International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 1402-1407 www.ijaem.net ISSN: 2395-5252

Study on Wireless Network Security: Technical Problem, Present Benefit, Future Evolution

Deepak Kumar Singraul
(Research scholar) a.p.s university rewa m.p)

Submitted: 30-03-2021 Revised: 06-04-2021 Accepted: 09-04-2021

ABSTRACT: I intend to make a survey in wireless data security since wireless networks are very common, both for organizations and individuals.Many mobile laptop computers have wireless cards pre-installed. This completely differs from a wired network where communication device are physically connected through cable and are node without direct association is unable to access the network for illicit activities.therefore,wireless networking has many security issues.

This paper addresses some of the key benefit and some of the shortcomings of wireless networks security. It reviews various types of security levels currently offered by standard wireless networks, such as the wired equivalent privacy (WEP); the Wi-Fi protected access (WPA); and IEEE 802.11 - the latter defined as the ultimate security available for wireless networks to date.Wireless sensor network has received increasing attention from the research community since last decade due to multiple problems associated with it. Out of many other significant problems e.g. routing, energy, load balancing, resource allocation, there is a lesser extent of effective security protocols towards solving security pitfalls in wireless sensor network. This paper studies the trend of research manuscript published in last six years about security problems to find that cryptographic techniques received more attention compared to non-cryptographic-based techniques. It also reviews the existing implementation towards addressing security problems and assesses its effectiveness by highlighting beneficial factor as well as limitations. Finally, we unexplored area of research, which is finalized to be implemented as a part of the future study to overcome the recent security issues

KEYWORDS: 3G-Thirdgeneration,WIFI-WirelessFidel ity,WEP-Wired equivalent privacy,IEEE -802.11,OSI Open systems interconnection,SMTP - stands for Simple Mail Transfer Protocol ,IP - Internet protocol,PKM - Privacy and key management ,QoS - Quality of service,WiMAX - Worldwide interoperability for microwave access,SMTP - Simple mail transfer protocol,WLAN - Wireless local area network,MIMO - Multiple input multiple output,OFDM - orathogonal frequency division,multiplexing,UWB - Ultra wide band,GSM - Global system mobile.

I. INTRODUCATION

Mobile, laptop,computer and wireless application development has come a long way in the past few years. It has progressed beyond the hype of wireless Web applications for consumers to the reality ofhigh- value mobile applications for corporate users.

Opportunities abound for creating new mobile and wireless applications that provide vital benefits to any business. A sampling of these benefits includes increased worker productivity, reduced processing costs, heightened accuracy, and competitive advantage. In contrast is the concern that developing mobile and wireless applications will involve many new technologies and concepts that many corporate developers are still learning to use.One of the challenges in the mobile application space is the variety of application architectures available. Though many by now are now familiar with Wireless Application Protocol (WAP) applications, they are not familiar with smart client and messaging application architectures. (Note: WAP is a specific protocol, but is commonly used to describe any type of thin client wireless application. For a detailed discussion of thin client applications, see Chapter 11, "Thin Client Overview," and Chapter 12, "Thin Client Development.") Thin client refers to server-based applications that make it possible to browse the Internet on a wireless device. All of the business logic and data access logic is located on the server. The only software required on the client is a microbrowser, which is often preinstalled on wireless devices. Thin client applications are attractive because they can build upon existing Internet applications and do not require deployment to the client device. They can be viewed by anyone with a wireless Web-enabled device and can be updated at any time simply by changing the software on the enterprise server.

Thin client applications have one fundamental shortcoming, however: They require a wireless network connection to be effective. Without a connection, information cannot be retrieved from the server, essentially making the application useless. Even when a connection is available, unreliable wireless network coverage, slow data transfer rates, and cost also impact the success of thin client applications.Consequently, a movement is growing toward smart client applications. These applications allow corporations to deploy an application to the mobile device so the user can continue to interact with the application even when a wireless data connection is unavailable. (For more detailed Chapter 7, "Smart Client Overview," and Chapter 8, "Smart Client Development.") These applications commonly include a form of persistent data storage that communicates with enterprise systems using data synchronization. This combination enables applications to have sophisticated user interfaces and high-performance data access, making them suitable for offline computing.information on smart client applications and technology, see Chapter 7, "Smart Client Overview," and Chapter 8, "Smart Client Development.") These applications commonly include a form of persistent data storage that communicates with enterprise systems using data synchronization. This combination enables applications to have sophisticated user interfaces and high-performance data access, making them suitable for offline computing.

The third mobile application architecture of interest is messaging. (For more detailed information on messaging technology, see Chapter 5, "Mobile and Wireless Messaging.") Messaging technology can be used either on its own or to enhance existing applications. Adding notification capabilities to an application can increase. its effectiveness dramatically. Mobile users can have important data "pushed" to them, as opposed to constantly requesting it from an enterprise server. Information notifications can be applied to both thin client and smart client applications.

Messaging applications can also be developed on their own using messaging as the data delivery mechanism. In these applications, message queues are present on both the client and the server, allowing for information to be stored when a user is not connected to the network. Once the user connects, the stored messages are automatically forwarded to him or her. This type of messaging is commonly referred to as store-and-forward.

The technologies available to companies that want to extend their enterprise systems to their mobile workforce are covered in depth in the chapters that follow. All three mobile applications architectures are covered in some depth, as is related information on mobile devices, wireless networks, mobile and wireless security, mobile information management, andlocation-based services. This book provides all of the information you require to build highly successful mobile and wireless applications.Though the content is mainly focused on the creationof enterprise applications, you will find information relevant to developing consumer applications as well.

Safety Instructions In Wireless Network

A wide variety of technical approaches and methods have been used or proposed to analyse system safety, hazards and risk over several decades. The concept of risk management is addressed by ISO 31000 [1] standard that provides a generic framework for assessing and managing risk across various industries. The aim is to obtain an understanding of the risk to inform decisions regarding whether risk is tolerable with respect to some criteria, to differentiate risk associated with different options/decisions, and to determine if (and which) risk treatment options should be implemented to control or modify risk. Barrier management is a safety philosophy widely used in the oil and gas industry [2]. The idea is to control risk by putting measures in place to prevent undesirable incidents from occurring and limit their effects if they occur. Barriers intended to reduce the likelihood of undesirable incidents are called preventive barriers, whereas barriers implemented to avoid escalation and reduce effects of incidents are called mitigating barriers.Systems-Theoretic Accident Model and Processes (STAMP) is a recent accident model, first introduced by [3], based on systems theory focusing on enforcing behavioural safety constraints rather than preventing failures. STAMP is able to assess complex sociotechnical systems by thinking of safety as a control problem rather than a reliability one.Failure Modes, Effects,and Criticality Analysis (FMECA) (a variant of FMEA adding the assessment of criticality)originated from the U.S. Military and was first described in a Military procedure MIL-P-1629A [4] and later used by NASA in the Apollo program. An FMECA involves reviewing components, sub-systems and assemblies to identify failure modes, causes and effects.The approach is described in [5]. Othersignificant approaches are the Fault Tree Analysis (FTA) and the Event Tree Analysis(ETA).

Security Issuses In Wireless Networking

In this topic, we present a systematic review of various security vulnerabilities and weaknesses encountered in wireless networks.Wireless technology releases us from copper wires. These days a user can have a notebook computer, PDA, Pocket PC, Tablet PC, or just a cell phone and stay online anywhere a wireless signal is available. The basic theory behind wireless technology is that signals can be carried by electromagnetic waves that are then transmitted to a signal receiver. But to make two wireless devices understand each other, we need protocols for communication. We will discuss the current security problems with wireless networks and the options for dealing with them. Then present methods that can be used to secure wireless networks. However, it is important to mention the ground reality that all the vulnerabilities that exist in a conventional wired network apply to wireless technologies [6].

208 A. Mushtaq It will be appropriate to discuss some vital concepts about wireless networking [7]. It is easier to understand wireless infrastructures by categorizing them into three layers, as shown below. The three layers are device, physical and application and service (protocol).

Application and service Wireless applications:- WAP, i-mode, messaging, Voice over Wireless network, VoIP, location-based services

Physical:- Wireless standards: 802.11a, 802.11b, 802.11g, AX.25, 3G, CDPD, CDMA, GSM, GPRS, radio, microwave, laser, Bluetooth, 802.15, 802.16, IrDA

Device:- Mobile devices: PDAs, notebooks, cellular phones, pagers, handheld PCs, wearable computers In the device layer (mobile devices) are gadgets ranging from the smallest cell phone to PDAs and notebook computers. These devices use wireless technologies to communicate with each other. The physical layer contains different physical encoding mechanisms for wireless communications. Bluetooth, 802.11x, CDMA, GSM, and 3G are different standards that define different methods to physically encode the data for transmission across the airwaves. We will focus on networks built upon the 802.11x and Bluetooth standards. The application and service layer, also referred to as ISO layers 2 to 7, contains the protocols that enable wireless devices to process data in an end-to-end manner. Protocols like Wireless Application Protocol (WAP), Voice over IP (VoIP), and i- mode reside in this layer. Many wireless networking security problems can be traced back to the end user in wired networks. Wireless networks are no exception, and it is typically the IT department's responsibility to protect the end user. Before an enterprise adopts the latest wireless network technologies, it will need to:

- Understand the capability of current products
- Understand its networking needs
- Understand the potential risk(s) it is facing

Then investigate and find the solution tailored to its environment[8-23]

WIRELESS PHYSICAL-LAYER SECURITY

The issues of privacy and security in wireless communication networks have taken on an increasingly important role as these networkscontinue to flourish worldwide.

Traditionally, security is viewed as an independent feature addressed above thephysical layer, and all widely used cryptographic protocols are designed and implemented assuming the physical layer has already been established and provides an error-free link. However, with the emergence of adhoc and decentralized networks, higher-layer techniques, such as encryption, are complex and difficult to implement. Therefore, there has been a considerable recent attention on studying the fundamental ability of the physical layer to provide secure wireless communications. This paradigm is called Wireless Physical Layer Security. Physical layer security is an emerging research area that explores the possibility of achieving perfect-secrecy data transmission among intended network nodes, while possibly malicious nodes that eavesdrop upon the transmission obtain zero information. The breakthrough concept behind wireless physical layer security is to exploit the characteristics of the wireless channel, such as fading or noise, to provide secrecy for wireless transmissions. While these characteristics have traditionally been seen as impairments, physical layer security takes advantage of these characteristics for improving the security and reliability of wireless communication systems and networks. Information theoretic security provides the theoretical basis behind wireless physical layer security.

Historically information theoretic security, which builds on Shannon’s notion of perfect secrecy, was laid in the 1970s by Wyner and later by Csiszar and K ´ orner, who proved seminal results ¨ showing that there exist channel codes guaranteeing both robustness to transmission errors and a prescribed degree of data confidentiality. In the 1970s and 1980s, the impact of these works was limited, partly because practical wiretap codes were not available, but mostly due to the fact that a strictly positive secrecy capacity in the classical wiretap channel setup requires the legitimate sender and receiver to have some advantage (in general, a better SNR) over the attacker. In recent times, information theoretic security has witnessed a renaissance due in part to the work of Maurer in the 1990s, who proved that even when a legitimate user has a worse channel than an eavesdropper, it is possible for him to generate a secret key through public communication over an insecure yet authenticated channel. In the past few years, significant effort has been applied to the study of information theoretic security for wireless channel models, enhancing the classical wiretap channel and including more realistic assumptions which allow for opportunistic exploitation of the space/time/user dimensions of wireless channels for secret communications. The goal of this special issue is to present recent results in wireless physical layer security that capture the research trends in the field. The papers to be found in this issue provide the reader with a good overview of these trends.This special issue collects 10 papers clustered into two groups: papers dealing with information theoretic aspects and papers focusing on practical scenarios. The first group of papers provides information theoretic results for wireless physical layer security. The first of these, by Bustin et al., derives a closed-form expression for the secrecy capacity of the multiple- input multiple output (MIMO) Gaussian wiretap channel, under a powercovariance constraint. The proof uses a clever relationship between information theory and estimation theory in the Gaussian channel that can be extended to other types of MIMO channels. The paper by Ekrem et al. characterizes the secrecy capacity region between a single transmitter and multiple receivers in a broadcast channel in the presence of an eavesdropper. It provides a clear understanding of secure broadcasting, studying several special classes of channels, with increasing generality. The third paper, by Aggarwal et al., looks at the secrecy capacity of relay channels with orthogonal components in the presence of an additional passive eavesdropper node. Inner and outer bounds on the secrecy capacity are developed for both the discrete memoryless and the Gaussian channel models. The paper by Wang et al. studies secret sharing over the fast- fading MIMO wiretap channel. The key capacity is evaluated where the effects of spatial dimensionality created by the use of multiple antennas at the source, destination, and eavesdropper are investigated. The fifth paper, by Liang et al., focuses on the compound wire-tap channel, which generalizes Wyner's wire-tap model to allow both the channel from the transmitter to the legitimate receiver and that from the transmitter to the eavesdropper to take a number of possible states. The secrecy capacity is studied and established for various cases of interest (degraded, MIMO, etc.). Finally, the paper by He et al. considers a source-destination pair that can communicate only through an untrusted intermediate relay node. In this two- hop communication scenario, in which the use of the untrusted relay node is essential, a positive secrecy rate is shown to be achievable and an upper bound on it is provided. The second group of papers focuses on more practical aspects of wireless physical layer security. The first of these papers, by Tsouri et al., makes use of channel randomness, reciprocity and fast decorrelation in space to secure orthogonal frequency division multiplexing (OFDM) with low overhead on encryption, decryption, and key distribution. These properties make this approach a good alternative to traditional software-based information security algorithms in systems where the costs associated with such algorithms are an obstacle to implementation. The second paper, by Zhan et al., proposes a space-time coding scheme for impulse radio ultra-wideband (UWB) systems. A novel real orthogonal group code is designed for multiantenna UWB signals to exploit the full spatial diversity gain and achieve perfect communication secrecy. The third paper, by Han et al., introduces a game theoretic approach to investigate the interaction between the source that transmits the useful data and friendly jammers who assist the source by masking the eavesdropper. To analyze the outcome of the game, a Stackelberg-type game is investigated and a distributed algorithm is provided. Finally, the paper by Kobayashiet al. studies the frequency-selective broadcast channel with confidential messages, in which the transmitter sends a confidential message to the first receiver and a common message to bothreceivers. A practical Vandermonde precoding approach is provided for which the achievable rate region isstudied.[23]

OPEN CHALLENGES AND FUTURE WORK

In a few years, literally billions of new wireless devices will come online. How should each wireless network treat each new device as it connects? Some devices will need lots of bandwidth. Some will require ultra-low latency. Some will be battery-power-limited. Some may be malicious.

It is surprisingly challenging for network admins to know what is even on their networks. Not all devices identify themselves. Malicious devices can lie about what they are. Furthermore, as more traffic becomes encrypted (as it should be for security) identification becomes even harder. But machine learning can fingerprint devices based on how they use the network (for example, who they talk to, frequency of transmission, or size of packets). And once a device or application has been classified as a particular type, analytics can be applied to confirm that the device continues to behave as expected, or to determine that it is malfunctioning, or that it has been compromised and is a security threat. There are significant research opportunities to improve security simply by allowing networks to know what devices are on them.The growing complexity will also make it more difficult to know if a network is operating as intended or if there is a problem. Ideally, for speed of reaction and for scalability, the network itself should be able to determine this, using AI if necessary, so it can alert an IT staffer when there's an issue outside the bounds of expected or desired performance.

In our work so far, machine learning, fed by huge amounts of rich, contextual information, has allowed us to reduce the alerts a network sends to its operator. In some situations, the reduction is one or two orders of magnitude. These are huge improvements, but there are opportunities for more.

In particular, once problems are found, we need to resolve them quickly. We believe machine reasoning is a key capability to identify the root causes of problems, and to identify likely fixes. This will help turn the dream of the "self- healing" wireless network into reality.[20] A. Mixed Attacks in Wireless Networks Most of the physical-layer

security research[21-23] only addressed the eavesdropping attacks, but has neglected the joint consideration of different types of wireless attacks, such as eavesdropping and DoS attacks.It will be of particularly importance to explore new tech niques of jointly defending against multiple types of wireless attacks, which may be termed as mixed wireless attacks. In order to effectively guard against mixed attacks including both eavesdropping and DoS attacks, we should aim for minimizing the detrimental impact of in terference inflicted by DoS attacks on the legitimate transmission. The security defense mechanism should not only consider the CSI of the interfering ink spanning from the DoS attacker to the legitimate receiver, but ideally should also take into account the CSI of the wire tap link between the legitimate transmitter and the eavesdropper, in addition to the CSI of the main link from the legitimate transmitter to the legitimate receiver. It will be of interest to investigate the security defense mechanisms in different scenarios in the presence of both full and partial knowledge of the CSI of the main link as well as of the interfering link and that of the wiretap link. The full CSI-based scenario will provide a theoretical performance upper bound as a guide for developing new signal processing algorithms to guard against mixed attacks. Moreover, considering the fact that the eavesdropper remains silent and the CSI of the wiretap channel is typically unknown, it is of practical interest to conceive security protocols for the scenario, where the eavesdropper's CSI is unavailable.[24]

II. CONCLUSION

Wireless networking provides numerous opportunities to increase productivity and cut costs. It also alters an organization's overall computer security risk profile. Although it is impossible to totally eliminate all risks associated with wireless networking, it is possible to achieve a reasonable level of overall security by adopting a systematic approach to assessing and managing risk. This paper discussed the threats and vulnerabilities associated with each of the three basic technology components of wireless networks (clients, access points, and the transmission medium) and described various commonly available countermeasures that could be used to mitigate those risks. It also stressed the importance of training and educating users in safe wireless networking procedures.

REFERENCE

[1]. Risk Management—Guidelines; ISO 31000:2018; Technical Report; ISO: Geneva, Switzerland, 2018.

[2]. Principles for Barrier Management in the Petroleum Industry; Technical Report; Petroleum Safety Authority Norway: Stavanger, Norway, 2013.

[3]. Leveson, N. A new accident model for engineering safer systems. Saf. Sci. 2004, 42, 237–270. [CrossRef]

[4]. United States Department of Defense. Procedures for Performing a Failure Mode, Effects and Criticality Analysis 1949; MIL-P- 1629A; Technical Report; United States Department of Defense: Arlington, VA, USA, 1980.

[5]. Rausand, M.A.H. System Reliability Theory: Models, Statistical Methods, and Applications; John Wiley and Sons: Hoboken, NJ, USA, 2004

[6]. Karygiannis, T., Owens, L.: Wireless Network Security: 802.11, Bluetooth and Handheld Devices, National Institute of

Standards and Technology Gaithersburg, MD 20899-8930 (November 2002)Google Scholar

[7]. http://www.wirelesstutorials.info/wireless_networking.html.http://en.wikipedia.org/wiki/Photophone# World.27s_first_wireless_telephone_communication_E2. 80.93_April_1880Google Scholar

[8]. Stallings, W.: Wireless Communications and Networks. Prentice Hall, Englewood Cliffs (August 2001)Google Scholar

[9]. Bidgoli, H.: The Handbook of Information Security. John Wiley & Sons, Inc., Chichester (2005)Google Scholar

[10]. Wireless networks have had a significant impact on the world as far back as World War. Through the use of wireless networks, wikipedia.org/wiki/Wireless_network

[11]. Wi-Fi Protected Access (WPA and WPA2) is a certification program developed by theWi-Fi Alliance toindicate compliance with the security protocol,wikipedia.org/wiki/Wi-Fi_Protected_Access

[12]. Brenner, P.: A Technical Tutorial on the IEEE 802-11 Protocol, Director of Engineering, BreezComGoogle Scholar

[13]. Zhang, Y., Wenke, L.: Intrusion Detection in Wireless Ad-Hoc Networks. In: Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (2000); Arbaugh, W.A., Shankar, N., Justin Wan, Y.C.: Your 802.11 Wireless Network has No Clothes. Department of Computer Science, University of Maryland, March 31 (2001)Google Scholar Journal of Computer Science and Network Security 8(7) (July 2008)Google Scholar

[14]. Borisov, N., Goldberg, I., Wagner, D.: Intercepting Mobile Communiccation Conference on Mobile Computing and Borisov, N.: Deploying Wireless LANs and Voice & Data. McGraw- Hill, New York (2001), doi.ieeecomputersociety.org/10.1109/6294.977772 Google Scholar Networking (2001), http://www.springerlink.com/index/cjut5dxd8 r9tvrpe.pdf

[15]. Borisov, N., Goldberg, I., Wagner, D., Berkeley, U.C., Cox, J.: LAN Services Set to Go Wireless, Network World, August 20(2001); IEEE Working Group forWLAN Standards,

[16]. Borisov, N.: Deploying Wireless LANs and Voice & Data. McGraw- Hill,New York(2001),doi.ieeecomputersociety.org/10.1109/6294.97 7772Google Scholar

[17]. Bradley, T.: CISSP-ISSAP, Introduction to Packet Sniffing, former About.com GuideGoogle Scholar Borisov, N., Goldberg, I., Wagnert, D.: Security of the WEP algorithm

[18]. wep@isaac.cs.berkeley.eduGoogle Scholar

[19]. Paul, S., Preneel, B.: A new weakness in the RC4 keystream generator and an approach to improve the security of the cipher. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 245–259. Springer, Heidelberg (2004)CrossRefGoogle Scholar

[20]. Khan, S., et al.: Denial of Service Attacks and Challenges in Broadband Wireless Networks. IJCSNS International Journal of Computer Science and Network Security 8(7) (July 2008)Google Scholar

[21]. Ingeborn, A., Ingeborn: Lucent Orinoco Registry Encryption/Decryption, http://www.cqure.net/ tools03.html

[22]. Tzu, S., Zi, S.: The Art of War. Dover Publications, New Paperback, 96 pages (2002) ISBN 0486425576

[23]. https://www.researchgate.net/publication/220537567_Wireless_Physical_Layer_Security https://blogs.cisco.com/networking/5-challenges-for-the-future-of-wireless-ne tworking.

International Journal of Advances in Engineering and Management
ISSN: 2395-5252

IJAEM

Volume: 03 Issue: 03 DOI: 10.35629/5252

www.ijaem.net

Email id: ijaem.paper@gmail.com