# A Systematic Review: Vulnerability Assessment of Wi-Fi in Educational Institution

**Conference Paper** · May 2020

CITATION
1

READS
217

**4 authors**, including:

Valerianus Hashiyana
The University of Namibia
**33** PUBLICATIONS **31** CITATIONS

SEE PROFILE

IST-Africa 2020 Conference Proceedings
Miriam Cunningham and Paul Cunningham (Eds)
IST-Africa Institute and IIMC, 2020
ISBN: 978-1-905824-65-6

# A Systematic Review: Vulnerability Assessment of Wi-Fi in Educational Institution

Rauha ALUEENDO[1], Nalina SURESH[1], Valerianus HASHIYANA[1],
Emily BAGARUKAYO[2]
[1]*University of Namibia, School of Computing, 340 Mandume Ndemufayo Avenue, Pionierspark, Private Bag 13301, Windhoek, 9000, Namibia*
*Tel: +264612056207, Email: patachokt@gmail.com*
[2]*Makerere University, University Road. P.O.Box 7062, Kampala, Uganda, 00000, Namibia*
*Tel: +256702511076, Email: Ebagarukayo@gmail.com*

**Abstract:** Wi-Fi has been widely accepted in today's generation since it provides liberty to gain access to the network without being physically bonded. Some institutions believe this results in an increase in service and productivity, while reducing the cost of physical wiring; as users bring their devices such as laptops and tablets. With embracing the benefits of Wi-Fi, potential cyber threats can arise through this usage. This paper discusses the greater concern on security issues arising and assessment while embracing the benefits of Wi-Fi. Existing literature was used to evaluate the vulnerability assessment mechanisms available and propose recommendations that educational environments can further adopt, in addition to existing measures to better protect its users.

**Keywords:** Wi-Fi networks, educational institution, vulnerability assessment, Wi-Fi security

## 1. Introduction

Wireless networks, mostly known as Wi-Fi, became increasingly popular in today's world. It has been confirmed that many communication devices today support and embrace the advancement of Wireless Fidelity (Wi-Fi) which has been widening to support at personal and organisational level [1]. These communication devices include laptops, smartphones, tablets and iPads. The significance of Wi-Fi includes: access to network resources, time taken in the installation is less and cost effective, flexible expansion with existing equipment and Wi-Fi devices can be moved without any interruption in the network [2]. The educational institutions may not have enough computers to cater to all students' needs, as a result students make use of their personal devices.

However, the risks of wireless security have become a major concern now that Wi-Fi has been used to support more internet-enabled devices than ever before. Due to the broadcast nature of radio propagation, the air interface is open and accessible to both authorized and illegitimate users. As a result, an open communication environment makes wireless transmissions more vulnerable to malicious attacks than wired communications [3].

The security vulnerabilities facing Wi-Fi are as a result of hardware limitations to sensor nodes, the wireless communication environment, real-time processing needs, heterogenic structure, large number of nodes need for measurability, mobility and cost [4]. As a result nowadays the various security protocols that consider these aspects and their nodes are being developed [4]. In addition, security protocols to be developed in the future

 

should not only implement security issues such as confidentiality, integrity, freshness authentication of the data; but also provide high security together with low energy.

This paper is presented as follows: section 2 outlines the objectives and section 3 explains the methodology used. The analysis of the literature is given in section 4 and the results in section 5. Section 6 discusses conclusion and future recommendations for research.

## 2. Objectives

The main objective of this paper was to review and evaluate the typical vulnerabilities assessment methods to Wi-Fi, against the best practices and to provide recommendations to ensure a secured environment. The different vulnerability assessments have been evaluated with the aim of identifying the work done, the efficient methods and evaluate them.

## 3. Methodology

The work presented in this paper is based on an analysis of literature, with the aim of understanding security issues associated with the usage Wi-Fi. Desktop review has also been used in collecting and evaluating information from multiple resources.

## 4. Technical Description

This section describes the attributes that contribute for assessing vulnerability techniques that are in place such as Wi-Fi Security Risks, Challenges in Security of Wi-Fi, Evaluation and Best Practices: Security Requirements and Principles.

### *4.1 Wi-Fi Security Risks*

With the new initiative called Bring Your Own Device (BYOD), as mobile devices are getting more portable and smarter, this allows users to bring their own personal devices [5]. Similarly in an educational environment, students and lectures utilise these with benefits such as management flexibility, cost saving and simplified IT infrastructure.

As the organisation deploy Wi-Fi, there are risks that threaten the organisations wireless network as identified by [6]:

- Eavesdropping: This is when an attacker gets access to the data transmitted illegally. That makes it impossible to control who can receive the signals in wireless LAN installation. Hence, eavesdropping by the third parties enables the attacker to intercept the transmission over the air from a distance
- Man-in-The-Middle (MITM) Attack: MITM positions an attacker between two hosts with the aim of hijacking the connection and try to inject traffic by installing rogue access points.
- Denial of Service (DOS) Attack: This happens when replaying packets by the attacker with the aim of sending de-authenticate packets to legitimate users in the subnet

### *4.2 Challenges in Security of Wi-Fi*

The vulnerability analysis is a part of risk assessment process that focuses on methods for identifying vulnerabilities and implementing measures to mitigate the vulnerabilities; by implementing suitable protection and safeguard to maintain acceptable network security level and protect information [7]. The need for security vulnerability assessment mostly comes as a result of the organisation that wants to better protect its information and its users on the network. As the threats are evolving and unrelenting increase in number and type of networked devices; decision makers believe their Wi-Fi is exposed [8]. The challenge comes when managing all the devices connected to this network, which can be complicated to network administrators. Similarly, as for educational environments that aims to provide

students with access to the network, finds itself faced with the same issue. Although there are implementations of a broad range of security measures, wireless LAN infrastructure and access are considered to be at the greatest risk to security breaches.

Internet of Things (IoT) devices present big security challenges as typically appliances and sensors are used for data collection and transfer [8].However, most of these devices are unsecured and unable to support common client-based security solutions. In these educational environments, the need for access to network is driven by access to teaching and learning resources, thereby requiring high bandwidth for faster access.

High density has a large impact on wireless networks due to the large amount of devices and the capacity requirements that follow it; as a result of hundreds of students in a large auditorium, lecture halls, stadiums and interactive applications [9]. In addition, as the Wi-Fi is in usage, the need to ensure that the devices connected to an access point are able to use their applications without noticing considerable degradation of performance, is not emphasised enough. For example, when a number of students open an educational video at the same time, this results in slow connectivity and poor experience.

Table 1 summarises some of the challenges faced in maintenance of Wi-Fi in relation to security in an educational environment.

*Table 1: Challenges in Wi-Fi Maintenance*

| Challenge | Source |
|---|---|
| An enormous number of connected devices results in control challenge | [9] |
| User devices that are unable to support common security solutions | [8] |
| Interference, due to medium transmission | [9] |

### *4.3 Institutions and General Public on Wi-Fi Evaluations*

In the paper of [10], the aim was to determine the impact of Wi-Fi in the academic performance of the students in a developing country. The findings indicated that majority of students find Wi-Fi beneficial to their studies, since it enables them to access internet in different spots around campus and allow them to submit academic work on time. In addition, also enable communication with classmates and lecturers.

In the study undertaken by [11], it is emphasised that the vulnerability in security of the university Wi-Fi is due to the fact that they are at the forefront of the technological advancement; and university computing environments are often large open networks. One of the risks in open network is that infection originating in just a single computer can propagate a worm or virus through the entire campus network within minutes [11].

Technical content filtering can also be adopted between lectures, students and technical staff [12]. While technical filtering tools should always be in place, teaching students to be responsible Internet users is the best long-term strategy. Although no technical filtering tool is hundred percent reliable; some objectionable content may still pass through, and savvy students will often find ways to circumvent filtering solutions [12].

It can be deduced from the reviews that more emphasis made highlighted the advantages of Wi-Fi deployment and its usages in these institutions. However, little has been made on evaluations on security, practical experiments to the Wi-Fi and the user restrictions while on this network.

### *4.4 Best Practices: Security Requirements and Principles*

As information is exchanged among users, the process is vulnerable to multiple malicious threats owing to the broadcast nature of the wireless medium. The security requirements of wireless networks are specified for the sake of protecting the wireless transmissions against wireless attacks and secure wireless communications. These should satisfy the requirements of authenticity, confidentiality, integrity and availability [3] as detailed in Table 2.

*Table 2: Security Requirements in Wi-Fi*

| Requirement | Description |
|---|---|
| Authenticity | Mechanisms to pick up messages and verify the identity deceptive packets that come from malicious nodes. If there is no authentication, a malicious node can behave as if it was a different node and might acquire some sensitive data and also hamper proper operation of other nodes. [4] |
| Confidentiality | Certain information is only accessible to those who have been authorized to access it. This means keeping confidential information a secret from all entities that do not have the privilege to access them. [13] |
| Integrity | Ensures that the message will not be altered during communication. [4], [13] |
| Availability | A node should maintain its ability to provide all the designed services regardless of the security state of it. [13] |

There are some principles that [14], [15] identified that a secured network should have:

- Network Segmentation and Segregation
  In order for the network to be secured safely for usage, core network and wireless network should be defined. This will prevent unauthorised parties from accessing the core network intentionally and to also filter out devices that intentionally limit out from the network.
- Firewall
  Filtering takes place as the system administrator restricts users from prohibited websites and programs. This can be achieved together with intrusion prevention systems, firewall, application identification and control.
- Policy Enforcement
  The organisation must clearly define an understandable policy or agreement of prohibited actions in wireless network such as packet sniffing or placing any device that can act as a RAP might help to reduce malicious activities in wireless network. For social engineering threats, a written agreement policy between users and administrators must be taken place from the first day of work. Users might be given certain unique password to login into the organisations Wi-Fi network and repeatedly reminding them not to share the password and other sensitive credentials to others.
- Device Management and Monitoring
  Managing devices can aid in controlling device management access to applications and programs. Should the device be lost or stolen, it can be wiped remotely. Access Points should be registered with an automated system that updates activities. With this comes a need for a role based access control that will assign roles to any device based on how they were authenticated. Monitoring user's activity in real time and managing application that are using the network helps the administrators identify malicious activities and take necessary steps for a safer environment. Moreover, all devices need to be registered and be assigned a unique IP, this can be done by the help of the network access control where users register themselves on the network.

## 5. Results

The reviewed literature indicates that there is a need of continuous review and monitoring in Wi-Fi security. To identify the security issues, a vulnerability assessment is conducted. The lack of alignment in terms of awareness and safety between the organisation and its users was indicated to be one of the challenges and this can lead to attackers exploiting the

system leaving the organisation and Wi-Fi users at risk. The following guidelines have been framed to be used in the threat management of the educational institution.

### *5.1 Wi-Fi Vulnerability Assessment through Penetration Testing*

Penetration testing can reveal to what extent the security of IT systems is threatened by attacks by attackers and whether the security measures in place are currently capable of ensuring IT security [16]. By employing a network penetration strategy, the organisation experiments on its infrastructure in the hands of an attacker; and can identify loopholes that need to be fixed.

### *5.2 Using a Defence-in-Depth Strategy*

In light of mitigating risks of Wi-Fi, organisations can use the Defence-in-Depth Strategy as shown in the Figure 1 [17].

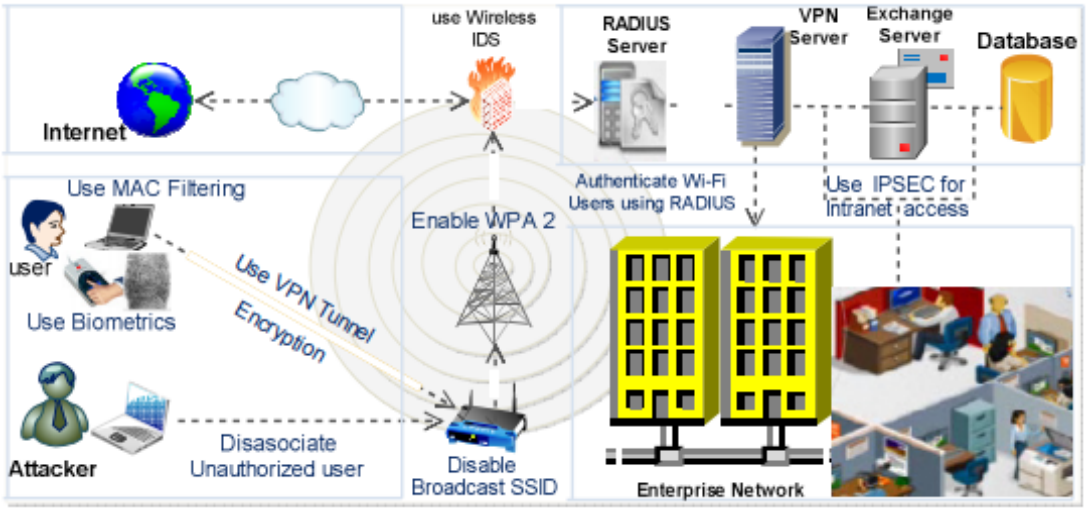


*Figure 1: Defence-in-Depth Strategy*

This strategy can be achieved by collecting, analysing and assessing security events in real time using Wireless Intrusion Detection Systems and Security Information and Event management solutions. For security, per-packet authentication using RADIUS and central encryption and security management using SSL VPN. To ensure application layer encryption, use HTTPS instead of HTTP; WPA2 and AES for data protection.

To ensure device security, use vulnerabilities and patches. For device control, it is essential to utilise VPN, IPSec, biometric for access control. However, packet analysers can be used to sniff exchange of frames over the network for knowing IP addresses in use, thus the use of static IP addresses is not fool proof but at least deterrent [6]. The use of encrypted proxies is also essential.

### *5.3 Enforce Wi-Fi Policies*

Tailor-made policies should be defined that meets the requirements of the educational organisation. These policies must include the forbidding of unauthorised access points, ad hoc networks and reconfigurations of access points. The policy must also operate on set channels at a certain speed and during selected hours to monitor suspicious activities [6].

### *5.4 Utilise VPN*

As iterated in [6], the VPN authenticates the users and encrypts their communication so that if anybody is listening to it, they cannot intercept it. This means the internet connection is encrypted to secure it and protects the user's privacy, therefore the information sent over the network is protected at all times.

## 6. Conclusions

This paper evaluated the security in Wi-Fi and the vulnerability assessment on the Wi-Fi network. The results of this discussion shows that the network administrators are faced with a challenge of controlling and managing devices on the Wi-Fi networks in educational institutions due to the increase in number of users. However, this can be alleviated by in-depth constant monitoring of the network. It has also been observed that more emphasis is given to the user to protect themselves when on the network than the network security functionality to provide the security.

In conclusion, the future work suggests to conduct a vulnerability assessment through a network penetration testing, experimenting on the Wi-Fi for an educational environment. This will reveal real time malicious activities on the Wi-Fi network and also for the organisation to view itself from an intruder's view on the loopholes. Various and reliable techniques will be employed to conduct the test in the environment to expose the loopholes. The results can be used by system administrators to better protect the network from intruders and also from legally authenticated users from malicious activities.

## References


[1] G. Zhan and A. H. K. Wong, "Consumer Adoption of Wi-Fi Network," in *Proceedings of the 8th International Conference on E-Education, E-Business, E-Management and E-Learning - IC4E '17*, 2017, pp. 1–5.

[2] R. K. Singh and N. Tiwari, "An Investigation on Wireless Mobile Network and Wireless LAN (Wi-Fi) for Performance Evaluation," *Int. J. Comput. Appl.*, vol. 126, no. 6, pp. 1–8, 2015.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[4] M. Dener, "Security analysis in wireless sensor networks," *Int. J. Distrib. Sens. Networks*, pp. 1–9, 2014.

[5] M. Olalere, M. T. Abdullah, R. Mahmod, and A. Abdullah, "A Review of Bring Your Own Device on Security Issues," *SAGE Open*, vol. 5, no. 2, p. 215824401558037, 2015.

[6] D. Dhiman, "WLAN Security Issues and Solutions," *J. Comput. Eng.*, vol. 16, no. 1, pp. 67–75, 2014.

[7] Z. I. Saleh, H. Refai, and A. Mashhour, "Proposed Framework for Security Risk Assessment," *J. Inf. Secur.*, vol. 02, no. 02, pp. 85–90, 2011.

[8] Fortinet, "Wireless Security Trends: State of the Market," 2016.

[9] "Higher Education Wi-Fi Challenges - Packet6," 2020. [Online]. Available: https://www.packet6.com/higher-education-wi-fi-challenges-and-solutions/. [Accessed: 12-Jan-2020].

[10] K. M. Moate, J. E. Chukwuere, and M. B. Mavhungu, "The Impact of Wireless Fidelity on Students Academic Performance in a Developing Economy," *31st Int. Acad. Conf.*, pp. 139–155, 2017.

[11] U. Kumar, C. Joshi, and N. Gaud, "Measurement of Security Dangers in University Network," *Int. J. Comput. Appl.*, vol. 155, no. 1, pp. 6–10, 2016.

[12] U.S.Department of Education, "Building Technology Infrastructure for Learning," 2017.

[13] S. Saini and Y. K. Sharma, "International Journal of Advanced Research in Computer Science and Software Engineering," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 6, no. 3, pp. 473–479, 2016.

[14] D. Mareco, "17 Features Every Fast, Secure WiFi Network Should Have," *Secure Edge*, 2017. [Online]. Available: https://www.securedgenetworks.com/blog/11-features-every-secure-wireless-network-should-have. [Accessed: 20-Feb-2020].

[15] M. M. Noor and W. H. Hassan, "Wireless Networks : Developments , Threats and Countermeasures," vol. 3, no. 1, pp. 119–134, 2013.

[16] Federal Office for Information Security (BSI), "Study: A Penetration Testing Model Security," *Bsi*. 2010.

[17] A. I. Angela, "Evaluation of Enhanced Security Solutions in 802.11-Based Networks," *Int. J. Netw. Secur. Its Appl.*, vol. 6, no. 4, pp. 29–42, 2014.