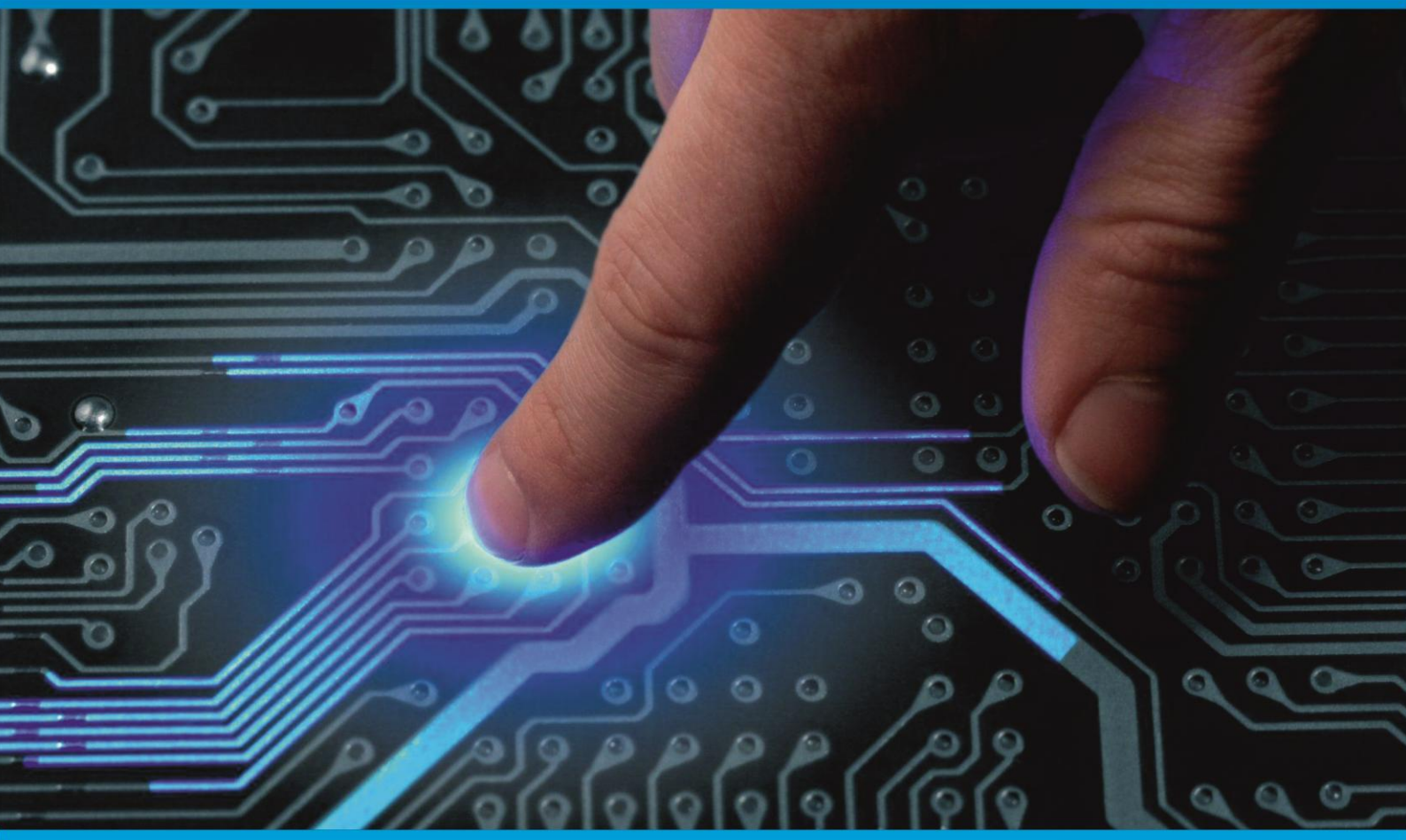
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 12, December 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 8, Issue 12, December 2020 ||

| DOI: 10.15680/IJIRCCE.2020.0812026 |

A Study on Wireless Network Security

Jagruti Vanjari, Rama S. Bansode

P.G Student, Department of Master in Computer Application, Modern College of Engineering, Shivaji Nagar, Pune, Maharashtra, India

Associate Professor, Department of Master in Computer Application, Modern College of Engineering, Shivaji Nagar, Pune, Maharashtra, India

ABSTRACT: Wireless network technology is frequently used in network technology. Several variants are available based on traditional wireless networking such as WSN, WMN, MANET, etc. In all the variants of wireless networks routing plays an essential role. Additionally, the attackers are mainly targeting the routing strategies for performing malicious activities. To secure the wireless ad hoc network a new kind of security system is proposed in this presented paper. Additionally able to improve the performance of the network in normal conditions as well as under attack conditions. The given paper includes the proposed system design and the concept that is helping to support the proposed security infrastructure.

I. INTRODUCTION

Wireless security is the prevention of unauthorized access to computers or data using wireless networks. Unauthorized access includes Wi-Fi networks. The most common type is **Wi-Fi security**, which includes Wired 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 not only basic laptop computers but also widely available software tools.

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

II. LITERATURE REVIEW

A secure and reliable network certainly enhances the day to day business of the organization. It also enhances the customer's confidence as a result in the case of web network. The most noteworthy breaches of the network are from within in the organization. The case of cyber-attack can result in severe and unrepeatable damage to the complete organization. So, Network security is important irrespective of the size /business of the network. Hence, It's important for small and large scale networks. Therefore, in the case of a cyber-attack when Connected to the internet all data may be lost in a second and this may result in misleading information on the network. Hence, Denial of the secure network may result in an unexpected loss to the organization that may lead to a huge disaster.

Importance Of Network Security For An Organization/Country:

Any organization the importance of the network cannot be denied. Besides this, so companies may lose their reputation, money, and assets in case of any negligence in the security of the network and Network security will ensure the availability of reliable and secure information for an organization or country. So network security breaches can cause countries/organizations to lose huge in terms of money. The reliability of information is important to ensure network security. Therefore, any information on the network is considered as an asset of the company but Organizations that deliver the services to meet the requirements and needs of their customers or end-users must protect their network. Hence, the response and preparation of an organization can be categorized into three major actions:

1. Protection of network: Complete network is configured and connected in the best possible way.
2. Detection of threat: How much an organization is prepared to detect any threat to the system or network.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 8, Issue 12, December 2020 ||

| DOI: 10.15680/IJIRCCE.2020.0812026 |

3. Reaction to any threat: Reaction of any organization to any threat after detection is important. The reaction should be quick and proactive.

III. WHAT IS WIRELESS NETWORK SECURITY

– Wireless network security is the process of designing, implementing, and ensuring security on a wireless computer network. It is a subset of network security that adds protection for a wireless computer network.

– Wireless network security is also known as wireless security.

– Wireless network security primarily protects a wireless network from unauthorized and malicious access attempts. Typically, wireless network security is delivered through wireless devices (usually a wireless router/switch) that encrypts and secures all wireless communication by default. Even if the wireless network security is compromised, the hacker is not able to view the content of the traffic/packet in transit. Moreover, wireless intrusion detection and prevention systems also enable the protection of a wireless network by alerting the wireless network administrator in case of a security breach.

– Some of the common algorithms and standards to ensure wireless network security are Wired Equivalent Policy (WEP) and Wireless Protected Access (WPA).

Wireless Network Security process:

Wireless security is just an aspect of computer security; however, organizations may be particularly vulnerable to security breaches caused by rogue access points.
If an employee (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 using an open USB port, they may create a breach in network security that would allow access to confidential materials. However, there are effective countermeasures (like disabling open switchports during switch configuration and VLAN configuration to limit network access) that are available to protect both the network and the information it contains, but such countermeasures must be applied uniformly to all network devices.

Types of Wireless Network Security:

Wireless protocols are designed to protect wireless networks used within homes and other types of buildings from hackers and unauthorized users. As previously mentioned, there are four **wireless security** protocols, each varying in strength and ability. **Wireless protocols** also encrypt private data as it is being broadcast over the airwaves. This, in turn, protects your private data from hackers and inadvertently protects you.

Below is an in-depth look at the type of wireless protocols that everyone should know about:

1) **The Wired Equivalent Privacy (WEP):** This is the first **wireless security** protocol ever developed. Even though it was designed in 1997, it is still in use today. Regardless, it is considered the most flawed and least secure **wireless security** protocol to use.
2) **The Wi-Fi Protected Access (WPA):** This **wireless security** protocol precedes the WEP. Hence, it is designed to deal with the flaws that are found with the WEP protocol. Notably, it uses the Temporal Key Integrity Protocol (TKIP) and preshared key (PSK), among others, for encryption.
3) **The Wi-Fi Protected Access 2 (WPA 2):** The WPA 2, a successor to WPA, comes with enhanced features and encryption abilities. For instance, the WPA 2 uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) instead of (TKIP). This replacement feature is known to be efficient in encrypting data. Hence, WPA 2 is considered the best **wireless security** protocol.
4) **The Wi-Fi Protected Access 3 (WPA 3):** This one is a recent wireless protocol. It is enhanced in terms of encryption abilities and keeping hackers at bay from both private and public networks.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 8, Issue 12, December 2020 ||

| DOI: 10.15680/IJIRCCE.2020.0812026 |

Below are the top Wi-Fi Security Tips:

1) **Check for Rogue Wi-Fi Access Points:** Rogue access points are a massive security risk since they provide a way in for hackers. The best way is to carry out a Wi-Fi site survey in your home or company building. The best app to use for this is the NetSpot app. This app not only detects rogue access points but gets rid of them effectively.
2) **Strengthen Your Wi-Fi Encryption:** to strengthen your Wi-Fi encryption, you need to identify your Wireless protocol as we saw above. Using NetSpot will help identify your type of encryption.
3) **Secure WPA 2 Password:** Change your WPA 2 password to something inconspicuous. To ensure that your password is strong, use different characters and numbers.
4) **Hide Network Name:** Your service set identifier, or SSID, is often set to broadcast the name of your wireless network. This increases your vulnerability. You can easily change it to "hidden", making it hard for anyone to connect to it if they do not know the name of your wireless network.

Advantage Wireless Network Security:

1) No Wires:

The most distinct advantage provided by wireless cameras is the fact that the technology does not include cables. Breaking into establishments that have fully wired business security systems only needs a pair of wire cutters.
Criminals can blind the latest corded surveillance cameras by disrupting power cables and telephone lines. On the other hand, wireless surveillance cameras have no wires for criminals to attack.
You may also need to drill holes in your wall and get some mounting kit when installing wired security cameras. Although it might not necessarily be a difficult task, putting together something to hold the camera often is time-consuming.
On the other hand, the installation of wireless cameras is incredibly easy, requires little time, and allows you to angle the cameras in whatever direction you choose.

2) Flexibility:

Wireless cameras come with an increased amount of flexibility since the lack of wires allows you to place the cameras in any desired location. Additionally, you won't have to worry about connecting them to an outlet.
Apart from placing them anywhere, you can also program wireless cameras to a range of settings, and physically move them to a different location without dealing with wires.
Having a wired camera works to restrict surveillance locations. It forces you to place your cameras only in the easy to reach spots for cables and other equipment regardless of whether or not these areas are suitable for surveillance devices. The ability to maneuver cameras quickly and install them in high or optimal areas without worrying about outlets could save you a whole lot of trouble. With wireless cameras, your imagination is probably the only restriction you will face when it comes to placement.
Also, having no wires makes hiding the cameras a lot easier, and this would come in handy if you are installing the cameras as a security measure. You probably know that nothing gives away a surveillance camera as much as a hanging wire.

3) Secured Footage:

Apart from the fact that wireless cameras usually come with alarm monitoring services, most of the wireless surveillance systems currently available save data directly to the cloud, which helps to keep the recordings completely safe.
There aren't much-stopping peoples from intruding, and then damaging or taking the surveillance footage for good measure if your wired security system records to an onsite backup. Despite efforts to destroy or delete the data, the surveillance footage will remain accessible if you have wireless cameras installed.
Additionally, wireless security systems use top-rate encryption techniques for the digital data, which makes your video feed safe from both common and cybercriminals.
Wireless cameras are also designed to function for extended periods on independent power sources. As such, they will keep working even during outages.

4) Easy Accessibility:

When it comes to wireless cameras, you can situate the receiver 700 feet to ten miles from the main camera and still pick it up, with total distance depending on the type of camera. The signal also can infiltrate up to eight walls, which includes going through solid objects such as metal, wood, plastic, and glass.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 8, Issue 12, December 2020 ||

| DOI: 10.15680/IJIRCCE.2020.0812026 |

Apart from being able to access a wireless camera from anywhere, you can also check your feeds anytime thanks to the advanced access control system featured. As such, you can leave for a long vacation without necessarily leaving your property undefended.

Disadvantage Wireless Network Security:

1) Cost:

Wireless security systems are technologically advanced and are new in the market. Because of these factors, their demand is higher than the traditional security systems. These systems come with all features that are found in the standard options, including control panels, remote key panels, sirens, and sensors. Each feature, however, also includes a radio transmitter to facilitate the wireless nature of these systems.

The radio transmitters and other features that make wireless systems advanced come at a cost, which makes the cost of the entire alarm system more than the same wired systems. Some people think that these alarm monitoring services are not costly since they do not need to be installed by a specialist.

However, one should put into consideration the cost of this system itself when comparing the cost of installation and the wired security systems. Many business owners purchase these systems for their ease of installation so as avoid spending a lot of their money.

However, this is not always the best thing to do unless you the required training. Non-professional installation can leave your system vulnerable to unintentional damage and hijacking. Because of these challenges, most entrepreneurs pay experts to install for their commercial security systems.

2) Interference:

Some features wired security systems have, but wireless systems do not have. This is a factor that makes this system prone to inference.

When a thief, for example, decides to cut the wire that connects a wired system first before breaking in, an alarm will sound. But that is not the case with a wireless system.

In wireless alarm systems, individual sensors and some of its other components communicate with the control panel using radio waves. Other systems using microwaves can interrupt communication between these components and expose your business security risks. In some cases, frequency interference can cause a false alarm.

And if this trend continues, the control center managers might be tempted to ignore some alarms. Many other things such as metal objects and electronic devices placed near sensors or the control panel can also interfere with radio frequencies.

3) Security:

Since wireless security systems integrate radio signals, they can expose you to great risk. You cannot call the police through a pre-recorded message, and so when you are under an attack and have no time to call the police yourself, you have no remedy.

Also, some of these commercial security systems operate within a narrow band of security codes, so a criminal who has a similar model of security system can disarm your access control system with just a remote control. Many factors can make your system to have unreliable behaviour.

4) Batteries:

Many components of the control panel such as sensors and motion detectors operate on battery power. Batteries can become weak and render the system ineffective as it ages. A failed sensor can leave your business vulnerable until you have the chance to replace the batteries.

As batteries grow weak, some security systems can begin to exhibit erratic behavior and consequently give false alarms or to fail to respond to some or all commands.

After everything is said and done, you can depend on advances in technology and professional security system installation to offset some of these issues. When you are buying wireless security systems, go for those that are built with your unique needs in mind and can last for years.

IV. CONCLUSION

Most importantly Computer and network security must ensure reliability, integrity, protection, and security of information in a meaningful manner. In the case of banking the customers will only avail of the services if the network is secured but in the case of military security of the information is paramount. Besides this, any breach in the security of information may lead to a huge disaster for the country. Network security came into existence on the day when

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 8, Issue 12, December 2020 ||

| DOI: 10.15680/IJIRCCE.2020.0812026 |

computers entered the life of humans. Therefore, Network security helps to protect the assets of the organization. which will ultimately result in securing and saving of reputation of the organization. Hence any breach in network security may lead to revenue loss for a country or an organization also. Because every person /employee of the organization working on the computer is responsible to ensure network security.

Therefore, the organization must educate its employees by conducting seminars and lectures on the importance. Emerging technological advancements demand education and realization of importance by every individual. Therefore, everyone must act responsibly to ensure optimum utilization of networks for the day to day businesses.

REFERENCES

1. www.tutorialspoint.com
2. www.geeksforgeeks.org/network-security
3. https://en.wikipedia.org/wiki/Network_security
4. https://www.techopedia.com/
5. https://www.cisco.com
6. http://about.com/**network security** devices

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details