MANAGING SECURITY RISKS IN WIRELESS NETWORKS

By: Michelle R. Sellers

March 22, 2016

Abstract

This is 2016 and wireless networks are an important part of the structure in nearly every business. Unfortunately they are also a large vector for attackers to compromise vulnerabilities in a system that hasn't been secured properly. This paper will discuss the inherent vulnerabilities of a wireless network and ways to manage and mitigate these risks properly.

The author will discuss the different types of vulnerabilities and threats that can put a business at risk of data loss and malicious attacks. In order to effectively secure a wireless environment, many steps need to be taken to ensure not only that the network is set up properly, but also that the network remains secure as technology adapts.

For the purposes of this paper, research has been conducted using reputable sources and has been compiled in a manner to make it easy for a technology department to understand what the concerns are and how to prevent themselves from being a victim of attack.

Table of Contents

Introduction

Wireless networks have increased in numbers and in popularity over the years. Users want the convenience of being able to access the internet from anywhere. For most businesses it's actually become more of a need than a want to have the convenience of wireless connectivity. With convenience also comes a security risk. A network that is convenient for users can also be convenient for attackers.

Although there seems to plenty of technical documentation on security risks in wireless networks, wireless networks are continuously being compromised leaving vulnerabilities that make it difficult to traverse a wireless network without knowledge of the security that lies within. With the constant change to wireless network technologies; documentation becomes outdated almost as fast as it can be made available.

Up to date research is important for security managers to adequately protect a network and manage the security risks in a wireless network. Having the knowledge needed to identify and manage risks will significantly reduce the number of vulnerabilities on a wireless network.

The purpose of this study is to identify risks in wireless networks and to explore ways to mitigate and manage those risks. By examining the current vulnerabilities that can compromise a wireless network we can better understand the potential risks and assess ways that security managers can attempt to mitigate those risks.

What is Wireless Communication?

According to Kumar and Gambir (2014), "Wireless communication is the exchange of data between two or more points that are not joined by an electrical transmitter." (p. 25). A

wireless network uses radio frequency transmissions such as electromagnetic waves for transmitting voice and data. The information transmits from sender to receiver through open space over frequency bands known as channels. There are currently 5 types of wireless communication, these are infrared, Bluetooth, Wi-Fi, radio, and cell phone. Because of the way these communicate through the open air, this makes them inherently difficult to secure and creates many avenues for attack. For the purposes of this paper we will focus mainly on the aspect of Wi-Fi environments.

WLAN Equipment

A typical home network consists of a modem, a router and wireless devices that can connect to the router. Wireless devices could be items such as laptops, tablets, cell phones, printers, gaming devices, TV's, security systems, etc. (See Figure 1.).

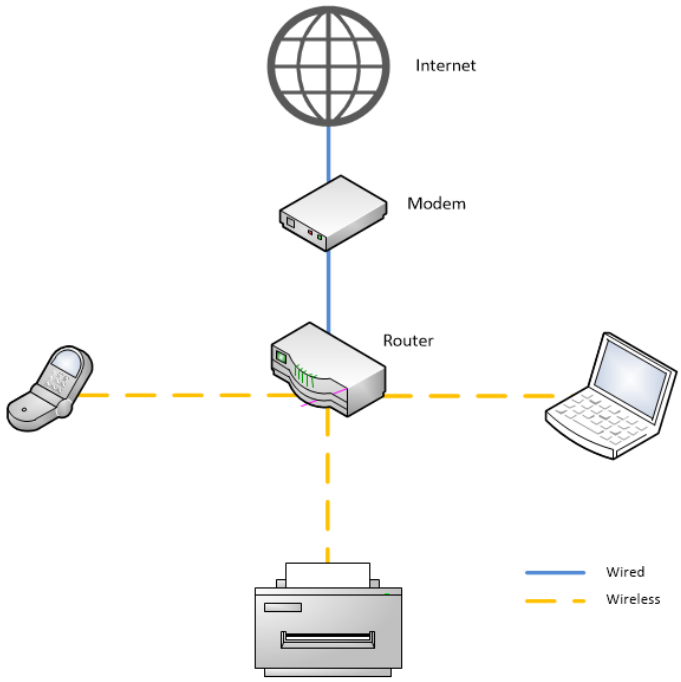

Figure 1- Example of a Home Network

A home network can appear simple, but still can have many avenues for attack. A corporate wireless network can vary and can be much more complex. Since a corporate wireless network can be much larger in size, this also increases the number of avenues for attack and can make it a security nightmare. For example, a corporate network can contain many access points, switches, hubs, repeaters, and wireless controllers, depending on the size of the campus. See Figure 2 for an example of what a small campus might look like. A wireless network could even extend to a separate campus in another location.

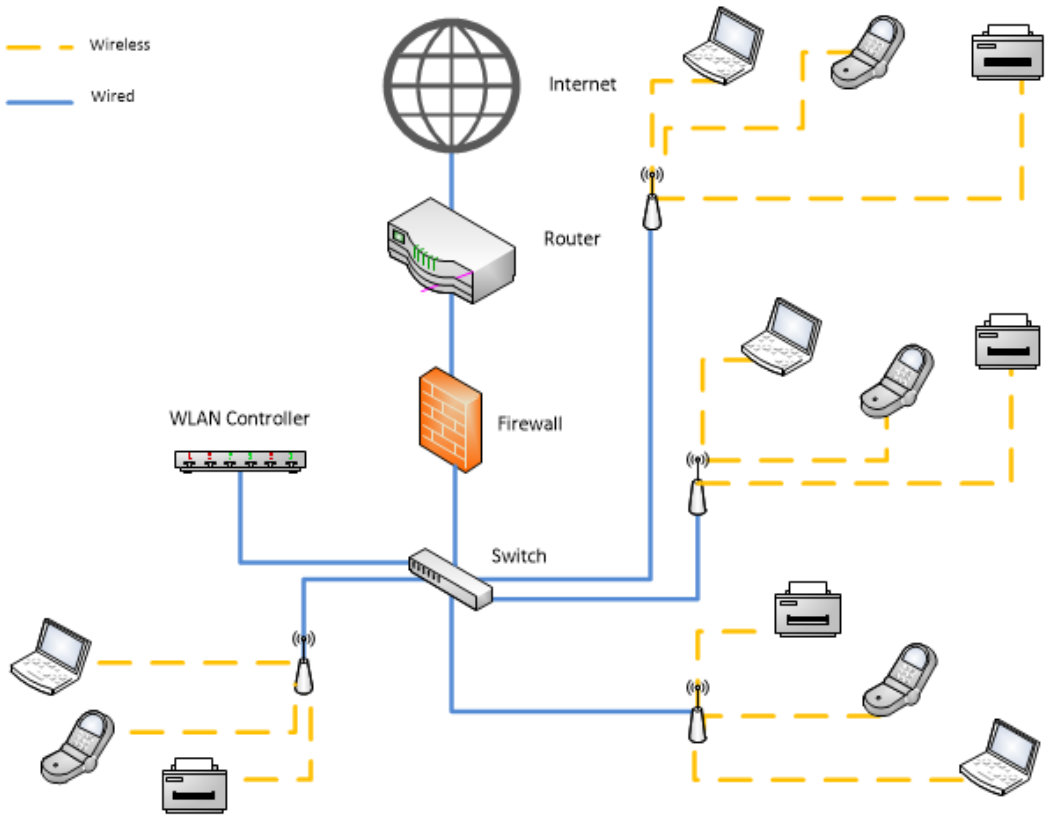

Figure 2 – Example of a Corporate WLAN

Wireless Standards

A wireless standard is a guideline that is set to standardize the frequency, range, and data rate of wireless transmissions using different applications or mode of transmission. This standard is set by IEEE, which is the Institute of Electrical and Electronics Engineers. IEEE develops the global standards for many technologies including wireless technology. The first wireless technology standard of 802.11 began in 1997. Several standards have followed since 1997 with the most recent being that of 802.11ac in 2013 and 802.11af in 2014. IEEE is working on newer standards currently which are long overdue. In my opinion, as fast as technology changes the standards should also change; RFiD Centre. (2016). [11]

Standard	Data Rate	Range	Frequency
802.11	1-2Mbps	20 feet indoors	2.4GHz RF
802.11a	Up to 54Mbps	25-75 feet indoors	5GHz
802.11b	Up to 11Mbps	Up to 150 feet indoors	2.4GHz
802.11g	Up to 54Mbps	Up to 150 feet indoors	2.4GHz
802.11n	Up to 600Mbps	175+ feet indoors	2.4GHz/5GHz

Wireless Security Protocols

There are a few different types of wireless security protocols that are available that are based on the standards provided by IEEE. Those standards are as follows:

WEP – WEP can be defined as Wireless Equivalent Privacy. WEP is a protocol defined in IEEE's 802.11 standard. When WEP initially began it was thought to be secure until a flaw was found allowing WEP to be cracked rather quickly. There were several flaws found in WEP such as its use of streaming algorithm, header vulnerabilities, it lacked authentication, and more. WEP is still used, but isn't a preferred security method due to its vulnerabilities; Ijeh, A. et al (2009). [3]

WPA – WPA is known as the Wi-Fi Protected Access protocol. WPA is basically a re-engineered version of WEP. To make WPA more secure than WEP several changes needed to be made. Authentication was added, the header was protected, it uses TKIP (Temporal Key Integrity Protocol) instead of AES, and it uses a non-linear algorithm. TKIP ended up not being a secure enough form of encryption, so WPA2 was developed to replace WPA; Ijeh, A. et al (2009). [3]

WPA2 – WPA2 is similar to the WPA protocol. WPA2 made the transition to using AES encryption, and it included an enhanced integrity check. WPA2 is currently the most secure protocol to use. WPA2 can be used with either the AES, TKIP, or mixed mode (AES/TKIP) options; Ijeh, A. et al (2009). [3]

Literature Review

Like most information in the field of technology, wireless information gets outdated and needs to be maintained to stay accurate. Articles that were written within the last year could already be outdated and difficult to use to secure a network in its entirety. The following literature is an attempt at the most recent updates in wireless security.

Ethical and Legal Concerns

Houston, Reams, and Zelinsky (N.D.) discuss a few of the ethical aspects involved in wireless networks. [1] Though this is not a complete list of ethical dilemmas that can arise by the use of a wireless network, it does pose some great ideas in who should be responsible for the security of wireless networks.

Security Concerns

Zaman, Ahmad, Azhar, Nawaz, Abbas, and Idrees (2014) discuss several types of vulnerabilities and threats that should be considered when configuring wireless networks. [2] There are many types of security risks possible in a wireless network, it's important to stay up to date on the most recent vulnerabilities and threats.

Kumar and Gambhir (2014) discuss the different types of security attacks and security protocols. [5] Knowing the types of attacks that can occur on a network is one of the best ways to mitigate risks.

Policies and Procedures

Ijeh, Brimicombe, Preston, and Imafidon (2009) examined the different types of protocols for wireless security and completed a study to determine how the location of the data that gets transmitted could be restricted in order to increase security on a wireless network. [3] The authors outline several security challenges that should be considered in the wireless network development process.

Mandeville (N.D.) has completed documentation for creating a security plan for wireless networks. He lays out options for security plans with different protocols that could help to secure a wireless network.

Sans (2014) has created a generic wireless communication policy that can be modified for use by anyone in the internet community. [6] Policies are great for having a guideline to go by when securing a network. There is an inherent flaw in using a template though, it's important to make sure it fits your network.

Monitoring

Waliullah, Moniruzzaman, and Rahman (2015) conduct an experimental analysis to study well know attacks and discuss ways to monitor and mitigate those attacks. [4]

Cai (2014) investigates different methods of monitoring wireless network technologies such as WiFi Networks, Cellular Networks, and Wireless Sensor Networks.

Literary Improvements

This study will provide literary improvements with updated wireless security information. We will add to existing literature with updated information on vulnerabilities, current threat information, and ways to manage risk.

Research Method

For the purposes of this study, I will be conducting up to date research from reputable sources, I will point out possible security issues involved in wireless networks, and will suggest using several different security methods that could help to improve any possible security vulnerabilities.

Results

For the purposes of this study, I have gathered important information from reputable sources through online journals, from professional sources in the network security field, and through my own prior knowledge and experience.

First I will list the different types of wireless vulnerabilities and threats; I will then follow with important information and suggestions for how to mitigate these possible issues before they have a chance to compromise a wireless network.

Wireless Vulnerabilities

Wireless vulnerabilities exist if there is a design flaw or a weakness that can be exploited by an attacker or a threat. A few possible wireless vulnerabilities are listed below.

Bluetooth Attacks – There are ways an attacker can access mobile devices through Bluetooth and create problems like DoS. Attackers can take advantage of an open Bluetooth port and insert infected code into a user's system without their knowledge. This has recently been known to happen to users who own a FitBit device. FitBit connects to a user's computer via Bluetooth. Since this port was left open waiting for a connection to FitBit devices, attackers injected code that would infect a computer or create a backdoor in.

Attackers can also take advantage of Bluetooth devices such as cellphones. As long as the Bluetooth is enabled, an attacker can find means to connect to it and steal pictures or private data. These types of attacks have many names, but are commonly known as Bluesnarfing, Bluejacking, and Bluebugging.

Lost and Stolen Devices – Though this isn't technically considered a vulnerability to wireless networks, if an attacker were able to get ahold of a device that has already gained access to the network, they would be able to take advantage of this and access the network themselves. Millions of devices are lost or stolen each year, which can increase the likelihood of an attacker gaining access by these means. Once an attacker has access to a device they would be able to access/steal data, inject malicious code, create a backdoor, access email, access applications with stored passwords, or access applications that don't require authentication when on the network.

Parking Lot Attack – If a wireless network extends outside the perimeter of buildings, attackers can sit on the outskirts of a company network and gain access to the wireless network. An attacker will try several means in order to attempt to get into a network, including attempts at listening to traffic, scraping data for passwords, retrieving access point information, or creating a fake access point. All of this can be done without the user's knowledge and from a safe distance.

Once an attacker is able to find a user to connect to, they are able to create dialogues that pop up that request a password and the user unknowingly gives the password to the attacker. Now the attacker has an authenticated means of access the network and can do and access anything that the user can do.

Rogue Access Points – An attacker can easily set up a rogue device if there is access to network jacks. Rogue access can also be easily setup by an uneducated user within their department or area. If an attacker gains access to a rogue device whether they set it up themselves, or it was by a user, it could be an open door to the network. Access to a rogue device could give an attacker the means to getting the necessary credentials to log into the legitimate access points on the network. Once into the network the attacker would be able to attempt to further access systems and devices.

Shared Key Authentication – A shared key authentication attack is when the attacker is able to access the challenge and the response that happens between the access point and the authenticated device. Once the attacker has this information, they are then themselves able to act as the authenticated device.

SSID Search – An attacker is able to obtain an SSID by capturing network traffic. Once they find this information they are able to access the network using other means and get to areas that were not intended for generic users.

Unsecured Access – Unsecured access to a wireless network is a common vulnerability. Unfortunately many wireless routers and access points are shipped from the factory with default credentials. If an attacker knows the default information, they are able to easily access a router or access point.

WEP Attacks – WEP is not a secure protocol to use when setting up a wireless network and causes vulnerabilities in a WLAN whether it is in use or not. These types of attacks can be used to modify data, decrypt traffic, and access unauthorized areas.

Wireless Threats

Wireless threats can be considered as the means to which an attacker can make use of one of the above vulnerabilities. Threats on a wireless network can be anything from just someone seeing if they can get in, to someone wanting in to cause malicious harm to the network. There's no way of knowing what an intruder intends to do, so it's best to avoid access altogether. Some possible threats are listed below.

Denial of Service – This type of attack can happen to either a wired or a wireless network. The attacker floods the network with requests that make it difficult for the server to handle and authorized users are unable to gain access; Kumar, U. et al (2014). [5]

Dictionary Attacks – This can be done on a wireless or a wired network. The attacker goes through passwords one by one trying to find a password that works; Kumar, U. et al (2014). [5]

Eavesdropping – This is when an attacker injects messages into wireless traffic so that when the messages are decrypted he is able to figure out the key. The attacker will then be able to decrypt all of the messages; Kumar, U. et al (2014). [5]

IP Spoofing – This type of attack requires the attacker to hide their own IP address and use a known good IP address to gain access by impersonation.

Malicious Code – Using wireless protocols virus threats and Trojans are able to spread through smartphones.

Man in the Middle Attack – The attacker creates dummy AP's then lets the user authenticate. With the AP in the middle of the connection the attacker is able to see the information that passes through the connection. ; Kumar, U. et al (2014). [5]

Traffic Analysis – The attacker gathers necessary information from the network in order acquire enough information to access the network; Kumar, U. et al (2014). [5]

Wardriving – The attacker searches for Wi-Fi signals in a moving vehicle.

Ways to secure

Securing a wireless network is a thought out process. All possible avenues of threat need to be considered so that one area is secure while an attacker just finds another way in. Many companies thought their network was secure, until information became compromised and leaked to the public.

Vendor Audit

The best way to secure a network is to think like an attacker. To find out just how secure your network is, it would be a great idea to have a wireless audit completed by an outside vendor. There are many advantages to using a vendor such as the thoroughness of the evaluation, a vendor may find things that were overlooked internally, using a vendor wouldn't tie up already busy employees, a vendor may have access to more resources and tools to do the job, a vendor would be able to get the job completed quicker, and since it would be the vendors specialty; they would be more knowledgeable in the field. The disadvantage of using a vendor is that it's expensive and can be difficult to get management buy-in.

When a vendor does an audit, they will attempt to compromise the network in ways that an attacker would; which is sometimes known as ethical hacking. The vendor will use several different methods to ethically hack a network and to check for vulnerabilities, such as:

- Password cracking attempts
- Site survey/Heat map
- SSID Search
- Search for Bluetooth connections
- Search for rogue devices
- Discuss policies and procedures

When the vendor is finished with the audit, they will give a summary of findings to outline any vulnerabilities that were found and offer suggestions to remediate the vulnerabilities. Hiring an auditor can be cost prohibitive for some companies, and it can sometimes be difficult to get approval for such an expense. In that case, there are steps that can be taken to make sure a network is secure without the use of an auditor.

Steps to Secure the End User

A large portion of security vulnerabilities on a wireless network can be prevented by securing the end user. Below are items to consider for mitigating end-user security weaknesses.

Policies – Enforcing policies for mobile devices, passwords, and acceptable use can help to create a secure environment in many ways. These policies not only need to be created, but they also need to be updated regularly and made easily available for users.

Security Training – Provide security training to end users on an ongoing basis, in an attempt to keep security in the forefront of their minds. Outside vendors can be used for this at a fairly reasonable cost. Users can benefit from this type of training not only at work, but also at home, so many users like to be involved in this type of training.

Secure Bluetooth Devices – Users should be educated on the use of Bluetooth devices and how to secure Bluetooth devices. Bluetooth devices; including printers, should have Bluetooth turned off when not in use.

Rogue Devices – Inform users about rogue devices and that these devices can cause a security issue and should not be installed. Attackers can access these devices if proper security protocols haven't been put into place by the untrained user.

Lost and Stolen devices – If users are to use a call phone or a laptop on a company network, they will need to adhere to a mobile device policy. This policy should outline device security and the procedure for lost and stolen devices.

Device security should include:

- Software installed by the company to locate the device or disable it.
- Passcode/password security to lock the device.
- There should not be any confidential data stored on a mobile device.

Lost device procedure should include items such as:

- Who to notify in the event that an item is lost or stolen.

Steps to Securing the Structure

Standards Policy – A technology department should have a set of wireless standards that all employees in the department can adhere to. This will help to assure that a secure wireless network remains secure. If an access point goes down, any employee in the department should be able to properly configure the new device to match existing devices. These types of items should be outlined in the wireless standards for a department.

- **Protocol Use** – This policy should include the mandatory use of WPA2 protocol rather than WEP or WPA which are less secure and could provide avenues of attack.
- **Hidden SSID's -** To prevent an attacker from finding your SSID, you will have to keep the SSID hidden by not broadcasting it. There are programs out there that will still help an attacker find hidden SSID's, so it's best not to give too many identifiers in the SSID even though it's hidden. You wouldn't want to name your accounting departments private SSID "ACCOUNTING" because this would make it too easy for the attacker if that's what they are attempting to gain access to.
- **Secure Devices** – Access points should be physically hidden from sight to make it more difficult for attackers to know what types of devices they are dealing with. Also, to prevent unsecured access it's important to make sure default passwords on all devices are changed. Attackers will attempt to use known default passwords in hopes of gaining access to the network. Once inside the network, they are potentially able to access secure information and change security criteria.
- **Perimeter Security** – Parking lot attacks and wardriving attacks can be reduced with proper planning when creating a wireless network. By making sure the

wireless access points don't bleed signal outside of the perimeter, attacks can be significantly reduced. To do this you may need to control the RF footprint of your network by using directional antennas and reducing power levels to a level that could still work for users within the buildings or boundaries. There are also methods that can be used such as shielding paint and window film that help to prevent signal from leaking outside of the perimeter.

Prevent Rogue Access Points – To prevent an attack with the use of a rogue device, it's important to make sure there are none on the network. This is difficult to do unless you have a dedicated wireless security person monitoring the network. Wireless controller management software can sometimes set a standard for rogue devices and a policy of when the device goes from just being on alert to needing to be contained. Containing a rogue device can lead to legal ramifications and should only be handled by a trained professional. Another safeguard against rogue devices is to use static IP addressing. If a rogue device is plugged into an empty data jack, it won't be able to acquire a dynamic IP address.

Enforced Policies – Dictionary attacks can be prevented with the use of strong passwords and an enforced password policy. It's much more difficult for an attacker to gain access using a dictionary attack if the passwords are longer, use special characters, numbers, and avoid using proper names or words that may actually be found in a dictionary. This makes it more difficult, but it doesn't make an attack impossible. The enforced password policy should also force users to change their passwords on a regular basis.

Encryption – Eavesdropping is a difficult threat to prevent without locking down the network so tight that even authorized users can't access it. The only way to really prevent eavesdropping is

to change the encryption key often, so that the attacker is unable to decrypt the messages that come through.

WIDS – Consider using a wireless intrusion detection system. Wireless intrusion detection systems can protect a company from nearly all vulnerabilities or attacks, but they can be quite expensive and difficult to maintain.

Antivirus – Install antivirus on wireless devices. If somehow a device suffers an attack of malicious code/software, the antivirus should help to notify the user that an attack has happened and give the user an idea of what they need to do, or it could remove the virus before it wreaks havoc on the network.

Recommendations

Securing a wireless network is not a weekend project. This is a task that requires a lot of planning. The planning starts long before the network is even powered up and should continue on indefinitely. This paper is in no way considered to be an exhaustive list of the only wireless security issues to consider. With changes in technology, also come new security issues and threats.

Following a few recommendations from this paper will help to steer a wireless security network in the right direction.

Here is a summary of recommendations to follow to do just that.

1. Create and put policies in place such as:
    - BYOD/MDM Policy - Policy should include:
        a. Device security requirements
        b. Lost or stolen device procedure
        c. Signed agreement annually
    - Wireless/Acceptable Use Policy – Policy should include:
        a. Signed agreement annually
        b. Users agree to monitoring
        c. Users agree to use the network for work use only
    - Password Policy
        a. Outline password length and complexity requirements
        b. Passwords changed at least every 3 months

2. User training should be conducted monthly as a requirement for continued wireless access.
    a. Training should be verified by the training department
    b. Training should include email security, wireless security, password security, and internet security
3. Wireless audits should be completed either internally or by a vendor. This should be completed quarterly to make sure the network hasn't been compromised since the last audit.
4. Create a standard for configuration and management of devices on the network in order to give the technology department a standard to go by in the event anything on the network needs changed or added.
5. Implement a change management system to track changes that have been made in case a security event occurs.
6. Install and maintain network level antivirus on all devices.
    a. Logs should be monitored daily for viruses.
    b. Virus definitions should be updated weekly.
    c. Virus scans should be performed weekly.

References

[1] Houston, N., Reams, D., and Zelinsky, N. (N.D.) *The Ethical Issues Surrounding Wi-Fi.* Retrieved from http://ethicapublishing.com/ethical/3CH10.pdf

[2] Zaman, M., Ahmad, J., Azhar, M., Nawaz, A., Abbas, S., and Idrees, U. (2014). Implementation of Some Enhancements in Wireless Network Security by Finding Vulnerabilities, Threats, and Attacks. *Journal of Global Innovations in Agricultural and Social Sciences.* DOI: 10.17957/JGIASS/2.3.597

[3] Ijeh, A., Brimicombe, A., Preston, D., Imafidon, O. (2009). Security Measures in Wired and Wireless Networks. Retrieved from http://www.bcs.org/upload/pdf/ewic_iict09_s4paper2.pdf.

[4] Waliullah, Moniruzzaman, B.M., & Rahman, S. (2015). An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network. *International Journal of Future Generation Communication and Networking Vol. 8, No. 1.* Retrieved from http://www.sersc.org/journals/IJFGCN/vol8_no1/2.pdf

[5] Kumar, U., and Gamhir, S. (2014). A Literature Review of Security Threats to Wireless Networks. *International Journal of Future Generation Communication and Networking.* Vol.7, No.4 (2014), pp.25-34 http://dx.doi.org/10.14257/ijfgcn.2014.7.4.03

[6] SANS (2014). Wireless Communication Policy. *Consensus Policy Resource Community.* Retrieved from https://www.sans.org/security-resources/policies/network-security/pdf/wireless-communication-policy

[7] Mandeville, S. (N.D.). Methodology: Security plan for wireless networks. *Hackerville Scientific Research.* Retrieved from https://www.exploit-db.com/docs/31170.pdf

[8] Cai, Y. (2014). Network Monitoring and Data Analysis in Wireless Networks. Retrieved from http://www.gc.cuny.edu/CUNY_GC/media/Computer-Science/Student%20Presentations/Yongje%20Cai/Yongjie_Cai_ThesisProposal.pdf

[9] Farrington, D. (2016). Enterprise Wireless Audit Checklist. Retrieved from https://www.sans.org/media/score/checklists/EnterpriseWirelessNetworkAudit.pdf

[10] Anderson, M. (2015). FitBit's open Bluetooth port enables rapid 'viral' malware infection. *The Stack.* Retrieved from https://thestack.com/security/2015/10/21/fitbits-open-bluetooth-port-enables-rapid-viral-malware-infection/

[11] Author Unknown. (2016). Wireless Standards. *RFiD Centre.* Retrieved from http://www.rfidc.com/docs/introductiontowireless_standards.htm