate network addresses • Transmitting individual packets across a network • Logical addressing: IP.
	2	Bit / frames	Data link	• Physical addressing
	1	Bits	Physical	• Physical network connection signal management • Binary bit transmission • Media

VII. TYPES OF SECURITY THREATS ATTACKS

Accidental Association is typically unintentional, however can happen while coinciding broadcasts between wireless access points are within close enough proximity to expose resources of a LAN to an authorized user. [11] Malicious Association is possible when a wireless device is configured to appear to a user as a legitimate access point. When the user inputs the password into the networking device the information is stolen allowing access onto the wired network via a WAP. [11]

Ad hoc networks are essentially peer-to-peer (P2P) wireless connected clients without an access point between them. This is often implemented in cases where disasters or emergency evacuation is required. They are quickly deployed and require each node connected to maintain its correct authentication list. Because there isn't a centralized access point between them for additional filtering or access control this can often be a significant threat. [11] Nontraditional networks such as Bluetooth devices and PDA's create opportunities for eavesdropping on traffic passing through the network. "Mac Spoofing" or Identity Theft as it is often referred to occur when a MAC address is able to be obtained by attackers where they make use of this information to gain access or exploit the network. [11]

Man-in-the-Middle attacks involve convincing a user they are they are communicating with one another while they are actually passing through intermediate devices that exposes them to vulnerabilities for attack. [11] Denial of Service (DoS) is meant to overwhelm a particular access point with jargon protocol messages and the resources of the wireless port are consumed. After this port is identified this information can bombard the processing and memory capabilities wearing down the resources of the port. Network Injection focuses on WAP's that openly welcome non-filtered traffic passing through the network. The object is to degrade network performance by affecting components such as routers or switches via false reconfiguration commands. [11] [12]

A Rogue Access Point is device unsanctioned by a network administrator that is functional on the network without authorization or consent. Typically this access point (AP) is an employee, intruder, or a company in the near vicinity. In some instances the SSID of the AP isn't your network identifier and its MAC address is also unlisted in the ARP tables as having permission. This could mean it was implementation by a third party and should arouse suspicion. The classifications that define a rogue AP are: Member, Neighbor, Suspect, and Rogue. Typical attacks from rogue access points include MitM, Network flooding, fake SSID broadcasting to infect other clients, DoS attacks, and even serious threats such as Wireless Bridge Frames which could lead to theft of proprietary information. In general, a rogue access point can behave as unsecure backdoor to the network. IEEE 802.1x was implemented as an authentication mechanism standard to prevent this. Countermeasures and Recommendations for Cyber Attacks While there any many efforts, techniques, and methods for improving wireless security, some of the recommendations at the top of the list include applying heavy-duty WPA2 encryption and authentication to the wireless network. The complexity of WPA2 security alone will often deter attacker to look for a more vulnerable target. [13]

In addition, understanding and gaining visibility of what is around by performing Wi-Fi scans to detect AP's that lack encryption and prevent backdoor intrusion from hackers. By Wireless Prevention Systems, around the clock Wi-Fi scanning adds additional security in the form of prevention.

Security Solution Techniques

Out of all the measures that network security personnel could integrate into the system, educating users in the workplace about the importance of wireless network security, applying best practices, as well as enforcing the usage of VPN and EAPs can greatly reduce threats and attacks. In addition restricting user access and control can also limit unauthorized users can also help secure the network and prevent damage to confidential information. [4] Encryption mechanisms are often chosen to be the standard and are often incorporated into the design of wireless routers, making them quite effective to thwart attempts of eavesdropping while saving the additional expense. [11]Additionally, once encryption keys are considered to be secure, encryption is a standard countermeasure for inserted and altering traffic passing from router-to-router. [13]

VIII. AEP ENCRYPTION BENEFITS for WPA2 (802.11i)

The Advanced Encryption Standard algorithm (AEP) and TKIP are the two standards of choices with regards to WPA2 (802.11i). WPA2 used Dynamic Session Key rotations and Automatic Key distribution. In addition it can use 802.1x and EAP for authentication purposes. The benefit of AES is more secure than TKIP which has better performance. [1]Depending on the seriousness of the threats or how the network security is design and implemented AES would be the choice to maintain a more secure network. AES also has a block cipher that replaces RC4. AP hardware has to be upgraded due to the computational complexity of this choice. 802.11i offers a significantly robust security for the future of wireless networks even though it still uses features such as Temporal Key Integrity protocol (TKIP), 802.1x, and both Key hierarchy and management both. The computational ciphers of AES offer its most effective means of security encryption. AES-based CCMP provides confidentiality, integrity and origin authentication. [1]

Limiting Computer Access to Reduce Risks

Another technique that can often be employed with general ease is limiting computer access to the wireless network. By only allowing explicit computer access to the network, this can greatly reduce access, although is generally ineffective against Identify theft considering it requires communication with an approved MAC address of the computers granted access to the network. Installing and enabling anti-virus as well as anti-spyware software in combination with a firewall on all endpoints can is another effective means to protect the network against threats.

One of the key considerations often overlooked, is changing the factory pre-set router configuration settings after it is purchased. Leaving them set to the default configuration creates the opportunity for hackers and attackers to access the manufacturing information from the devices and access the wireless devices with ease. Creating and customizing an administrative password and assigning specific login credentials is a prudent attempt to increase security and make this process significantly more difficult to penetrate. [5]

In addition, changing the default router identifier from the factory default to a new ID can also add protection. Finally, disabling broadcasting identifier (SSID) can limit the routers visibility and prevent attackers from knowing of its existence. This can also be done in conjunction with applying MAC filtering

IX. CONCLUSION

Regardless if you are a Chief Security Officer, Network Engineer, Administrator, or simply an end user at home, there is a significant possibility you will utilize wireless network technology at some point. Understanding the fundamental risks associated with network security and the possibilities that your private information could be solicited unknowingly and without your explicit permission is crucial to taking the necessary precautions and making the investment to protect yourself, your business, your assets, and even your identity from cyber attackers. Even wired connections have their own set of risks, although air transmission of presents entirely new set of opportunities for creative and talented hackers to impose their will upon a less than secure network infrastructure. We live in the age of advanced wireless technology. The need to cut the wires and be productive from a mobile environment is in high demand be end users globally and the need to advance even further is evitable. Understanding the standards and limits that apply to our technology will allow the necessary software and hardware functions and applications outlined in the OSI Model and IEEE 802.11 to keep our valuable information secure and private.

X. REFERENCES

[1] M. Solomon, "Vulnerabilities, Threats, and Attacks," in Fundamentals of Information, Clou, GlobalSine, 2006, pp. 2-7, 8-36.

[2] M. Stawowski, "The Principles of Network Security Design," The Global Voice of Information Security, pp. 29-31, 2007.

[3] AFP, "Cyber attacks a growing threat for US financial system," 20 May 2015. [Online]. Available: https://phys.org/news/2015-05-cyber-threat-financial.html. [Accessed 14 Feb 2017].

[4] S. &. D. D. Alam, "ANALYSIS OF SECURITY THREATS IN WIRELESS SENSOR NETWORK," International Journal of Wireless & Mobile Networks (IJWMN) Vol. 6, No. 2,, pp. 37-38, 40-44, April 2014.

[5] HKSAR, "WIRELESS NETWORKING SECURITY," Hong Kong, 2010.

[6] P. Simoneau, "The OSI Model: Understanding the Seven Layers of Computer Networks," 2006. [Online]. Available: http://ru6.cti.gr/bouras-old/WP_Simoneau_OSIModel.pdf. [Accessed 13 February 2017].

[7] V. Beal, "The 7 Layers of the OSI Model," 24 February 2009. [Online]. Available: http://www.webopedia.com/quick_ref/OSI_Layers.asp#OSI-6. [Accessed 11 February 2017].

[8] D. E. Capano, "Wi-Fi and OSI Model," 18 09 2014. [Online]. Available: http://www.controleng.com/single-article/wi-fi-and-the-osi-model/8b71b0494b6b7fd5291856d02e104eb4.html. [Accessed 23 01 2017].

[9] C. Hoffman, "How to Use Wireshark to Capture, Filter and Inspect Packets," 14 10 2014. [Online]. Available: https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/. [Accessed 11 02 2017].

[10] T. White, "DDoS Quick Guide," 29 Jan 2014. [Online]. Available: https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf. [Accessed 02 Feb 2017].

[11] W. L. Stallings, "Computer Security: Principles and Practice, 3rd Edition.," 07 2014. [Online]. Available: https://online.vitalsource.com/#/books/9781323080313/. [Accessed 11 02 2017].

[12] W. L. Stallengs, "Computer Security: Principles and Practice, 3rd Edition.," 07 2014. [Online]. Available: https://online.vitalsource.com/#/books/9781323080313/ . [Accessed 11 02 2017].

[13] L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends," in IEEE, Hong Kong, 2016.