International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 11 | Nov -2016 www.irjet.net p-ISSN: 2395-0072

Survey on Classification of Attacks and Security Mechanism in Wireless Network

Ashwini A. Lokhande[1],Rupali D. Shinganjude[2],Leela S. Bitla[3]

[1]Ashwini A. Lokhande ,Assistant Professor ,Dept of Information Technology, Priyadarshini Bhagwati college of Engineering,Nagpur,Maharashtra ,India
[2]Rupali D. Shinganjude ,Assistant Professor,Dept of Information Technology, Priyadarshini Bhagwati college of Engineering,Nagpur,Maharashtra ,India
[3]Leela Bitla,Assistant Professor,Dept of Electronics, Priyadarshini Bhagwati college of Engineering,Nagpur,Maharashtra ,India

---

Abstract-*In peoples daily life the usage of wireless devices has been increase ,such as mobile devices and cellular phones .The security for communication by means of this devices is challenging. Communications are sensitive to various types of attacks which arrive due to insecure wireless channels. In this paper we mention different types of attacks and preventive measures .Several prevention methods to avoid such types of attacks is also mention.*

***Key Words*: Wireless devices, Mobile devices, security, communication, attacks, prevention method.**

1. INTRODUCTION

The rapid advancement in a range of mobile and wireless network technology leads to mobile subscribers (MSs) to access Internet service anytime and anywhere[2][3]. The development in the wireless telecommunication is rapidly increasing, but the complementary nature of the existing network and inter-working among them is difficult[4]. Wireless Networks gather and distribute data from the fields where common networks are unreachable for various environmental and strategic reasons.

The need of the hour for every emerging business is Wireless data networks. It's equally essential for an established business to incorporate wireless networks in their IT infrastructure to gain a technological edge over its peers. The mobility, flexibility and expand-ability in the business is greatly added by wireless data network. Besides, there is considerable cost saving when compared to traditional wired networks. However, organizations should be well prepared to face the problems that come with wireless networks.There may be huge number of mobile user that needs to be revoked in the network anytime due to various reasons, e.g. when any prohibited or exceptional event occurs. Computer and network security aim to provide confidentiality, data integrity, and service availability. Confidentiality prevents untrusted third parties from accessing secure data, and data integrity guarantees that data isn't modified in transit and that replayed packets aren't accepted as the original. Availability ensures that authorized parties can access data, services, or other computer and network resources when requested. DoS attacks target availability by preventing communication between network devices or by preventing a single device from sending traffic.

As people will be encouraged to use a secured network, it is important to provide wireless network with reliable security mechanisms if we want to see this exciting technology become widely used in a next few years. Before the development of any security methods to to provide security to mobile wireless networks, it is important to study the variety of attacks that might be related to such networks. With the knowledge of some

common attack issues, researchers might have a better understanding of how mobile wireless networks could be threatened by the attackers, and thus might lead to the development of more reliable security measures in protecting them.

2. RELATED WORK

Security is the process of preventing and detecting unauthorized use of wireless computer. Prevention measures help you to stop unauthorized users from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into wireless network system, if they were successful, and what they may have done. X. Liang [10], [14] propose some mutual authentication and key exchange methods in wireless network for secure communication. In [13] and [14], public key cryptography such as digital signature and Diffie‐Hellman key exchange, is accepted on the basis of SC-based Schemes, which can further improve the security of Wireless Service. Mainly existing wireless schemes for secure communication in network can mainly be classified into three categories: symmetric-cryptosystem-based (SC based), asymmetric-cryptosystem-based (AC-based), and hybrid schemes. The EAP-based authentication and key agreement protocols [8],[16],can also be called as SC-based secure wireless method are designed based on standard protocols. SC-based methods are widely used because they are well match with accepted protocols.

3. ATTACK CHARACTERISTICS

Dynamic topology, distributed operation, and resource constraints are some of the unique characteristics that exist in the wireless networks, which increase the vulnerability of such network. Many characteristics might be

used to differentiate attacks in the wireless networks. Examples would include looking at the behaviour of the attacks (passive vs. active), the source of the attacks (external vs. internal), the processing capability of the attackers (mobile vs. wired), and the number of the attackers (single vs. multiple)

3.1.Passive vs. active attacks

Passive attacks are launched to steal valuable information in the targeted networks. Examples of passive attacks in wireless network are eavesdropping attacks and traffic analysis attacks. Detecting this kind of attack is difficult because neither the system resources nor the critical network functions are physically affected to prove the intrusions [5].While passive attacks do not intend to disrupt the network operations, active attacks on the other hand actively alter the data with the intention to obstruct the operation of the targeted networks. Examples of active attacks comprise

actions such as message modifications, message replays, message fabrications and the denial of service attacks.

3.2.External vs. internal attacks

External attacks are attacks launched by adversaries who are not initially authorized to participate in the network operations. These attacks usually aim to cause network congestion, denying access to specific network function or to disrupt the whole network operations. Bogus packets injection, denial of service, and impersonation are some of the attacks that are usually initiated by the external attackers. More severe attacks in the wireless networks might come from the second source of attacks, which is the internal attack. Internal attacks are initiated by the authorized nodes in the networks, and might come from both compromised and

misbehaving nodes. Internal nodes are identified as compromised nodes if the external attackers hijacked the authorized internal nodes and are then using them to launch attacks against the wireless networks.

3.3. Mobile vs. wired attackers

Mobile attackers are attackers that have the same capabilities as the other nodes in the wireless networks. Since they have the same resources limitations, their capabilities to harm the networks operations are also limited. For instance, with the limited transmitting capabilities and battery powers, mobile attackers could only jam the wireless links within its vicinity. They are not capable to launch the network jamming attacks to disrupt the whole networks operations.

On the other hand, wired attackers are attackers that are capable of gaining access to the external resources such as the electricity. Since they have more resources, they could

launch more severe attacks in the networks, such as jamming the whole networks or breaking expensive cryptography algorithms. Existence of the wired attackers in the wireless networks (especially in the open environment networks) is always possible as long as the wired attackers are able to locate themselves in the communication range and have

access to the wired infrastructures.

3.4.Single vs. multiple attackers

Attackers might choose to launch attacks against the wireless networks independently or by colluding with the other attackers. One man action or single attackers usually generate moderate traffic load as long as they are not capable to reach any wired facilities. Since they also have similar abilities to the other nodes in the networks, their limited resources become the weak points to them [7]. For instance, complex cryptography algorithms could be used to help in defending the authentication, integrity, and the confidentiality services from a single attacker. As it becomes very expensive for the single attackers to break the encrypted messages, nodes in the networks could share the expensive cryptography workloads with each other by exploiting the distributed operations and the multiple connections they had among them.

4.METHODS TO SECURE WIRELESSCOMMUNICATION.

To secure the wireless network there are basic three methods to secure the network from online security attack.

- Prevention: To secure the working wireless network house, prevention would be similar to placing dead bolt locks on network doors, locking network devices, and perhaps installing a chain link fence around network environment. To keep the threat out in wireless network everything can be possibly done.

- Detection: To secure the working wireless network house for detecting such failures happens. Once again using the house analogy, this would be similar to putting a burglar alarm and motion sensors in the wireless network house. These alarms go off when someone breaks in. If prevention fails, you want to be alerted to that as soon as possible.

- Reaction: Detecting the failure has little value if network do not have the ability to respond. What good does it to be alerted to a burglar if nothing is done? If someone breaks into network house and triggers the burglar alarm, one hopes that the local police force can quickly respond. The same holds

true for information security. Once you have detected a failure, you must execute an effective response to the incident.

5.PREVENTION METHODS FROM ATTACK

- Recovering from Viruses, Worms, and Trojan Horses
- Avoiding Social Engineering and Networking Attacks
- Avoiding the Pitfalls of Online Trading
- Using Caution with USB Drives
- Securing Wireless Networks

6. CONCLUSION

In this paper, one can see that attacks against the wireless networks may vary depend on environment the in which attacks are launched, communication layer in which attacks are targeting, and level of wireless network. Mechanisms in which it is targeted.Sseveral attack characteristics that must be considered in designing any security measure for the wireless network are also mentioned. By investigating the characteristics and variations of the attacks, one can make a long list of attacks that could be launch against the wireless networks.

REFERENCES

[1] Chengzhe Lai, , Hui Li, Xiaohui Liang, Rongxing Lu, Kuan Zhang, , and Xuemin Shen, —CPAL: A Conditional Privacy- Preserving Authentication With Access Linkability for Roaming Service‖ IEEE internet of things journal, vol. 1, no. 1, february 2014.

[2] A. Al Shidhani and V. Leung, "Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers," IEEE Trans. DependableSecure Comput., vol. 8, no. 5, pp. 699–713, Sep./Oct. 2011.

[3] P. Taaghol, A. Salkintzis, and J. Iyer, "Seamless integration of mobile WiMAX in 3GPP networks," IEEE Commun. Mag., vol. 46, no. 10,pp. 74–85, Oct. 2008.

[4] Y. Soh, T. Quek, M. Kountouris, and H. Shin, "Energy efficient heterogeneous cellular networks," IEEE J. Sel. Areas Commun., vol. 31, no. 5, pp. 840–850, May 2013.

[5] Huang, X. Hong, and M. Gerla, "Situation-Aware Trust Architecture for Vehicular Networks," *IEEE Communication..Mag.*, vol. 48, no. 11, 2010, pp. 128–35.

[6] A. Bikos and N. Sklavos, "LTE/SAE security issues on 4G wireless networks," IEEE Security. Privacy, vol. 11, no. 2, pp. 55–62, Mar./Apr. 2013.

[7] D. He, C. Chen, J. Bu, S. Chan, and Y. Zhang, "Security and efficiency in roaming services for wireless networks: Challenges, approaches, and prospects,"IEEE Communication. Mag., vol. 51, no. 2, pp. 142–150, Feb. 2013.

[8] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in Proc. IEEE INFOCOM, 2008, pp. 1229–1237.

[9] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy preserving opportunistic computing framework for mobile-healthcare emergency," IEEE Trans. Parallel Distribute. Syst., vol. 24, no. 3, pp. 614–624, Mar. 2013.

[10] X. Liang, X. Li, H. Luan, R. Lu, X. Lin, and X. Shen, "Morality-driven data forwarding with privacy preservation in mobile social networks," IEEE Trans. Technol., vol. 61, no. 7, pp. 3209–3221, Sep. 2012.

[11] Yang, Q. Huang, D. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," IEEE Trans. Wireless Communication.., vol. 9, no. 1, pp. 168–174, Jan. 2010.

[12] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," IEEE Trans. Wireless Communication.., vol. 10, no. 2, pp. 431–436, Feb. 2011.

[13] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Cross-FeatureAnalysis for Detecting Ad-Hoc Routing Anomalies," in Proc.of The 23rd International Conference on DistributedComputing Systems (ICDCS), pp. 478-489, May 19-22, 2003.

[14] Z. Wan, K. Ren, and B. Preneel, "A Secure Privacy-Preserving Roaming Protocol based on Hierarchical Identity- based Encryption for Mobile Networks," *Proc. ACMWiSec '08*, 2008, pp. 62–67.

[15] Yang *et al.*, "Universal Authentication Protocols for Anonymous Wireless Communications," *IEEE Trans.Wireless Communication..*, vol. 9, no. 1, Jan. 2010, pp. 168–74.

[16] D. He *et al.*, "Privacy-Preserving Universal Authentication Protocol for Wireless Communications," *IEEE Trans. WirelessCommunication..*, vol. 10, no. 2, Feb. 2011, pp. 431–36.

[17] D. He *et al.*, "Secure and Efficient Handover Authentication based on Bilinear Pairing Functions," *IEEE Trans. WirelessCommunication..*, vol. 11, no. 1, Jan. 2012, pp. 48–53.

[18] D. He *et al.*, "Handauth: Efficient Handover Authentication with Conditional Privacy for Wireless Networks," *IEEE Trans. Computers*, published online 27 Dec. 2011.

[19] D. He *et al.*, "Strong Roaming Authentication Technique for Wireless and Mobile Networks," *Int'l. J. Communication.Systems*, published online 4 Jan. 2012.

[20] A. Juels and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks," *Proc. NDSS '99*, 1999, pp. 151–65.

[21] K. Zeng, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," *IEEE Wireless Communication..*, vol. 17, no. 5, Oct. 2010, pp. 56–62.

[22] M. Chuang, J. Lee, and M. Chen, "SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks," IEEE Syst. J., vol. 7, no. 1, pp. 102–113, Mar. 2013.

[23] A.Menezes, P. V. Oorschot, and S. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC press, 2010.

[24] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy preserving aggregation scheme for secure smart grid communications," IEEETrans. Parallel Distribute. Syst., vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[25] M. Shi, H. Rutagemwa, X. Shen, J. Mark, and A. Saleh, "A service-agent based roaming architecture for WLAN/Cellular integrated networks," IEEE Trans. Veh. Technol., vol. 56, no. 5, pp. 3168–3181, Sep. 2007.

[26] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routingmisbehavior in mobile ad hoc networks," in Proc. of the 6th annual international conference on Mobile computing andnetworking, pp. 255-265, Aug. 6-11, 2000.

BIOGRAPHIE

Prof.Ashwini A. Lokhande, Assistant Professor, Information Technology Department, Priyadarshini Bhagwati College Of Engineering, Nagpur, Maharashtra, India having one and half years of teaching experience in the field of Computer Science and InformationTechnology.She has received the Master of Engineering Degree in Mobile Technology from Autonomous University, Nagpur,Maharashtra, India, in 2015 and B.E. degree in Information Technology from the University of Nagpur,Maharashtra, India, in 2013.Sheowe number of international journals and conference publications.

Prof.Rupali D. Shinganjude, Assistant Professor, Information Technology Department, Priyadarshini Bhagwati College Of Engineering, Nagpur, Maharashtra, India having 2 and half years of teaching experience in the field of Information Technology.She has received the Master of Engineering Degree in Mobile Technology from Autonomous University, Nagpur,Maharashtra, India, in 2014 and B.E. degree in Information Technology from the University of Nagpur,Maharashtra, India, in 2012. She owe number of international journals and conference publications and is a Life Member of the Indian Society for Technical Education (ISTE).

Prof. Leela S. Bitla From Priyadarshini Bhagwati College Of Engineering, Nagpur, Maharashtra, India having 7 year of teaching experience in the field of Electronics.She received the M.tech in VLSI design from Nagpur University,Maharashtra,in 2013.She proposed her research work in many international Journals as well as International Conferences.She is a Life Member of the Indian Society for Technical Education (ISTE), International Association of Engineering(IAENG).