Legislation Vulnerabilities, Threats and Counter Measures in Wireless Network Security

Kushagra Dhingra*
Ankit Verma**

Abstract

Wireless network deliver us numerous advantages, but it also sprinkle up with new security risks and modify overall information security threats profile. Although accomplishment of technological results is the usual reply to wireless security risks and vulnerabilities, wireless security is initially a management outcome. We comes out with a framework to help to conclude and assess different risks running mate with the use of wireless technology. We also comes out with enumerated solutions for combat those threats or risks.

Keywords: Wireless Network, Wireless Security, Wireless Threats, Signal-Hiding

Introduction

A **wireless network** is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method through which we can connect Home (Telecommunication Network) and Enterprise (Business) networks. With the help of wireless network installations in these areas, we can avoid the coastally process of introducing cables into a building, or as connections between various equipment locations. Wireless telecommunications networks are generally implemented and administered using "Radio Communication". This implementation takes place at the physical level (layer) of the "OSI model" network structure. Examples of wireless networks include cell phone networks, Wi-Fi local networks and terrestrial microwave networks. Wireless networking presents many advantages to improve productivity because of increased accessibility to information resources, Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile.[3] For example, as wireless network communications takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If we not encrypt the message, or message is encrypted with a weak algorithm, the attacker can easily attack and read it, it means we are compromising with our confidentiality. Although wireless networking is not secure but it alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems. The objective of this paper is to assist in making such decisions by providing them with a basic understanding of the nature of the various threats associated with wireless networking and available countermeasures. To test the performance of wireless network, we consider some bases such as their convenience, cost efficiency, and ease of integration with other networks and network components. In today's world majority of computers sold to consumers with pre-equipped with all necessary wireless Networks technology. The benefits of wireless Networks include: Convenience, Mobility, Productivity, Deployment, Expandability and Cost. Wireless Network technology, is absolutely same with the advantages and conveniences described above has its share of downfalls. For a given networking situation, wireless Networks may not be desirable for a number of reasons. Most of these reasons occur because of the limitations of the technology. The disadvantages of

Kushagra Dhingra*
Student of BCA
IITM, Janakpuri, New Delhi

Ankit Verma**
Assistant Professor
IITM, Janakpuri, New Delhi

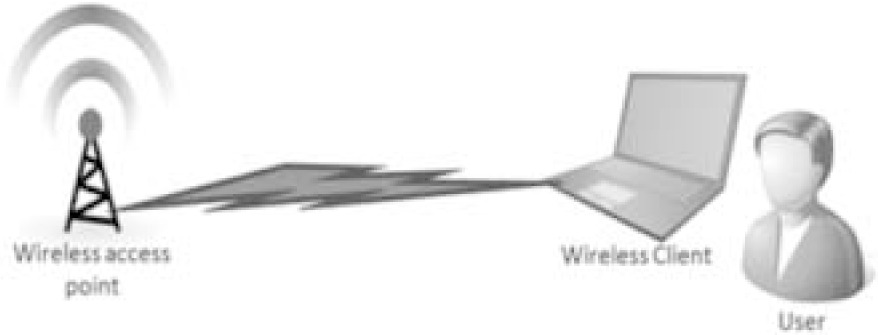

Figure 1. Wireless networking components.

using a wireless network are: Security, Range, Reliability, and Speed. A host of issues for network managers presented by wireless network. Unauthorized access points, broadcasted SSIDs (*service set identifier)*, unknown stations, and spoofed MAC (media access control) addresses are just a few of the problems addressed in WLAN (*wireless local area network)* troubleshooting. Most network analysis vendors, such as Network Instruments, Network General, and Fluke, offer WLAN troubleshooting tools or functionalities as part of their product line.

Wireless Vulnerabilities

For connecting wireless networks we have to consider of four basic components: The transmission of data using radio frequencies; Access points that provide a connection to the organizational network and/or the Client devices (laptops, PDAs, etc.); and Users. Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability.

Wireless Network Attacks

Accidental association. Unauthorized access to company wireless and wired networks 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.[3] 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.

Malevolent Association. There are different intents and methods to access any organization's wireless or

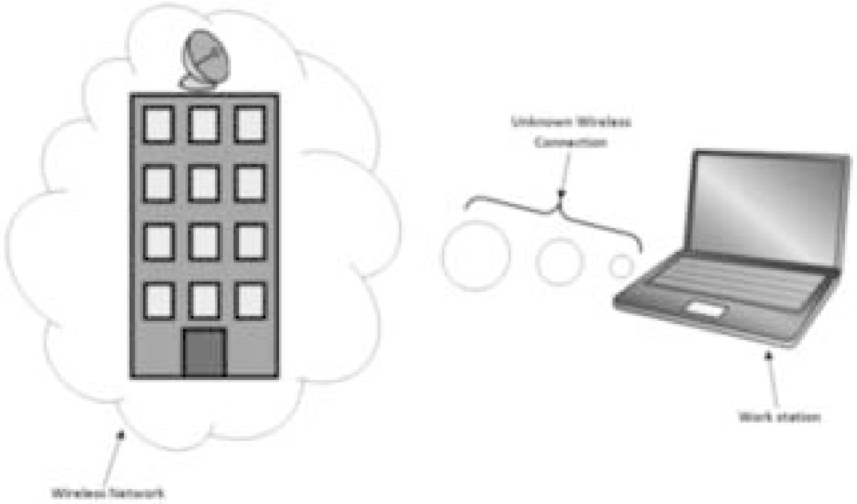

Figure 2. Malevolent Association

wired network which is unauthorized. "Malicious association" is the one of these methods. For example:- if a user switch ones his computer and if there is a wireless access point nearby and if it's computer catches with that wireless access point, even he don't know that his system is connected to that wireless network. However, it is a vulnerable situation for the company, as their security is broken and their information is in endangered (one company can make a link to other and can style information). This vulnerability can also with the case if there is a wired network example: if the system is hooked to cables.[2]

Virulent Association. It is also known as "Malicious association". This association are when crackers actively make a connection (through wireless device, a wireless Connection) to a running network through their hardware cracking device (like laptop) instead of that's network's AP (Access Point). Hardware devices which are used here are known as "soft APs". Cracker develop these network by running some software which help to look lawful Access Point that wireless network which is developed to attack. Once if he/she (cracker) gets access he/she can thieve the password, he/she can attack te wired or wireless network. There are some security authentication such as in level 3 and VPNs, and as we know wireless network is at layer 2 level. The wireless 802.1 x authentications is a kind of protection but it is still vulnerable and can be cracked. But attacker's idea is not to break VPNs or any other security measures. Crackers misty take over the client at layer 2 level.

Computer to Computer Network. It is also known as ("Ad-hoc network "). It acts as a security hazard this type of networks is defined as peer- to -a peer network which is work within the wireless computers which doesn't have any access point in between. Protection is less with these types of networks, for providing security we can use encryption method.

Non-Heritage Network. We can also call it "non-traditional network". These types of networks such as Private Network Bluetooth devices. These types of networks are not safe and can easily crack by crackers and should be estimated as a security hazard. Some non-heritage networks such as wireless printers, barcode reader, copiers should be secured. These type of networks can easily be outlook by an IT Personnel who have slender axis on laptops and AP's.

Injecting Networks. An attack which is known as Injecting Network (also known as "Man-in-the-middle" attack) , in this AP(Access Point) is used by an attacker that are endangered with the network traffic which is not fettered, "Spanning Tree" (802.D), RIP,HSRP & OSPF are especial broadcasting network traffic. Attackers injects true networking re-framing the commands that can attack (or affect) switches , intelligent hubs and routers , rebooting or reprogramming the network is done for the intelligent networking device.[7]

DOS Attack. This attack is known as denial-of-service attack. This attack takes place when a cracker (or attacker) ceaselessly assaulting a targeted access point(AP) or network with artificial requests, getting early messages of thriving connections, messages of failure, and many other commands . This scenario can affect legitimate (or true) users not able to get connected with network and even effects network failure or crash of the network. Abuse of protocols like EAP (Extensible Authentication Protocol) is the thing on which attack depends on.

Wireless Transmission Security

Interception, disruption & alternation are three basic threats which are created by the nature of wireless communication.

Securing the Confidentiality of Wireless Transmissions

There are couples of countermeasures which exist for decreasing the threats of eavesdropping on wireless transmissions. The first approach involves for materialize it more hellacious to discover and interrupt the wireless signals. The second approach involves the application of encryption to secure the confidentiality even if the wireless signal is interrupted.[8]

Techniques of Hiding-Signals. Initially attackers need to identify & discover wireless networks and then intercept the wireless transmissions. So user can follow a number of steps to make it more hellacious to discover their wireless access point. It is totally dependent upon user that which method the user should use. If the user needs signal hiding in easiest & least costly technique he should perform the following ambulate: Turning off the service set identifier (SSID), provide mystic names to SSIDs, degrade signal strength to the level where only the user is able to use or locating wireless access points in the interior of the building, away from windows & exterior walls. More potent, but also more costly methods for dominating or shielding signals include: Using directional antennas to constrain signal emanations within specific areas of coverage. Sometimes, TEMPEST is referred as using of directional emanation of wireless signals.

Encryption. Encrypting all wireless traffic is the best technique for securing the confidentiality of transmits data over wireless networks. This is essentially meaningful for users subject to bylaw.

Head off modifications of Interrupted Communications:

Interruption & modification of wireless transmission shows of form of "man-in-the middle" attack. Strong encryption & strong authentication are the two types of countermeasure can revelatory decreases the threads of such attacks for both devices & users.

Risk of DOS Attacks can be reduced with following Countermeasure:

Denial-of-service also endangers to wireless communication. For reducing the risk of such unintentional DOS attacks organization can take several steps. One of the measure to identify location where signals from other devices exist by regulating careful site surveys; while locating wireless access points the backwash of such surveys should be used. Regular steady scrutiny of wireless networking activity & performance can identify knot areas; appropriate of the outraging devices or measure to signal vigor & scope within the knot areas.

Wireless Networks Security

WAP Security

Unsecured, deficient construction of WAP can leads us to compromise with some importance or confidentiality by permitting accessibility to some unauthorized one to the network.

Counteragent for Security WAP

We can downgrade the threats of unknown/unwanted access to wireless networks by the help of follow three steps:

1. Exclude duplicitous access port
2. Protected architecture of authorized access point.
3. Application 802.1 x to authenticate all devices.

Exclude Duplicitous Access Point. The finery way for reducing the risks/threats of duplicitous access point is application 802.1x to authenticating all devices which are connection into a wired network application 802.1x will anticipate any underpowered devices from hooked to the network.[5]

Protected Architecture of Authorized Access Point. It should be assure that each and every authorized WAP's (wireless access points) are securely configured. Attackers can easily attack to AP (access point) with default setting because they are renowned by attackers so these settings are specifically to be changed.[4]

Assuring Wireless Client Devices

There are couples of major risks to wireless client devices are:

1. Mislay or steal 2. Compromise

Mislay or stealing of some hardware or storing devices like laptops or PD's is a grave matter these hardware or storage devices can stored information which is highly confidential. Evenly mislay or stealing of these hardware devices can lead to reveals the information parties. Second risk to this is that they can compromised. This compromising makes information sensitive to be attacked and access to distinct system resources (which is unauthorized to access).

Application Encryption

Encryption is the most secured way for transferring any information on wireless network. Some of the devices like access points, wireless routes, and base stations have encryption mechanism in-built in them. If you don't have the wireless router it is preferable to get which does have it. Manufacturers make the encrypted feature of wireless routers turned off. It is suggested to turn on it.[1]

Application Anti-Spyware and Anti-Virus Software and a Firewall

As we give protections to the computers which are connected with the internet. This same type of protection system is needed for the computers that are installed and maintained them up to the date.

Switched Off Identifier Spread

Identifier spread is a mechanism which is used by max wireless routers. This mechanism is use to transmit signals to any device in the proximity enunciate it presence. If any device preliminarily known & connected to network then there is no need to spread or broadcast the information. With the use of identifier spread, attackers can easily attack and expose wireless network. It is suggested that switches off the identifier spread mechanism if wireless router permit is.

Alter the Default Identifier for Your Router

Your router likely have a standard identifier, manufactures provides default ID to all devices of that model. It doesn't matter that your router not broadcasting its identifier to all, attackers can try to access your network as he know the default ID's. You should change and uniquely identify your identifier and don't forget to provide the same ID to your computer and your wireless router so they can interface among them. It is suggested that your password should be long at least of 10 characters: As longer is you password, is become most difficult to be break by the attackers.

Permit Only Specific Devices that Access Your Wireless network

Each and every device provides its own unique MAC (Media Access Control) Address for communicating with a network. A mechanism is included with wireless router that permits only devices that have specific MAC address which can access the network. MAC address can be imitate by the attackers, so do not rely on this pad only.

When you are Not Using Wireless Network Make Turn off It

Turn off wireless router can't be access by the attackers. If you are timely turn off the wireless router ("when you are not using it"), then you are decreasing the vulnerability to be hacked.[2]

Public "HOT SPOTS" are not secured

If you are thinking that wireless public Hot Spots are secured, then your thinking is wrong, these are not secured.

Educate & Train Users

Training & educating will help users to be aware about the securing of wireless networking. To make it effective, the user training &educating process is needed to be repeated periodically. The major part of WLAN policy of security is wireless network inspecting. For decreasing the baddie hardware, network needs to inspect on the daily bases.[6] This method performs scanning & mapping processes for each & every WLAN nodes and access point of network. After it, previously mapped network is compared with this. Wavelan-tool which is usually is use. Airsnort is a specialized tool used for auditing the network for asthenic keys.

Conclusion

Wireless networking furnishes many opening the accrual of productivity in declivity of costs. Collectively (using wireless network) computer security risk profile is altered. Totally elimination of risks is impossible even with wireless networking, but it is possible to attain a consequent level of collectively securing the network by embracing systematic approach for managing risks. In this paper we discussed about the vulnerabilities & risks hooked up with three wireless networking technical components such as transmission medium, AP (Access points) and client, and describe varied of common methods for decreasing risks. It evenly suggests to educate and give training to users about the safety of wireless networking operations.

References

1. Graham, E., Steinbart, P.J. (2006) Wireless Security
2. Cisco. (2004). Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, July 19.
3. CSI. (2004). CSI/FBI Computer Crime and Security Survey.
4. Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.
5. Kelley, D. (2003). The X factor: 802.1x may be just what you need to stop intruders from accessing your network. Information Security, 6(8), 60-69.
6. Kennedy, S. (2004). Best practices for wireless network security. Information Systems Control Journal (3).
7. Nokia. (2003). Man-in-the-middle attacks in tunneled authentication protocols.
8. Paladugu, V., Cherukuru, N., & Pandula, S. (2001). Comparison of security protocols for wireless communications.