East African Journal of Education and Social Sciences
EAJESS July –August 2023, Vol. 4, No. 4, pp. 8-15
ISSN: 2714-2132 (Online), 2714-2183 (Print). Published by G-Card
DOI: https://doi.org/10.46606/eajess2023v04i04.0298.

Comprehensive Analysis of the Wi-Fi Security: A Case of the National Institute of Transport, Tanzania

Lazaro Inon Kumbo
ORCiD: https://orcid.org/0000-0002-6375-9992
Department of Computing and Communication Technology, National Institute of Transport, Tanzania
Email: lazaro.kumbo@nit.ac.tz

Fatma Said Kombo
ORCiD: https://orcid.org/0009-0006-3655-9967
Department of Computing and Communication Technology, National Institute of Transport, Tanzania
Email: fatma.kombo@nit.ac.tz

Peter Godwin Mwakalinga
ORCiD: https://orcid.org/0009-0006-1199-8074
Department of Computing and Communication Technology, National Institute of Transport, Tanzania
Email: peter.godwin@nit.ac.tz

Neema Phillip Bhalalusesa
Department of Computing and Communication Technology, National Institute of Transport, Tanzania
ORCiD: https://orcid.org/0009-0002-9113-5586
E-mail: neema.bhalalusesa@nit.ac.tz

Leticia Edward Mihayo
ORCiD: https://orcid.org/0009-0006-2537-6348
Department of Computing and Communication Technology, National Institute of Transport, Tanzania
Email: leticia.mihayo@nit.ac.tz

Abstract: This study conducted a comprehensive analysis of the Wi-Fi security at the National Institute of Transport in Dar es Salaam, Tanzania. The study used the experimental research design. The study involved testing a variety of devices, including 30 traditional Access Points and 10 smartphones, which can act as access points for other devices. The study utilized a total of 40 devices, selected through convenient sampling. Among these devices, 30 were traditional Access Points and 10 were smartphones acting as Access Points. The primary tool used in this study was a software called Instabridge, which was employed to collect information on wireless networks. The software gathered the names of the wireless networks for further analysis. The experimental process was divided into two main phases: Password extraction and Pairing of Devices. In the Password extraction phase, a smartphone equipped with the Instabridge software was used to collect information on the wireless network which are names and assessed the security of the passwords used. The software detected active devices offering wireless services and could easily unveil the passwords with a single click. In the Pairing of Devices phase, the passwords gathered from the wireless devices were used for authentication. The devices were successfully connected to the access points using the extracted passwords. The study indicated lack of proper security measures, with a significant majority of access points using unencrypted passwords for authentication. To address the existing shortcomings, respective recommendations were made.

Keywords: Information Systems; Information Security; Wireless Local Area Network; Wi-Fi Security.

How to Cite: Kumbo, L. I., Kombo, F. S., Mwakalinga, P. G., Bhalalusesa, N. P. and Mihayo, L. E. (2023). Comprehensive Analysis of the Wi-Fi Security: A Case of the National Institute of Transport, Tanzania. East African Journal of Education and Social Sciences 4(3), 8-15. Doi: https://doi.org/10.46606/eajess2023v04i04.0298.

Introduction

The invention of Wireless networking offers seamless interconnection of devices. Devices require no physical connections to pair and subsequently communicate. The configurations are made easier, physical hindrance is limited and it is faster and convenient. Other advantages include mobility, productivity, deployment and expandability (Yousafzai & Rehman (2017) and Uzunov & Jantchev (2019). It requires few physical devices to offer connection and hence it is less expensive. Despite that, a wireless network is coupled with several security challenges that can impact an organization's general information security. Infrastructures encompass a comprehensive set of policies, procedures, technologies and practices aimed at safeguarding sensitive data and information (Razzaq et al., 2013), Abdul, et al & Choi (2008).

Number of scholars identified security threats that may include but not limited to eavesdropping, a significant threat to WLAN security, which can compromise the confidentiality of data transmitted over the network (Ali et al. (2022. The second possible threat that is associated with wireless Local Area Network is Rogue Access Points, which pose a significant threat to WLANs, as they can be used by attackers to launch various attacks (Ramkumar & Vetrivelan (2021). The authors proposed a novel method for detecting Rogue Access Points in WLANs using machine learning techniques. The third possible concern associated with Wireless Local Area Network is Denial-of-Service Attacks (DoS), serious threat to WLANs which can cause network downtime and can disrupt business operations (Singh et al., 2021). On the other hand, Azimi et al. (2022) reported that Malware is a significant threat to WLANs as it can compromise the security of wireless devices connected to the network. Singh and Kumar (2021) suggested that a new approach for detecting DoS and malware in WLANs is by using machine learning techniques. On the other hands, Asokan and Nithin (2021) pointed out that weak encryption protocols, such as WEP, pose a significant threat to WLAN security, as they can be easily cracked by attackers; the authors proposed a new approach for enhancing WLAN security by using a hybrid encryption protocol that combines symmetric and asymmetric encryption.

Despite efforts to minimize threats, the seamless nature of wireless network makes its administration even more difficult. Users communicate and share information without seeing each other (Obotivere, 2020). The author added that this kind of threat is most dangerous because one never see it coming. Scholars and cyber security practitioners proposed several approaches to address security issues. The profound and most used approach is said to be, the application of technological solutions and policies as aforementioned. The application of technological solutions and policies are believed to be the most used approaches to respond to cyber security threats and vulnerabilities (Obotivere, 2020) and Choi (2008). The administration of the threats related to wireless technology needs an in-depth assessment of the risk linked with wireless technology.

The approaches towards responding to cyber-attacks may differ depending on the particular environment (Parte, 2012). Based on the particular environment, a particular approach may suit that environment but the other may not. On top of that, Parikh (2017) observed that technology plays a big role to minimize cyber-attacks. The author added, threat and vulnerability are the consequence of human behavior and therefore, the outcome can be reduced by educating the community using the particular network. This study conducted a comprehensive analysis of the Wi-Fi security at the National Institute of Transport, Tanzania.

Literature Review

This section explores and synthesizes the existing body of knowledge on Information Security, specifically focusing on the area of wireless setup. It sheds light on key findings, trends and gaps in the field, with a particular emphasis on fundamental components of wireless setups that may serve as potential entry points for intruders into systems. Wireless network is made up of four fundamental parts, the radio frequency for data transmission, access points that link to the corporate network and/or client devices (laptops, PDAs, etc.) and users (Al-Fayoumi et al. (2018). All components must be secured since compromising on any of these components can offer a potential attack vector and the entire network would be at risk.

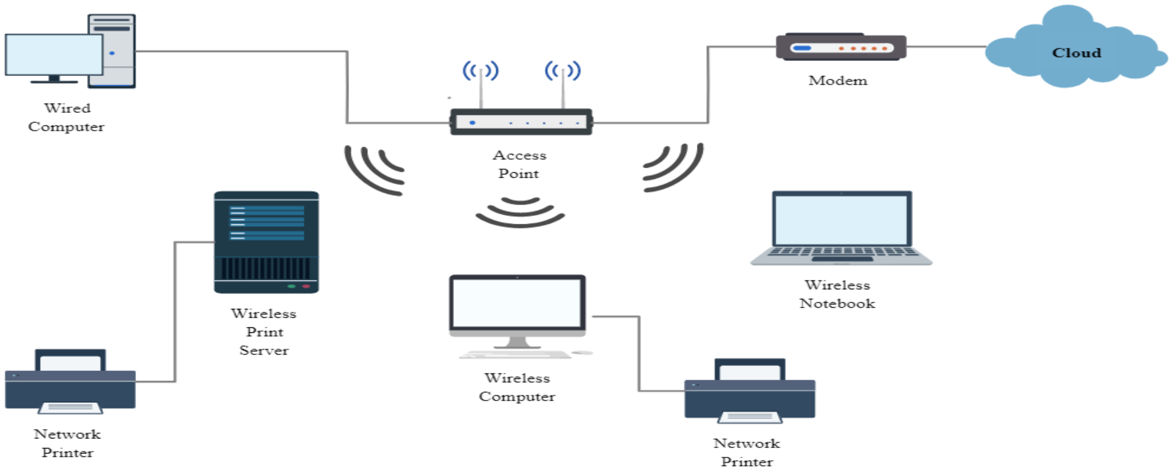

Figure 1: Local Area Network showing interconnection of wireless devices

Source:https://creately.com/diagram/example/g6n53ip01/wireless-network-diagram-template

The authors divided the literature into two groups. The group of possible threats and vulnerabilities and the group of protecting wireless networks. Shrestha and Adhikari (2019) pointed out that if proper security solution is not implemented, the intruder can take advantage and get into the system through faked MAC addresses, unknown stations and illegitimate access points. To address the aforementioned threats, there must be an information security infrastructure mechanism that will offer three essential security objectives which are confidentiality, integrity and availability (Sheth, 2021; Choi, 2008). The three objectives ensure that only authorized users can get into the system, see what is intended for that user and change data and information delegated to change (Parte, 2012). Contrary, unauthorized users can easily connect to an unsecured access point and gain access to sensitive information (Singh & Singh, 2014).

On the other hand, Al-Shaer (2013) and Khurana and Singh (2020) pointed out that unsecured access points for wireless are the Gateway to malicious activities. The study examined security risks associated with unsecured access points and reported that the risks may include malicious activities such as hacking, data theft and virus attacks. The authors concluded that securing access points is crucial for protecting wireless networks from security threats and vulnerabilities. In addition, Li et al. (2017) observed that security risks associated with Wi-Fi networks are eavesdropping, password cracking and man-in-the-middle attacks. The author concludes that securing Wi-Fi networks is crucial for protecting sensitive information from unauthorized access.

The second group of the literature suggests a way of protecting wireless networks. Jang-Jaccard (2014), Li et al (2017) Singh & Singh (2014) argued that to complement the weakness of passwords, encryption is an effective way that secures wireless networks against unauthorized access. The author added, the use of encryption can significantly improve the security of a partially or unsecured wireless network. On top of that, Khalid et al. (2017) compared the security of different wireless network protocols, including WEP, WPA, and WPA2. The study found that using unencrypted passwords on access points is a significant security risk that is more prevalent in networks that use WEP or WPA than in those that use WPA2. In addition, Ali et al. (2019) and Choi (2008) conducted a comprehensive survey of the risks, threats and countermeasures associated with wireless network security. The authors highlighted that the use of unencrypted passwords on access points is a common practice but it poses significant security risks, making the network vulnerable to attacks. Singh and Singh (2014) highlighted that using unencrypted passwords on access points makes it easier for attackers to gain unauthorized access to the network, leading to potential data breaches. The conclusive remarks of Ali et al. (2019) reviewed the current trends and future directions of wireless network security. The authors emphasized the importance of using strong encryption protocols to secure wireless networks.

Methodology

This section explains the methodology used for this study by considering the design, population and Sampling, instruments used, validity and reliability, statistical treatment of data and ethical considerations.

Design
The study used the experimental research design. The study involved testing a variety of devices, including 30 traditional Access Points and 10 smartphones, which can act as access points for other devices.

Population and Sampling
The study was conducted at the National Institute of Transport in Dar es Salaam, Tanzania. It utilized a total of 40 devices, selected through convenient sampling. Among these devices, 30 were traditional Access Points and 10 were smartphones acting as Access Points.

Research Tools
The primary tool used in this study was a software called Instabridge, which was employed to collect information on wireless networks. The software gathered the names of the wireless networks for further analysis. The experimental process was divided into two main phases: Password extraction and Pairing of Devices. In the Password extraction phase, a smartphone equipped with the Instabridge software was used to collect information on the wireless network which are names and assessed the security of the passwords used. The software detected active devices offering wireless services and could easily unveil the passwords with a single click.

In the Pairing of Devices phase, the passwords gathered from the wireless devices were used for authentication. The devices were successfully connected to the access points using the extracted passwords. The study's experimental setup was further explained through a block diagram, illustrating the process of password extraction using the Instabridge software.

Overall, this methodology provides a clear and comprehensive outline of how the data was collected, the tools used and the procedures followed to assess the security of access points. By conducting the experiment in a controlled and systematic manner, the study ensures a reliable investigation into the vulnerabilities and security measures of wireless network.

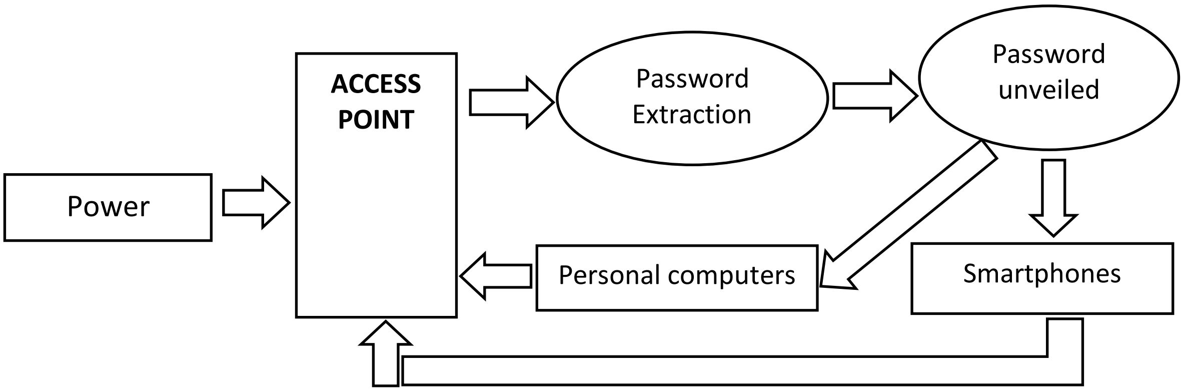

Figure 2: Block Diagram Extraction of password and Pairing to the access point

Validity and Reliability
To ensure the validity and reliability of the data, strict adherence to experimental protocols and guidelines was maintained. The use of Instabridge as a data collection tool aimed to provide accurate and consistent results.

Statistical Treatment of Data
The collected data underwent statistical analysis to determine the effectiveness of security measures used by the devices. The passwords used for the wireless networks were examined for their vulnerability and level of encryption.

Ethical Considerations
The study adhered to strict ethical guidelines, obtaining informed consent from participants and respecting the confidentiality of data held in the devices. The research process prioritized the protection of participants' privacy and ensured ethical conduct throughout the study.

Results and Discussions
This section presents the results and discusses the findings of the study. The study delves into an in-depth analysis of the collected data to provide valuable insights and implications related to the study's objectives. To ensure ethical considerations,

this study adhered to strict guidelines and protocols, obtaining informed consent from participants, maintaining data confidentiality.

The researchers conducted trials on access points to investigate the security of 40 devices. Among these devices, 30 were traditional Access Points (APs) and the remaining 10 were smartphone-based Access Points, commonly known as Smartphone Hotspots. The main objective of the study was to determine the passwords used by each device.

All 40 devices, including the Access Points (X1 to X30) and Smartphone Hotspots (Y1 to Y10) were intentionally involved in the process of password discovery. Throughout the study, the devices were identified and referred to as X and Y, to distinguish between the traditional Access Points and the Smartphone Hotspots. Tables 1 and 2 provide detailed information about specific names assigned to each device, clarifying the distinction between the Access Points and the Smartphone Hotspots.

The following report outlines methodologies, procedures and findings of trials performed on the access points, shedding light on the security measures employed by these devices and their vulnerabilities.

Table 1: Password Extraction for Access Points

Device Name	Status of password after test performed
X_1	Password Unveiled
X_2	Password Unveiled
X_3	Password Unveiled
X_4	Password Unveiled
X_5	Password Unveiled
X_6	Password Unveiled
X_7	Password Unveiled
X_8	Password Unveiled
X_9	Password Unveiled
X_{10}	Password Unveiled
X_{11}	Password Unveiled
X_{12}	Password Unveiled
X_{13}	Password Unveiled
X_{14}	Password Unveiled
X_{15}	Password Unveiled
X_{16}	Password Unveiled
X_{17}	Password Unveiled
X_{18}	Password Unveiled
X_{19}	Password Unveiled
X_{20}	Password Unveiled
X_{21}	Password Unveiled
X_{22}	Password Unveiled
X_{23}	Password Unveiled
X_{24}	Password Unveiled
X_{25}	Password Unveiled
X_{26}	Password not Unveiled
X_{28}	Password Unveiled
X_{29}	Password Unveiled
X_{30}	Password Unveiled

Table 2: Summary Password Extraction for Access Points Source

	Frequency	**Percentage %**
Password Unveiled	29	96.7
Password not Unveiled	1	3.3
Total	**30**	**100**

The study looked at how the hotspot can be accessed by unauthorized users. The results from Table 2 present frequencies and percentages.

The unauthorized access was achieved by using the Instabridge software to crack the passwords that were meant to protect the devices while adherence to ethical considerations. According to the data in table two, 96.7 percent of the access points were not properly configured. The devices were protected by unencrypted passwords and the passwords for these devices were unveiled while 3.3 percent of the Password of access points were not unveiled. These findings demonstrate that the degree of devices being not properly secured was high. The majority of access points were protected by plain passwords while encryption was the most commonly used approach for securing access points.

According to Ali et al (2019) and Choi (2008), unencrypted passwords for authentication are subjected to hacking. If a hacker can get the password of a particular access point, it is possible to enter that network and hence endanger the entire organizational network. The consequences of unprotected wireless networks include security risks and bandwidth theft. This was also observed by Al-Shaer (2013) and Khurana & Singh (2020). The presence of tools like Instabridge allows hackers to uncover passwords, leaving networks partially protected.

Table 3: Password Extraction for Hotspots

Device Name	Status of Password After Test Performed
Y_1	Password Unveiled
Y_2	Password Unveiled
Y_3	Password Unveiled
Y_4	Password Unveiled
Y_5	Password Unveiled
X_6	Password Unveiled
X_7	Password Unveiled
X_8	Password Unveiled
X_9	Password Unveiled
X_{10}	Password Unveiled

Table 4: Summary Password Extraction for Hotspot

	Frequency	Percentage %
Password Unveiled	10	100
Password not Unveiled	0	0
Total	**10**	**100**

The study looked at how the hotspot can be accessed by unauthorized users. The gathered data from Table 3 were analyzed and summarized in Table 4.

According to the data in Table3, all hotspots surveyed were found to be protected by unencrypted passwords, making them vulnerable to potential security breaches. The findings highlight a significant lack of proper security measures in place for these devices, as no hotspot had an encrypted password. This indicates a concerning trend where a majority of access points rely on unencrypted passwords for authentication, exposing them to various intrusions.

The implications of these findings are critical, as unencrypted passwords pose a considerable risk to network security. If a hacker gain access to the password of a specific hotspot, they could potentially infiltrate the entire organizational network, putting sensitive data and resources at risk. To mitigate this security threat, immediate action is required to implement robust encryption measures and promote awareness among hotspot users about the importance of employing secure authentication methods. To address these security issues, various approaches are suggested, including password protection, encryption, firewalls and keeping software updated (Ali et al., 2022). The use of passwords alone may not be sufficient due to the presence of cracking software like Instabridge, which exposes the network to threats.

To improve WLAN security, additional measures are recommended, such as network segmentation, network access control (NAC), artificial intelligence (AI), Machine Learning (ML) and Blockchain Technology. These solutions aim to detect and respond to threats in real-time, enforce security policies and create a tamper-proof ledger of network transactions to prevent unauthorized access and data integrity (Ramkumar & Vetrivelan (2021).

Conclusions and Recommendations

The findings indicate lack of proper security measures, with a significant majority of access points using unencrypted passwords for authentication. This vulnerability exposes devices to potential cyber-attacks and unauthorized access, posing a serious threat to organizational and personal data. To ensure safety and integrity of wireless networks, it is crucial for system administrators and network managers to take immediate actions. Implementing strong encryption protocols for passwords is essential to protect against potential breaches. Additionally, promoting awareness among users about secure authentication methods can help mitigate security risks and prevent unauthorized access. Continuous efforts should be made to improve WLAN security and stay abreast of evolving threats. By proactively addressing vulnerabilities and following recommended settings, organizations can create a safe and secure wireless environment, safeguarding their valuable data and ensuring the integrity of their networks.

System administrators should ensure that all passwords used in the Wireless Local Area Network (WLAN) are encrypted rather than stored as plain text. Strong encryption methods, such as WPA2 and WPA3 should be implemented to protect against cyber-attacks and unauthorized access. The security of WLANs should be continuously reviewed and updated to address new types of threats and vulnerabilities. System administrators must stay informed about the latest security patches and updates for the 802.11 standard to keep the network secure. Periodic security audits should be conducted to assess the overall security posture of the WLAN. This includes evaluating encryption protocols, access controls, firewall settings and network segmentation. Any vulnerabilities or weaknesses identified should be promptly addressed.

References

Ali, M., Khan, F. U., Naeem, M., & Shah, M. A. (2019). Wireless network Security: Current trends and future directions. Wireless Personal Communications, 107(1), 145-169. doi: 10.1007/s11277-019-06357-9.

Al-Fayoumi, M. A., Al-Rawashdeh, E. M., Al-Shibly, H. J., & Jararweh, Y. (2018). Wireless Network Security: A Survey of Risks, Threats and Countermeasures. Journal of Network and Computer Applications, 103, 1-23.

Ali, M., Moustafa, N., & Youssef, A. (2022). Securing wireless communication using encryption, authentication, and key management. Journal of Information Security and Applications, 67, 102828. https://doi.org/10.1016/j.jisa.2021.102828.

Asokan, P., & Nithin, R. (2021). Hybrid encryption approach for wireless local area network security. International Journal of Innovative Technology and Exploring Engineering, 10(12), 625-629. https://doi.org/10.35940/ijitee.L6022.1012619.

Azimi, A., Shiravi, A., & Amini, M. H. (2022). A machine learning-based approach for malware detection in wireless local area networks. Journal of Cybersecurity and Information Management, 1(1), 35-43. https://doi.org/10.1007/s41130-022-00014-9.

Al-Shaer E. (2013), "Unsecured Access Points: A Gateway to Malicious Activities," 2013 International Conference on Advances in Computing, Communications, and Informatics (ICACCI), Mysore, 555-559.

Choi, M. K. (2008). Wireless Network Security: Vulnerabilities, Threats and Countermeasures. International Journal of Multimedia and Ubiquitous Engineering, 77-86.

Khalid, O., Hayat, Z., & Shahid, A. (2017). Comparative study of WEP, WPA, and WPA2 On wireless LAN. International Journal of Advanced Computer Science and Applications, 8(7), 289-295. doi: 10.14569/IJACSA.2017.080741.

Khurana, R., & Singh, K. (2020). Security Vulnerabilities of Wi-Fi Networks. In Wireless Networks and Security (pp. 31-54). Springer, Singapore.

Jang-Jaccard, J. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 973-993.

Li, Y., Zhou, H., Zhang, Y., Xiang, Y., & Chen, S. (2017). Security of Wireless Networks with Unencrypted Passwords. IEEE Access, 5, 5343-5350.

Obotivere, B. A. (2020). Cyber Security Threats on the Internet and Possible Solutions. International Journal of Advanced Research in Computer and Communication Engineering, 92-97.

Parikh, T. P. (2017). Cyber security: Study on Attack, Threat, Vulnerability. International Journal of Research in Modern Engineering and Emerging Technology.

Parte, S. (2012). A Comprehensive Study of Wi-Fi Security – Challenges and solutions. International Journal of Scientific & Engineering Research, 1-5.

Ramkumar, S., & Vetrivelan, R. (2021). Detecting rogue access points in wireless local area networks using machine learning techniques. International Journal of Advanced Networking and Applications, 13(1), 6367-6374. https://doi.org/10.14569/IJANA.2021.130108**.**

Razzaq, A., Hur, A., Ahmed, H. F., Masood, M. (2013). "Cyber security: Threats, reasons, challenges, methodologies, and state of the art solutions for industrial applications. “Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on. IEEE, 2013.

Sheth, A. (2021). Research paper on cyber security. Contemporary research in India, 246 - 251.

Shrestha A. and Adhikari B. (2019), the Importance of Securing Unsecured Wi-Fi Networks, 3rd International Conference on Advanced Information Technologies and Applications (ICAITA), Sydney, NSW, Australia, 1-5.

Singh, D., Singh, D., & Kumar, N. (2021). A machine learning approach for detection and mitigation of denial of service attacks in wireless local area networks. Journal of Network and Computer Applications, 186, 103033. https://doi.org/10.1016/j.jnca.2021.103033.

Singh S. K. and Singh K. (2014), "Protecting Unsecured Access Points With Encryption," 2014 International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 1352-1355.

Uzunov, A., & Jantchev, D. (2019). WLAN security: Overview and analysis of common attacks. 2019 19th International Conference on Computer Systems and Technologies (CompSysTech), Ruse, Bulgaria, pp. 295-301. doi: 10.1145/3345252.3345289.

Yousafzai, S. A., & Rehman, A. (2017). Analyzing the security challenges of wireless local area networks. International Journal of Information Security, 16(6), 703-711. doi: 10.1007/s10207-016-0347-8.