NATIONAL BOARD FOR TECHNICAL EDUCATION
NIGERIAN JOURNAL FOR TECHNICAL EDUCATION
Volume 21 Nos. 1 2023
ISSN No. 2992 - 3522

Framework on Improved security of a Wireless Campus Network using Hybrid Techniques(Wi-Fi-Protected Access 3 and Virtual Private network)

Chika Lilian Onyagu[1] and Moses Titus Yilleng[2]

Department of Science, Grundtvig Polytechnic Oba, Anambra State
Department of Polytechnic Program, National Board for Technical Education, Kaduna State
***Corresponding Author Email:** chiscollinpaul@gmail.com

Abstract
The advent of wireless network contributed to the advancement in information technology systems such as mobile phones, handheld devices and tablet computers. With mobile technologies and wi-Fi technologies, people get access to internet and surf online at comfort of their zone. Campus network is an independent network of an organization such as governments, institutions and corporate bodies. It connects different LANs or WLAN within the specified geographical area. The current wireless security standard of much campus is based on WiFi Protected Access 2(WPA2), which confirmed to have some vulnerabilities such as being prone to Password attack. The aim of this research is to enhance the existing security of wireless Campus Network using hybrid techniques. The methodology adopted is a hybrid wireless security technique which includes; WiFi Protected Access 3(WPA3) and Virtual Private Network. The implementation of the hybrid techniques (WPA3 and VPN) on the Existing security of the campus strengthens the security. With the hybrid systems, the wireless network of a campus will be strong as WPA3 prevent attack on password while VPN secures the campus network from public network (internet). Network security is better managed using strong hybrid approach, because network attacker could get hold of one layer and the second security layer will still be efficient in securing the network. The use of WPA3 and VPN is considered good practice as both uses strong Cryptographic encryption algorithm.

Keywords: WPA3, VPN, Cyber-threat, Wireless Security

Introduction

The emergence of Information technology has revolutionized the world. Its benefits and application had cut across various fields of life such as education, businesses, military, transportation and others. With computer network and internet features, exchange of information has become easy. Khan Academy in its publication on Computer network defined Computer network as a group of interconnected devices with capability of exchanging data or information. The work further explained various computer network as; Local Area network (LAN), which is a network with small geographical area, the Metropolitan area network coverage could be limited within a city, while campus network is a network a network of an institution, which could be a LAN and Wide

Area Network, which has the widest coverage. These computer network types can assume two forms: wired and wireless. While the wired consist of physical connections of information Technology gadgets, the wireless network uses radio waves for its connections Microtech (2021).

The advent of wireless network has contributed to the advancement in information technology systems such as mobile phones, handheld devices and tablet computers. Mobile technologies have affected positively in the modern digital world; online training, research, e-commerce, information sharing, team collaborations, business management, cloud services and information storage and management.

Campus network is an independent network of an organization such as governments, institutions and corporate bodies. It connects different LANs or WLAN within the specified geographical area Ali et al.(2015). Campus network plays a vital role in modern educational system as institutions are gaining online presence. Features of internet and online activities in educational sectors made campus network a vital tool for teaching, learning, administrative Management, on-campus and off–campus study Khani et al.(2018). Although Information systems presented many benefits to businesses, organizations, and education systems, the greatest challenge remained privacy and security of Information Ali et al.(2015). The authors maintained that security issues in information technology is a global challenge that have cut across many fields, which education system is one of them. Some of the identified issues in campus network are physical security threat and unauthorized access to the network. Unauthorized users could launch cyber-attack through virus infection, eavesdropping, and sniffing attack. With these attack techniques, threat actors could gain entry to the network on the campus in order to steal information, modify vital data or even disrupt activities of the system.

No matter how secure a system is, there are security vulnerabilities that adversaries will be able to explore. As more network security measures are developed, Cyber threat actors advanced their mechanism and invent more tools to perpetrate their attack However, more attention should be given to network devices and its connectivity by doing continuous upgrade to reduce security threats and cyber-attacksArjun et al, (2017). This research proposes an improved security framework for a campus network with wireless fidelity protected access 3 (WPA3) protocol, virtual Private network (VPN) technology, to strengthen the existing security measures of a wireless Campus network.The essence of campus network in an institution is to provide internet connectivity within an institution, to enable students and staff use internet features for teaching and learning. According to (Kaspersky, 2016), many Wi-Fi network connections used in online communication is unsecure and poses risk for the users. The general problem of wireless network is mostly on its user authentication, managed by Wifi security protocol.

The work of authors reviewed in this paper focused on analysis of threats on wireless network and security measures taken to manage them. (Arjun et al,. 2017) analyzes various wi-fi protocols used in wireless network as it relates to the case study. The authors used "Acrylic Wi-Fi Home Go Pro " and weka software for collection and analysis of data through the case study router. (Khani et al,.2022) analyzes various threats of a wireless campus network and proffer strategic guidelines to counter the threats., However, (Losonczi et al,.2019) analyzed security of a wi-fi network in campus and suggested a secured approach using firewall and Intrusion detection system. (Huang et al 2019) in their work, proposed secured campus network using Secured Socket Layer (SSL) and Secured Internet Protocol (IPS) with firewall, while (Kumari et al,.2011) presented a hybrid approach for a secured campus network with VLAN, Encryption systems multiple OS at servers and Virtual Private Network. The work of (Zhang, 2018) designed a secured information security of campus network by analyzing the network architecture of the case study and introduced multiple techniques; Firewall, Anti-virus, and Intrusion detection system. Research by Tao et al.,(2012) analyzes the internal and external threat to a campus network and proffer a security strategy to manage the situation. However, (Cuihong ,2010) analyzes problems of campus network suggested a secured approach using VLAN, Encryption Systems and Public Key Infrastructure. The work of (Zheng et al,.2021) used a network tool: "Webhunt" to analyze the security status of seven-campus network, which discovered so many vulnerability, concealed in campus network. (Terry, 2022) presented security framework for managing university network. The author incorporated strategic procedures and use of depth-in approach to ensure security of the network and information.

Researchers have identified vulnerabilities in WiFiProtected Access 2 (WPA2), which is the current security protocol use in wireless network connection.Wi-Fi Protected Access-2 is the upgrade version WPA that supports two modes of security: "Personal mode" and "Enterprise mode". In Personal User, pre-shared passkey is use for authentication. The passkey is not resistant to passwordattack. However, the "Enterprise mode" uses RADIUS server for its authentication not pre-shared key. The RADIUS Server is also vulnerable to KRACK Attack (Key Reinstallation attack). With KRACK attack, an attacker can intercept the access point and create a "Rogue Router", to lure victims of signing to the "rouge router" as the legitimate router Ahmad et al. (2021). The above problems pose a lot security challenges to the campus: first, the use of a single server in the campus causes downtime whenever the server is overloaded. Secondarily attackers can easily target the server with DDoS attack, which disrupts other online activities on the campus. Unauthorized users could have access to the network and causes harm without easily detected. Hence the purpose for a secured campus network which this work present with WPA3, multiple webservers and Virtual private Network.

Wireless Network Attack

This section analyzes various threats in wireless campus network. The threat of a wireless network is categorized into two: the physical security threats and unauthorized accesses to the network.

Physical security Threats

The work of (Ji,2015) explained the possible physical threats to a wireless network which can come from natural disaster (Flood, earthquake, and fire), environmental conditions(high temperature, humidity, lightening and heavy rainfall) and theft of wireless technologies). These physical threats could destroy wireless technologies in the campus. Theft activities is another big challenge to wireless technologies, as hoodlum can locate the area and made away the technologies because it is installed in an open place.

Unauthorized Access

Unauthorized access is gaining entry to computer network, application software, or information without permission. This is the major security threat to a campus network, as students or other threat actors could gain entry into the school portal and stole or even modify vital information Li (2012).

Unauthorized access threats to computer network could be from various sources such as; phishing, Password attack, sniffing, Virus Invasion and DDoS.

Virus Invasion

Computer virus is the most common computer attack. Virus attack to a system could spread to other systems on the network and cause harm. With virus attack, attackers can steal vital information such as example questions, modification of students result, hijacking a session and crashing of web and Database server Hung et al.(2019).Virus attack can be from internal users of network (staff or students), with intentional or unintentional motives.

Phishing attack

Attackers could launch attack to the campus network through a felony websites to lure students and staff accessing the website. (Whitney, 2020) in his publication opined that phishing attack had targeted schools. Through spear phishing, which its target is to specific individuals or offices, or Business email compromise attack. With spear phishing, aggrieved students can target server system in exams and record by sending a phishing link to lure staff into click on the link. Through this means, security breach such as alteration to student result or leakage of exam questions. In addition to spear phishing,

Distributed Denial of Service (DDos):

Distributed Denial of Service is attack from a multiple source to a targeted system, which could be website, server, or other network resources in order cause downtime, unresponsive, which denied users access to the system Lutkevich (2020). Attackers could launch DDoS attack through a vulnerability in a system, malware, phishing and Adware. With DDoS attack, attacker can disrupt activities in the campus network such as online exams, interviews, class and research.

Sniffing Attack

Sniffing attack occur when an attacker uses packet sniffer to monitor network traffic in order to steal vital information. The target of sniffing attack is usually on “financial information, Login credentials and email messages” Sniffing attack can occur in two ways; Passive and Active. In Passive attack, the attacker monitors the network traffic without causing harm just to study the victim's activities while attacker in active sniffing, attacker's motive is to cause harm to its target in order to steal information or make an alteration. There are various kinds of sniffing attack; TCP session stealing, LAN sniff, Protocol sniff, Application-level sniffing, attackers target could be on any of this type Biasco (2021).

Password Attack

Password attack is a process that involve attacker, gaining entry to a system secured with password. It is a common attack to user account. This requires special techniques by hackers. There are various password attacks; brute force attack and dictionary attacker. Through brute force, attacker could easily guessed a weak password. Attackers uses victim's personal information from social media or relatives to guess password. In dictionary attack, attacker uses a special application to check common password used online EasyDemarc (2022).

Security Technologies in Wireless Network

Securing wireless Technology is a major challenge facing wireless network. As attackers advanced in their attack techniques, the fight against unauthorized access to wireless network becomes harder. There are various wireless technologies and protocols specified in IEEE standard found in 802.11. IEEE 802.11 standard are group of Technological advancement specified by Wi-Fi Alliance. Every advancement is noted by a suffix after eleven, (802.11a, 802.11b, 802.11i, 802.11n). The suffix represent the upgrade on the standard either on speed, or on coding algorithm. Various Wireless security protocols specified in Wi-Fi 802.11 standard are; Wired Equivalent Privacy (WEP) is the first protocol followed by Wireless Protected Access (WAP), Wireless Protected Access 2(WAP2) and the latest, which is Wireless Protected Access 3(WAP3) Kawshik&Sewal (2018).

Wired Equivalent Privacy (WEP)

WEP was the first security protocol used in wireless network, introduced in 1997. The purpose of WEP was to improve the security of wireless network by encrypting data against eavesdropping and sniffing attack. With Data, encryption the interceptor will not recognized the data except the authorized system on the network. Wired Equivalent Privacy used symmetric algorithm of 64-128bit key. WEP had been identified to have some vulnerabilities such as; use of open and shared key value, use of easy to crack encryption algorithm. These vulnerabilities made WEP a weak protocol hence not reliable for data security Arjun et al.(2017).

Wi-Fi Protected Access (WPA)

WPA was introduced in 2003 by Wi-Fi Alliance to replace wired equivalent Privacy (WEP) because of its vulnerabilities. Wi-Fi protected Access shared some similarities with WEP but differs in a way both handled security keys. While WEP uses same key for authorization ofsystems, WPA use Temporary key Integrity Protocol (TKIP), which dynamically changes the system key. WPA uses encryption key of 256 bit length which higher than the Key length. The Temporary key Integrity Protocol (TKIP) later upgraded to Advanced Encryption standard. Despite the advanced encryption key of WPA, some vulnerabilities was identified in them. WPA is prone to KRACK attack, in addition, has compatibility issues with operating systems and hardware Lomas (2017).

Wi-Fi Protected Access 2(WPA2)

WPA2 is an improved version of WPA, which uses IEEE standard 802.11i with data encryption algorithm. WPA2 is a default protocol for modern routers, with Advanced Encryption standard (AES) for data protection. Wi-Fi supports two security modes: Home use and Enterprise use, a pre-shared Key is home use configuration. “Access points are manually configured for the authentication”. Most modern mobile devices use WPA2 protocol to connect to other Wi-Fi devices. WPA2 protocol considered unsafe due to its vulnerabilities, which is KRACK attack. During KRACK attack, attacker manipulate encrypted data. In addition to this vulnerability, WPA2 speed is relatively slow Ahmad et al. (2021).

Wi-Fi Protected Access 3(WPA 3)

WPA 3 is the latest updated Wi-Fi security protocol, released in 2018. The protocol was developed to counter the vulnerabilities of WPA2. WPA 3 supports three security modes: Personal WPA3, Enterprise and Wi-Fi enhanced Open Mode. These modes have strong encryption algorithm that is better than its predecessor is.

It provides automatic encryption to user password. With its automatic encryption method, weak passwords are protected against brute force and dictionary attack. WPA 3 Simultaneous Authentication of Equals (SAE, “replaces WPA2-PSK”. In addition to SAE, WPA3 Enterprise mode have the following features: 256-bit Galois/Counter Mode Protocol (GCMP-256) provides First authenticated encryption. Second, key derivation uses 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (SHA), thirdly, Key establishment uses Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA), lastly Frame protection is based on 256-bit Broadcast/Multicast Integrity Buczkowski (2018).

Virtual Private Network (VPN)

Virtual Private Network is a network security technology that secures internet connection against sniffing and eavesdropping attack. It protects internet packet by providing data encryption. With VPN organization's private network is protected from unsecured public network such as internet. VPN masks IP address online to remains private and untraceable. Even when attackers get hold of the data, it makes no meaning because of the encryption. Implementation of VPN is cheaper and scalable. It offers staff to use their private network remotely while still secured Powell (2010).

Overview of the proposed Network

Wi-Fi Protected Access 3- Simultaneous Authentication of Equals (WPA3-SAE)

Wi-Fi Protected Access 3 replaced WPA2 Pre-shared Key with Simultaneous Authentication of Equals (SAE). SAE is a new authentication method for the 802.11 wireless standards. Wi-Fi Protected Access 3 uses SAE to generate a unique Hash key during authentication. This differentiated Wi-Fi Protected Access 3(WPA3) from Wi-Fi Protected Access 2(WPA2), which uses the same pre-shared key for all authenticated systems. The establishment of a hashed unique key, whenever the user and server interact, makes it difficult for an attacker to guess the passkey Buczkowski(2018).

Wi-Fi Protected Access 3 comes in two security modes: personal mode and Enterprise mode. The personal mode authentication uses a password or passkey for authentication. However, the Simultaneous Authentication Equal (SAE) secures the password by providing a Hash function of it. This feature protects weak passwords against brute force or dictionary attacks. Simultaneous Authentication Equals ensure packet forward secrecy by encrypting the traffic. Even if an attacker gets hold of transmitted data, it cannot be decrypted easily. However, the Enterprise mode provides additional protection with an encryption key of 192 bits over transmitted data. Another improvement of the WPA3 enterprise is the use RADIUS (Remote Authentication Dial-In User Service) server for its authentication. RADIUS is a protocol that allows remote server communication with the central server to authenticate users that request its services Loshen(2021).

Cryptographic WPA3

Wi-Fi Protected Access 3 is permitted to use Advanced Encryption Standard (AES), unlike WEP and WAP2, which support the "Temporary Key Integrity Protocol". The AES has an encryption key of about 128 bits, and WPA3 provides an additional encryption key of 192 bits, which enhances its Cryptographic feature. WPA3 uses its Cryptographic strength to ensure secure Authentication on a wireless network.

WPA3 has two major versions: the Personal and Enterprise mode. The versions came with different capabilities.

WPA3-Personal

The WPA3-personal, also known as WPA-SAE (Secure Authentication of Equals) supports the Microsoft windows operating System with WLAN Device Driver Interface 1.18 and higher. WAP-SAE supports Windows Desktop OS (version 10) and Mobile device OS (Android 13, Mac OS, Apple iOS13, and iPadOS). The Authentication method of SAE takes place on the windows Operating system with its supported Driver. WAP3-SAE supports individualized connection, home or small business networks. WPA3-SAE does not support a network with an authentication server.

WPA3-personnel Authentication

WPA3-Personal uses Simultaneous Authentication Equal (SAE) encryption, which permits only WPA3-supported devices to have access to its network. SAE provides security of perfect forwarding secrecy, even if an attacker gets hold of the transmitted packet and cannot decrypt the packet. The feature is beneficial to Hotspot and IoT Harkins (2012). SAE uses its Handshake negotiation process to generate dynamic hash keys unique to each authentication, instead of the same pre-shared key in Wi-Fi-protected old versions. The Authentication process takes place between stations (STA), devices that connect networks, and Access Points (AP).

WPA3-Enterprise

The enterprise mode supports multiple users that require an authentication server. This option is preferred for a large network, businesses, and institutions. WPA3-enterprise mode is compatible with CISCO Meraki and Aruba routers with the latest model. The WPA3-enterprise mode supports an additional key of 192 encryption keys.

The use of WPA3 on the Campus network will strengthen the security of the network because of its encryption features.

The introduction of a Virtual Private network tunnel would boost the security of the campus network. Virtual Private Network is a network security technology that secures an organization's network from unauthorized access by encrypting transmitted packets.

VPNs work on the Operating System level to reroute all traffic to other servers to ensure the anonymity of web users. It also masks the IP addresses of users, making it difficult for attackers to spy on web users. With a VPN encryption tunnel, an attacker cannot decrypt the traffic even when getting hold of transmitted traffic Powell(2010).

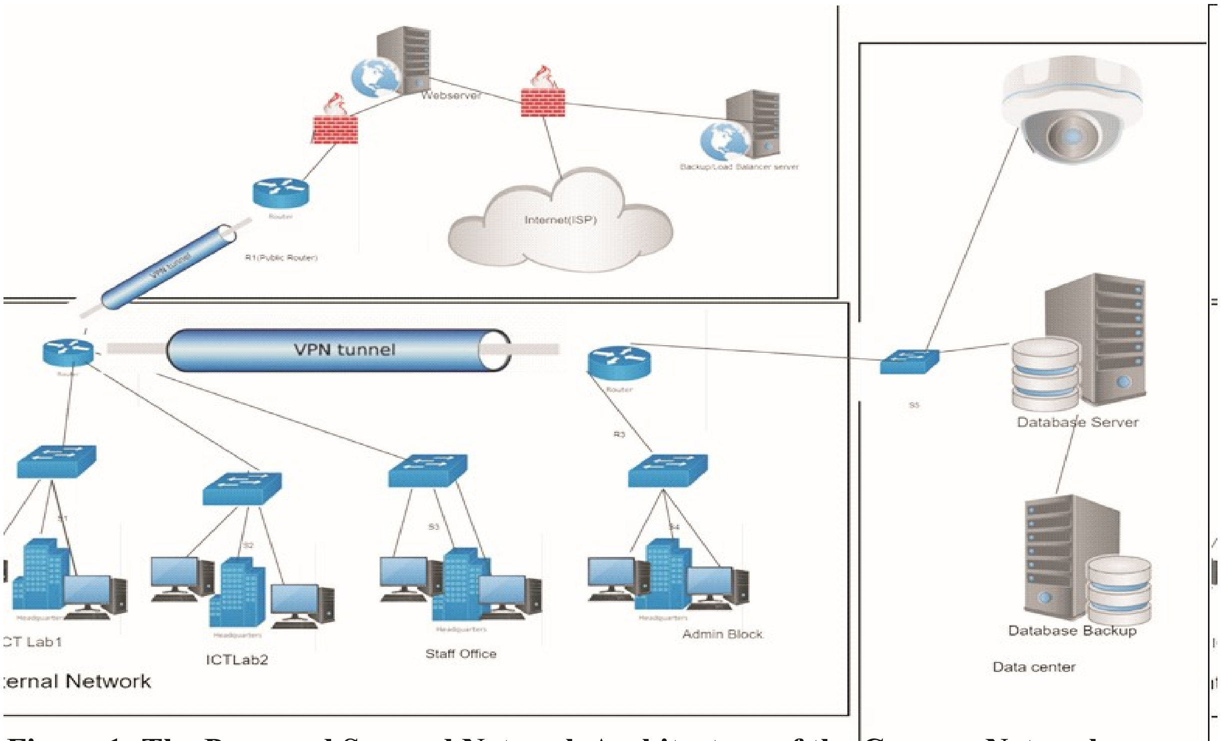

Figure 1: The Proposed Secured Network Architecture of the Campus Network

Implementation Schedule of the proposed system

Wi-Fi Implementation Plan would be of four phases according to (Access Agility online Publication, 2017): Requirement gathering, Wi-Fi site Design, Configuration, and installation, Service Turn up, and Acceptance.

Requirement Gathering

This section presents information needed for the implementation of the proposed System, which includes the existing network equipment, the coverage areas, and additional equipment for implementation of the proposed system.

On-site Design

This phase describes the design and coverage area of the network. It is required that the project supervisor, checks the areas or the access point in the network of the campus that the upgrade will take place. This includes the wiring if needed and the Access points to configure.

WPA3 configuration Procedure

The first step involves the installation of a CISCO router on the window operating System version 8 or 10, and enabling Wi-Fi Protected Access 3 Enterprise mode. The configuration follows this Procedure: Navigate to the wireless dashboard on the Router GUI

Choose "Enterprise with Radius server" Set Wi-Fi Protected Access encryption to "WPA3 only"Then add WLAN security features, which include the WPA3 192 Key encryption.

The next step is to configure the RADIUS server to allow VPN authentication, which ensures the best security practice on the Network. RADIUS Server uses RADIUS Extensible Authentication Protocol (EAP) to authenticate and manage user Requests on a central server.

VPN Configuration

To Implement VPN on RADIUS, the following are required in Windows Operating System (Window8 server or 10). The first step is to Install Network Policy Server (NPS), followed by configuration of RADIUS server for VPN Connections. The essence of a Network Policy Server is (NPS) for processing connection requests sent by the VPN server.

NPS does this by performing authentication to verify the user's identity, secondarily to authorize users with permission to connect and lastly to keep an accounting log on the connection path that users take. After the installation of the Network Policy Server on the Window operating system, the step involves the configuration of the RADIUS server with VPN security features. CISCO Meraki, online Publication 2022 update, presented the following procedures for the configuration of RADIUS Authentication with Client VPN.

The first step to the configuration is to install the Network Policy server on the window Operating system version 8 or higher. A Network Policy server is a security feature of a network server that manages the role and access feature of a network (Microsoft Window server Online Publication). NPS with Virtual Private Network will authenticate and verify user identity when connecting to the network and perform network log with the aid of the RADIUS server.

Service Turn-up and Acceptance.

This last phase requires the testing of the entire network to ensure its functionality and security strength. After which, training is conducted for network personnel for maintenance and management of the network, followed be documentation of the procedures.

System Justification.

Implementation the of the proposed system, (WPA3, VPN, and Backup servers,) will boost the security of a Campus Network. The combination of the RADIUS server of WPA3 Enterprise mode and VPN considered the best practice because of its user request management at the central server with RADIUS authenticator. The VPN feature will provide masking of the network ID to avoid the attraction of network intruders. Wi-Fi Protected Access 3(WPA3) provides users with; automatic hashing of the user authorization key, which makes password stuffing attacks difficult. The SAE (Simultaneous Authentication Equal) generates a dynamic unique key for each Authentication, making it difficult for hackers to sniff on the user's login detail. When an attacker gets hold of the passphrase, decryption is not easy. In addition, WPA3-enterprise mode supports multiple users and manages a large network that requires an authentication server.

Conclusion

The analysis of the present network security of the Campus Network identified the vulnerabilities inherent in WPA2. The proposed network, with its hybrid technologies (Wi-Fi Protected Access3, and Virtual Private Network) increases security with a reduction in attack risk on the Campus network and information assets. The Access log collected by Radius server, aid network Administrator to manage all user activities on the network in order to track unauthorized access or attempt.

Definition of terms

WPA2 (Wi-Fi Protected Access 2)**:** a wireless security protocol version 2 widely used in for wireless security.
WPA3 (Wi-Fi Protected Access 3): Wi-Fi security protocol version 3 newly launched by Wifi Alliance standard to counter vulnerabilities of WPA2
VPN (Virtual Private Network): Virtual Private Network is a network Security technology that secures organization's network from unauthorized accesses by encrypting transmitted packet
RADUIS (Remote Authentication Dial-In User Service)**: it is a** protocol that allows remote server communication with central server in order to authenticate users that request its services.
SAE (Simultaneous Authentication of Equals (SAE): new authentication method for 802.11 wireless standard.

Command- Line Interface (CLI): an interface that uses set of command inputted from keyboard to interact with a system. Mostly non-graphical user interface system such as MS-DOS.
GUI (Graphical User Interface): a graphical user-base environment that uses graphical pointer and menus and icons for interaction to the system.

NPS (Network Policy service): Network Policy and Access Services is a component of Windows Server 2008
SSID (Service Set Identifier): the name of your wireless network, also known as Network ID.
WLAN (*wireless Local Area Network*): is a wireless computer network that links two or more devices using wireless communication to form a local area network.

Advanced Encryption Standard (AES):symmetric block cipher that protect classified information.
SHA-256 (Secure Hash Algorithm 256-bit): used for cryptographic security.
Protected Management Frames (PMF):standard defined by WiFi Alliance to enhance WiFi connection safety.

Alliance Key Manager (AKM):This is a program that you install on a *Windows machine that communicates directly with the key server via a secure TLS session*.
MX-record (Mail eXchange-record): This system indicates to what specific IP address emails need to be sent.

References

Arjun,K., Mohammed,k.&Liava,E.(2017). Campus Area Network Wi-Fi Security. International journal of scientific & technology research volume 6, issue 07

Biasco,P.(2021). What is packet sniffing and how to prevent it. Privacy Bee. https://privacybee.com/blog/what-is-packet-sniffing/

Buczkowski,M.(2018). Wi-Fi Security Evolution. https://www.grandmetric.com/ended-wpa3-wi-fi-security-evolution/

EasyDemarc (2022). https://securityboulevard.com/2022/05/what-is-a-password-attack-in-cyber-security

Harkins D 2012. Simultaneous Authentication of Equals. IEEE. Retrieved from https://www.ieee802.org/11/

Huang, M., Luo, w., &Wan,X.(2019). Research on Network Security of Campus

Kawshik, K., &Sewal,N., (2018). Research Paper on Security of wireless network. Internal journal of current advanced Research NetworK.

Khani, P., Sharbaf,M.,Beheshti, M., &Faraji, S.,(2018). Campus network security threats, Analysis and strategy. Conference paper available. at https://www.researchgate.net/publication/338361469

Li, F. (2012). Study on Security and Prevention Strategies of Computer Network. International Conference on Computer Science and Information Processing (CSIP)

Loshen P.(2021): "RADIUS (Remote Authentication Dial-In User Service)":https://www.techtarget.com/searchsecurity/definition/RADIUS#:~:text=RADIUS%20(Remote%20Authentication%20Dial%2DIn%20User%20Service)%20is%20a,the%20requested%20system%20or%20service.

Lošonczi, P., Vacková,M., & Necas, P.,(2019). The Security of the WI-FI Networks in University Environment. https://www.researchgate.net/publication/337481293

Powell .M(2010): "The Impact of Vir The Impact of Virtual Priv tual Private Network (ate Network (VPN) on a Company VPN) on a Company's Network" https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1056&context=honors

Tao, M., Shaoquian, W., Minglian, L.,& Boa, z., W(2012). Strategy of building campus network security. Available at www.sciencedirect.com

Whitney, L.,(2020).How phishing attacks are targeting schools and colleges. https://www.techrepublic.com/article/how-phishing-attacks-are-targeting-schools-and-colleges/

Zheng,R., Ma,. H., Wang, Q., Fu, J. & Jiang, Z., (2021). Assessing the security of seven-campus network. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7795939/