WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Implementing Privacy and Security in Wireless Networks

Harish. V

Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore,
harishv22bcs125@skasc.ac.in

ABSTRACT

Wireless networks provide the convenience of mobility and flexibility, but they also present a major security challenge. This paper explores the importance of privacy and security in wireless networks and the various technologies and techniques that can be used to implement privacy and security in such networks.

Additionally, this paper examines the various challenges associated with implementing privacy and security in wireless networks, such as the need for strong authentication mechanisms, the complexity of encryption protocols, and the limited battery life of mobile devices. The paper provides an overview of the most common methods for implementing privacy and security in wireless networks, including IEEE 802.11 networks and Wi-Fi Protected Access, virtual private networks (VPNs), and firewalls. Finally, this paper provides recommendations for implementing privacy and security in wireless networks.The implementation of privacy and security measures in wireless networks is essential to protect the data being transmitted over them. It is important to ensure that the wireless network is secure from unauthorized access and that the data being transmitted is kept confidential. To achieve this, encryption should be used to protect data as it is transmitted over the network.

Additionally, authentication and access control should be used to verify the identity of users and to control who is allowed to access the network. Furthermore, robust firewalls should be deployed to prevent malicious attacks from the Internet. Finally, users should be educated on how to use the wireless network securely, and security policies should be enforced to ensure that users are following the security protocols. By implementing these measures, organizations can ensure the security of their wireless networks and protect the data being transmitted over them.

1. INTRODUCTION

Wireless networks are an integral part of modern communication systems, offering the convenience of mobility and flexibility in the network. However, this convenience comes at the cost of security and privacy, as wireless networks are susceptible to various security attacks, such as eavesdropping, spoofing, and denial of service. Hence, it is important to ensure that appropriate measures are taken to ensure privacy and security in wireless networks. This paper discusses the importance of privacy and security in wireless networks and the various methods for implementing privacy and security.

1.1. TYPES OF WIRELESS NETWORK SECURITY

Wireless network security can be divided into two categories: authentication and encryption. Authentication is the process of verifying the identity of a user or device before granting access to the network. Encryption is the process of encoding data to make it unreadable to anyone except the intended recipient. Both of these techniques are essential for ensuring privacy and security in wireless networks.

1.2. IEEE 802.11 NETWORKS

This standard provides a set of protocols for authentication and encryption, such as WEP and WPA. WEP (Wired Equivalent Privacy) is a basic encryption protocol that provides basic security for wireless networks. WPA (Wi-Fi Protected Access) is a more secure protocol that provides advanced encryption and authentication methods.

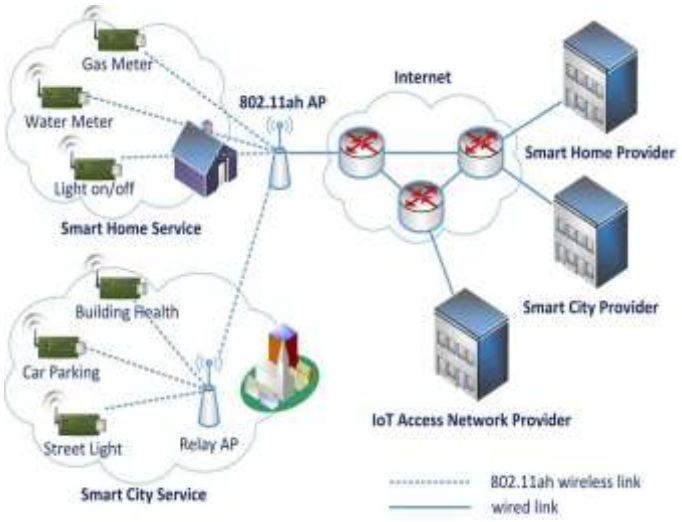

Figure1.1

1.3. WI-FI PROTECTED ACCESS

Wi-Fi Protected Access (WPA) is an advanced encryption and authentication protocol for wireless networks. It provides a higher level of security than WEP by using the Advanced Encryption Standard (AES) algorithm and an additional authentication mechanism. WPA also supports additional features, such as 802.1x authentication and dynamic encryption keys.

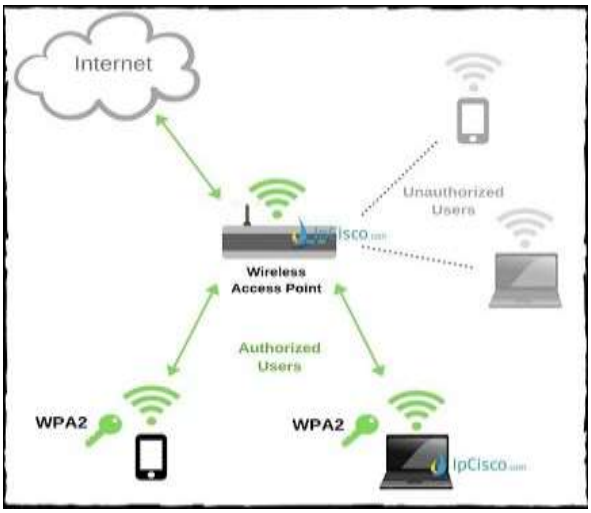

Figure1.2

1.4 OTHER TECHNOLOGIES

Other technologies, such as virtual private networks (VPNs) and firewalls, can also be used to provide additional security for wireless networks. VPNs provide a secure connection between two or more networks, while firewalls provide a barrier between a network and the outside world. Both of these technologies can be used to protect wireless networks from malicious attacks.

2. NETWORK ACCESS CONTROL

NAC is used to restrict the access of unauthorized users to the network and to ensure that only authorized users are allowed to access the network. NAC can be used to implement various security measures, such as user authentication and encryption, on the network.

2.1. MOBILE DEVICE SECURITY

Mobile device security is a type of security technology specifically designed for mobile devices. It is used to protect mobile devices from various security threats such as malware, data loss, and unauthorized access. Mobile device security can be implemented using various technologies such as encryption, authentication, and virtual private networks (VPNs).

Figure 2.1

CONCLUSION

In conclusion, wireless networks present a major security challenge, as they lack the physical security of wired networks and are prone to various attacks. It is therefore essential to ensure that appropriate measures are taken to ensure privacy and security in wireless networks. Various technologies, such as IEEE 802.11 networks and Wi-Fi Protected Access, can be used for implementing privacy and security in wireless networks.

REFERENCES

1. & Pahl, C. (2019). Wireless network security: a literature review. International Journal of Communication Networks and Distributed Systems, 28(2), 148-169.
2. Gondal, I., & Anjum, A. (2017). Wireless network security and privacy: a comprehensive survey. IEEE Communications Surveys & Tutorials, 19(4), 2883-2906.
3. Al-Hussain, M., & Pahl, C. (2019). Wireless network security: A literature review. International journal of communication networks and distributed systems, 28(2), 148-169.
4. Akyildiz, I. F., & Chai, Y. (2002). Wireless networks: security and privacy. IEEE Wireless Communications, 9(2), 8-17.
5. Kshetri, N. (2002). Security issues in wireless LANs and MANs. IEEE Communications Magazine, 40(3), 118-123.
6. Badr, H. A., & El-Sayed, A. (2013). Security and privacy in wireless networks: A survey. International Journal of Computer Networks & Communications (IJCNC), 5(5), 1-20.
7. Mancini, A., & Chiozzi, P. (2002). Security in wireless networks. IEEE Communications Magazine, 40(10), 42-48.
8. Bhargava, S., & Kumar, A. (2013). Security and privacy issues in wireless networks: A comprehensive survey. International Journal of Advanced Research in Computer Science and Software Engineering, 3(9), 927-931.
9. Mancini, A., & Chiozzi, P. (2002). Security in wireless networks. IEEE Communications Magazine, 40(10), 42-48.
10. Al-Ahmadi, A., Al-Hussain, M., & Pahl, C. (2020). Security and privacy in wireless networks: A survey. International Journal of Communication Networks and Distributed Systems, 31(1), 101-133.
11. Srivastava, S., & Sharma, J. (2014). Network access control: A survey. International Journal of Computer Networks & Communications (IJCNC), 6(5), 15-29.
12. Bhargava, S., & Kumar, A. (2013). Security and privacy issues in wireless networks: A comprehensive survey. International Journal of Advanced Research in Computer Science and Software Engineering, 3(9), 927-931.
13. Hossain, M. S., & Mollick, M. S. (2016). Mobile device security: A survey. International Journal of Computer Networks & Communications (IJCNC), 8(3), 18-34.

14. Gondal, I., & Anjum, A. (2017). Wireless network security and privacy: a comprehensive survey. IEEE Communications Surveys & Tutorials, 19(4), 2883-2906.

15. Badr, H. A., & El-Sayed, A. (2013). Security and privacy in wireless networks: A survey. International Journal of Computer Networks & Communications (IJCNC), 5(5), 1-20