Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Implementation of a RADIUS server for access control through authentication in wireless networks

Cristopher Alezander Ochoa Villanueva [1,*], Avid Roman-Gonzalez [2,3]

[1]*Electronics and Telecommunication Department, Universidad Nacional Tecnológica de Lima Sur, Lima, Peru*
[2]*Aerospace Sciences and Health Research Laboratory (INCAS-Lab), Universidad Nacional Tecnológica de Lima Sur, Lima, Peru*
[3]*Image Processing Research Laboratory (INTI-Lab), Universidad Nacional Tecnológica de Lima Su, Lima, Peru*

ARTICLE INFO

Article history:
Received 7 September 2022
Received in revised form
6 December 2022
Accepted 22 December 2022

Keywords:
Client-server
Vulnerabilities
NAS
Wireless security
RADIUS

ABSTRACT

In this study, a remote authentication dial in user service (RADIUS) server was implemented, which offers a wireless security method based on registering users authorized to use the network. For this, a computer with 4GB of RAM and a fourth-generation i3 processor was used, mounted on the Ubuntu Server 18.04 operating system and using the free RADIUS open-source software. This server was connected to the network through the TL-WR940N router using the AES encryption method and the WPA2 – Enterprise wireless security protocol, which allows a RADIUS server to authenticate wireless users. Evaluating this method with three registered users, two of them administrators, and one guest, and a total of 8 wireless devices, the experimental results showed that, for the five failed attempts to enter the network, the RADIUS server was able to identify them with an accuracy of 100% in real-time. In addition, the two administrators' correct identification and subsequent access were achieved; one used the same credential to have another device connected to the network, so an identified user can connect to more than one device without creating other credentials. Finally, this security method was compared to WPA2 Personal for 4 hours, where it was verified that the RADIUS server maintains a maximum of 3 devices connected, while the second method allowed the entry of any device, whether or not it was foreign to the network, showing that the RADIUS server is a robust method with great potential to protect wireless networks.

1. Introduction

Tests carried out in 2019 on access to wireless local network resources and control over the infrastructure in government, industrial, education, and telecommunications systems show that 88% contain critical vulnerabilities. Of these 63% are related to weaknesses in the password policy, 75% of the most common vulnerabilities are related to the use of known passwords, and 25% are related to the lack of authentication for access to resources (PTSC, 2019). Studies on cybersecurity in 2020 (Miloslavskaya, 2020; Saharkhizan et al., 2020) reveal that the two biggest threats detected in business networks are suspicious activities within them (97% of companies) and non-compliance with infrastructure security policies (94% of companies). Among the main suspicious activities, 64% of organizations suffer from hidden traffic (use of proxies or VPNs) and 33% from internal network scans. Regarding non-compliance with security policies, 81% of companies transfer sensitive data over an unencrypted network, 67% use remote access tools, 33% use weak passwords, and 6% have open networks (PTSC, 2020). The incidents in the first quarter of 2021 increased by 17% compared to the previous year, with 88% of the attacks going toward government institutions, industrial companies, and research and education institutions. The main reasons to attack these institutions are for obtaining personal data, credentials, and theft of intellectual property, in general, access to data (PTSC, 2021). In the Latin American framework, at the end of 2020, the main business security incidents are related to malicious code (34%), social engineering attacks (20%), and unauthorized access (16%). Companies in Brazil were the most affected with 19% of all detections, followed by Mexico at

* Corresponding Author.
Email Address: 2017100027@untels.edu.pe (C. A. Ochoa Villanueva)

https://doi.org/10.21833/ijaas.2023.03.022
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-5314-7909
2313-626X/© 2022 The Authors. Published by IASE.

17.5%, Argentina at 13.3%, Colombia at 10.6%, and Peru at 8.9% (ESET, 2021). These statistics show that the main disadvantage of wireless networks is the lack of security with which they are designed, evidenced by the entry of unauthorized users who can obtain confidential information from different entities.

In this paper, the implementation of the access control system using a remote authentication dial in user service (RADIUS) server for real-time authentication over wireless networks is developed.

In previous studies on access control in wireless networks, the WI-FAB mechanism was developed and focused on the encryption of the WPA2 key, its division into pieces, and the transmission of each fragment to the network. Users capable of reconstructing the information and decrypting the WPA2 key are those authorized to use the network (Pisa et al., 2016). Another mechanism used to combat rogue access point attacks is hardware fingerprinting, which remains constant over time but varies by device brand, model, and firmware. The fingerprints used were the power amplifier nonlinearity and the frame interval distribution fingerprints, which show an efficiency of 96.55% for the detection of unauthorized access points and a false alarm rate of 4.31% (Lin et al., 2020). Regarding security support in IoT environments, they used the TACACS+ protocol to reinforce the Restricted Application Protocol (CoAP) security to discover unknown IoT devices, supporting access control, authorization, and accounting. All this is implemented on a mobile phone as a client and a Raspberry Pi as a server. The results showed that such an approach is compatible with IoT devices (Khalil et al., 2020).

One of the limitations of this study is related to the software used to implement the server. Older versions of FreeRADIUS can only use PAP as the authentication method. This method does not encrypt text passwords and limits WiFi devices to be configured as TTLS or PAP, which is not compatible with specific Windows operating systems before version 10. Another limitation is scalability since, Conventionally, IMAP servers are used to store the user registry and are considered slow compared to others (Petrosyan et al., 2021). These limitations can be overcome by using updated versions of FreeRADIUS, which use more secure authentication methods, and servers based on LDAP or Bindable Authentication Modules (PAM), which offer faster storage methods using caching.

RADIUS is a network protocol that defines rules and conventions for communication between network devices for remote user authentication and accounting (Naman et al., 2020). It works on the Client-Server model, where the NAS (Network Attached Storage) devices function as RADIUS clients, being in charge of receiving the credentials of the designated users and sending them to the RADIUS server (Rigney et al., 2021). The RADIUS server is responsible for authenticating RADIUS client requests and authorizing registered users to enter the network (Feng, 2009). Both components have a shared secret key, which is exchanged so that the RADIUS server can correctly identify the client receiving the login requests (Park and Jung, 2017). The authentication and authorization process in RADIUS can be seen in Fig. 1.

In Fig. 2, one can see the proposed architecture for the present research.

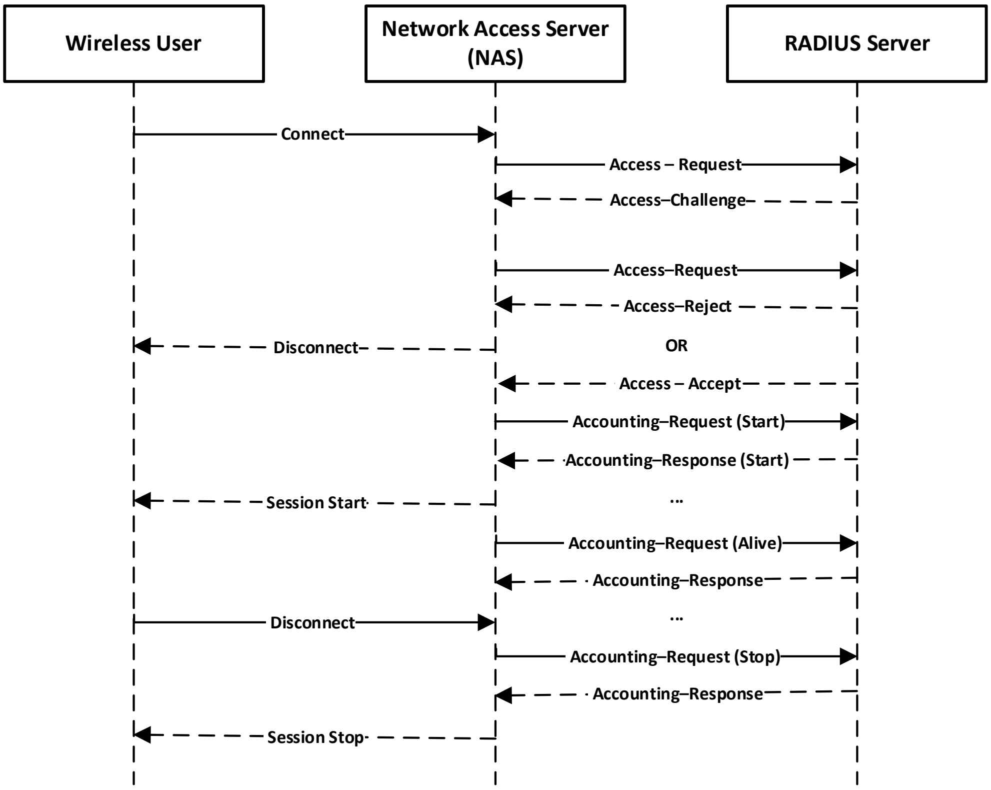


Fig. 1: Authentication and authorization process in RADIUS

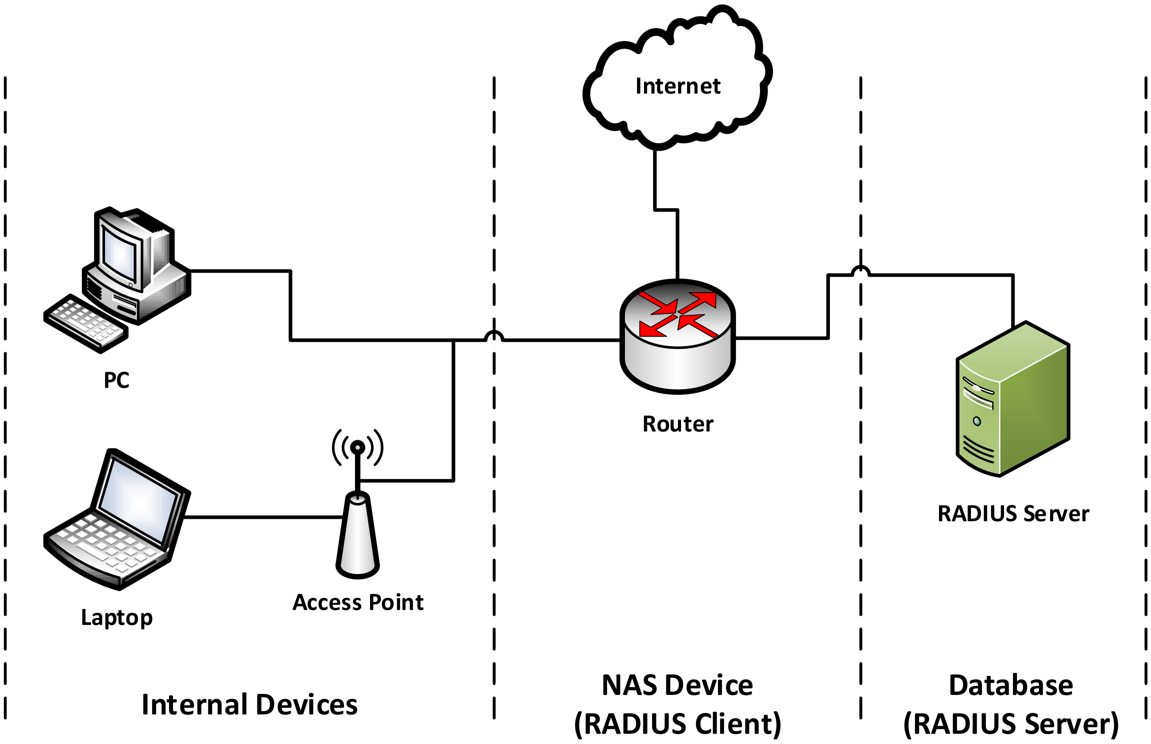


Fig. 2: Proposed network architecture

The document is organized as follows. Section II presents the methods and describes the experimental study. In section III, the experimental results obtained are presented. Finally, the discussion and conclusion are presented in the last two sections.

2. Methodology

2.1. Networks elements

For the research development, one will use FreeRADIUS and Ubuntu Server 18.04. FreeRADIUS software is a free open-source tool that allows us to implement a RADIUS server compatible with all AAA authentication protocols, maintaining components such as DHCP, BFD, and ARP, among others. This tool will be installed on the Ubuntu Server 18.04 operating system, a Linux distribution intended for server management. This OS only has a textual interface based on command lines, making it ideal for low-performance computers. On this distribution, one will store all the information of the RADIUS client and the end users, providing us with real-time information on the attempts to enter the network. Table 1 shows the characteristics of the server and wireless router used.

Table 1: Description of network elements

Element	Description
Server	- Processor: Intel Core i3-4130 3.40GHz - RAM: 4GB - Storage: SSD 240GB
Wireless Router	- Model: TL-WR940N - Working modes: Standard Wireless Router, Access Point, Repeater. - Security protocols: WEP, WPA/WPA2 personal and enterprise. - Services: DHCP, ARP, MAC Filter, etc.

2.2. Configuration of network elements

2.2.1. RADIUS server level

After installing FreeRADIUS on the Ubuntu server, one proceeds to configure the files that will allow us to identify the RADIUS client and register authorized users, as is shown in Fig. 3.

To identify the RADIUS client, one must remember that the client is in charge of receiving network connection requests; it will serve as a bridge between the user and the RADIUS server, so the latter must successfully recognize it. The validation of the client is given by employing its IP and a password that it must share with the RADIUS server in order for it to establish the authentication service.

This validation process is done by configuring the clients.conf file and add the device's IP that will act as the client, the shared password, and the recognition ID. This step can be seen in Fig. 4.

For the registration of users, one modifies the user's file and adds the ID and password of each final client that will be authorized to use the network (Fig. 5).

Finally, one must enable real-time authentication on both successful and failed attempts. This situation is achieved by modifying the radiusd.conf file, where authentication is disabled by default.

2.2.2. RADIUS client level (wireless router)

With the RADIUS server configuration complete, one will move on to configuring the wireless router to be recognized as the RADIUS client. To do this, we access the wireless router and assign the SSID to it so authorized users can recognize it.

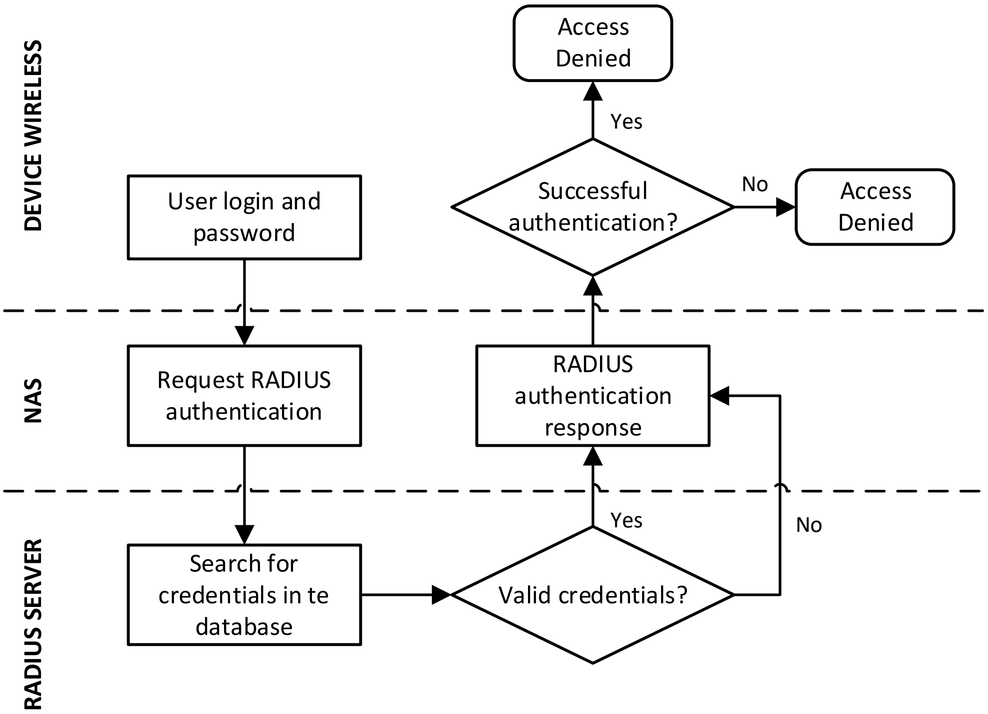
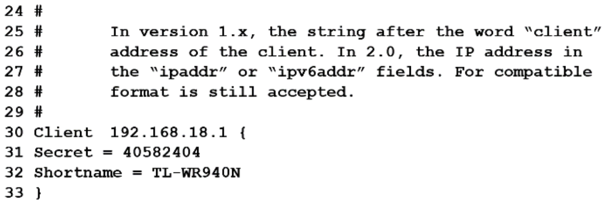
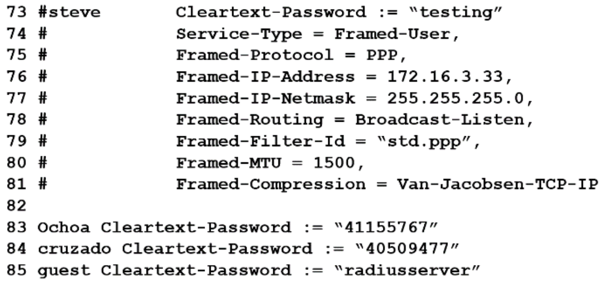

DEVICE WIRELESS
NAS
RADIUS SERVER
User login and password
Request RADIUS authentication
Search for credentials in te database
Valid credentials?
Yes
No
RADIUS authentication response
Successful authentication?
Yes
No
Access Denied
Access Denied

Fig. 3: Authentication process



```
#
#       In version 1.x, the string after the word "client"
#       address of the client. In 2.0, the IP address in
#       the "ipaddr" or "ipv6addr" fields. For compatible
#       format is still accepted.
#
Client  192.168.18.1 {
Secret = 40582404
Shortname = TL-WR940N
}
```

Fig. 4: RADIUS client configuration



```
#steve        Cleartext-Password := "testing"
#             Service-Type = Framed-User,
#             Framed-Protocol = PPP,
#             Framed-IP-Address = 172.16.3.33,
#             Framed-IP-Netmask = 255.255.255.0,
#             Framed-Routing = Broadcast-Listen,
#             Framed-Filter-Id = "std.ppp",
#             Framed-MTU = 1500,
#             Framed-Compression = Van-Jacobsen-TCP-IP

Ochoa Cleartext-Password := "41155767"
cruzado Cleartext-Password := "40509477"
guest Cleartext-Password := "radiusserver"
```

Fig. 5: Registration of authorized users

Finally, one changed the security protocol to WPA/WPA2 – Enterprise, and one put the IP of the RADIUS server and the shared password created when one declared the RADIUS client. One restarts the wireless router so that the changes are applied and, in this way, the authentication service through the RADIUS server is up and running.

3. Results

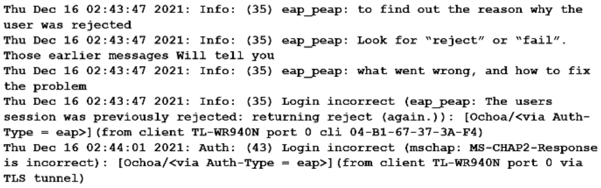
3.1. Authentication process

To test the operation of the RADIUS server, a smartphone was used that was connected to the RADIUS client using the previously registered ID and password. The authentication protocol inherited from the RADIUS server corresponds to MSCHAPv2, so one must select it, and, since one does not incorporate certificates for authorization, one put not validate. As soon as the device successfully enters the network in the RADIUS server, one will be able to see, in real-time, its successful authentication. The sudo tail -f /var/log/freeradius/redius.log command was used to observe the last lines of text, in real-time, of the radius.log file that contains the log of authentication requests from users trying to access the network.

3.2. Incorrect user detection

After testing, a total of 5 network access attempts were made using an administrator's credential with an incorrect password (Fig. 6); previously, real-time access request detection was enabled on the RADIUS server. Simultaneously with the connection, the RADIUS server was able to detect all 5 attempts, displaying the following information successfully:

- Username: Ochoa
- Authentication Type: EAP
- Client by which connected: TL-WR940N
- Encryption Path: TLS Tunnel

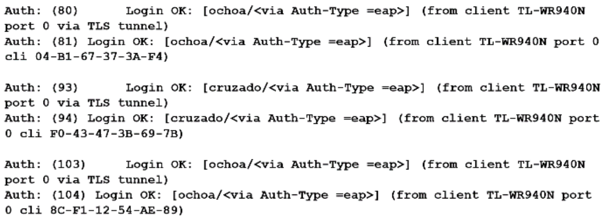


```
Thu Dec 16 02:43:47 2021: Info: (35) eap_peap: to find out the reason why the
user was rejected
Thu Dec 16 02:43:47 2021: Info: (35) eap_peap: Look for "reject" or "fail".
Those earlier messages Will tell you
Thu Dec 16 02:43:47 2021: Info: (35) eap_peap: what went wrong, and how to fix
the problem
Thu Dec 16 02:43:47 2021: Info: (35) Login incorrect (eap_peap: The users
session was previously rejected: returning reject (again.)): [Ochoa/<via Auth-
Type = eap>](from client TL-WR940N port 0 cli 04-B1-67-37-3A-F4)
Thu Dec 16 02:44:01 2021: Auth: (43) Login incorrect (mschap: MS-CHAP2-Response
is incorrect): [Ochoa/<via Auth-Type = eap>](from client TL-WR940N port 0 via
TLS tunnel)
```

Fig. 6: Verification of access attempts on the RADIUS server

3.3. Connecting multiple devices using a single user

The second test consisted of using a registered user's credentials to access another device on the network (Fig. 7). User "ochoa" was used to add the host with MAC address 04-B1-67-37-3A-F4, cataloged as the primary device, and later added to the device with MAC 8C-F1-12-54-AE-89, which is current as secondary. The RADIUS server successfully identified this second host, keeping both devices connected to the network.



```
Auth: (80)      Login OK: [ochoa/<via Auth-Type =eap>] (from client TL-WR940N
port 0 via TLS tunnel)
Auth: (81) Login OK: [ochoa/<via Auth-Type =eap>] (from client TL-WR940N port 0
cli 04-B1-67-37-3A-F4)

Auth: (93)      Login OK: [cruzado/<via Auth-Type =eap>] (from client TL-WR940N
port 0 via TLS tunnel)
Auth: (94) Login OK: [cruzado/<via Auth-Type =eap>] (from client TL-WR940N port
0 cli F0-43-47-3B-69-7B)

Auth: (103)     Login OK: [ochoa/<via Auth-Type =eap>] (from client TL-WR940N
port 0 via TLS tunnel)
Auth: (104) Login OK: [ochoa/<via Auth-Type =eap>] (from client TL-WR940N port
0 cli 8C-F1-12-54-AE-89)
```

Fig. 7: Entering two devices using a registered user

3.4. On-site test

After implementing the server and verifying its operation, a comparative test was carried out between the security method offered by the RADIUS Server in conjunction with WPA2 Enterprise and the WPA2 Personal method conventionally used for the protection of wireless networks. Each method was implemented for 4 hours during two days of regular office work. During each hour, the registry of the wireless users that were connected to the network was taken; the results of the test are shown in Fig. 8.

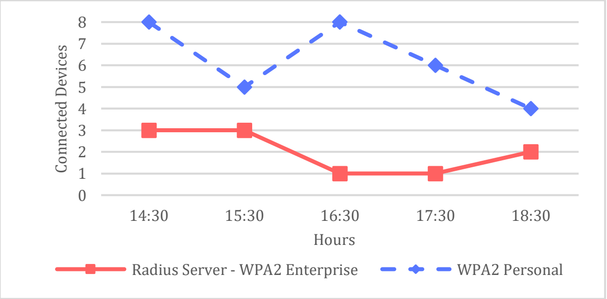


Fig. 8: Comparison of connected devices between the RADIUS server and WPA2 Personal

From this, it can be seen that, in the first two hours, the RADIUS server maintains a maximum of 3 devices (each with its respective user). During the next few hours, the number of connected devices varies between 1 and 2, corresponding to users registered on the server.

Simultaneously, the WPA2 Personal security method allows access to 8 devices. It is observed that the number of connected devices is above 4, including the three base users that should use the network. This situation means that the number of unauthorized devices in the study wireless network varies between 1, in the best cases, and 5.

Using the RADIUS server limits the number of devices that can be used on the network by registering users on the server. Additionally, foreign devices could be identified through the information provided by the real-time registration of the authentication service. In this way, it is demonstrated that the RADIUS server is a robust method that allows for providing security in wireless network environments.

4. Discussion

It was verified that the RADIUS server-based authentication method limits WiFi devices' entry into wireless networks. The correct identification of the RADIUS Client was verified employing IP and shared password, and the registration of users authorized to use the network. As demonstrated, it is possible to carry out continuous monitoring in real-time using the RADIUS server, obtaining information on each device and the number of attempts it makes to enter the network. The RADIUS server-based security method is very robust compared to WPA2 Personal, keeping only registered devices connected. Although the infrastructure used is considered simple (hosts, router, and server), the topology in companies is usually much more complex, and the scenarios are different from what we tested; for this reason, knowing the typical structure of the RADIUS authentication service allows us to identify what network elements perform the function of client or server. For the implementation, it is necessary to consider using a server that meets the minimum characteristics so that the service can work full-time. Therefore, we recommend that users who implement the RADIUS authentication service use devices that contain at least 2GB of RAM and mount it on a light operating system, the presence of a graphical interface are not necessary; the development can be done using the command line on any lightweight Linux distribution. In the future, we plan to implement this on a low-power server based on Raspberry Pi, supporting the authentication and authorization service and adding the Accounting service to create an account statement for each user, allowing the type of service to be known and provided to define various applications such as cost allocation and trend analysis.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

ESET (2021). Security report Latinoamérica 2021. ESET Software Company, Bratislava, Slovakia.

Feng J (2009). Design and implementation of RADIUS client based on finite state machine. In the Pacific-Asia Conference on Circuits, Communications and Systems, IEEE, Chengdu, China: 435-438. https://doi.org/10.1109/PACCS.2009.53

Khalil K, Elgazzar K, Abdelgawad A, and Bayoumi M (2020). A security approach for CoAP-based internet of things resource discovery. In the IEEE 6th World Forum on Internet of Things (WF-IoT), IEEE, New Orleans, USA: 1-6. https://doi.org/10.1109/WF-IoT48130.2020.9221153

Lin Y, Gao Y, Li B, and Dong W (2020). Accurate and robust rogue access point detection with client-agnostic wireless fingerprinting. In the IEEE International Conference on Pervasive Computing and Communications (PerCom), IEEE, Austin, USA: 1-10. https://doi.org/10.1109/PerCom45495.2020.9127375

Miloslavskaya N (2020). Security zone infrastructure for network security intelligence centers. Procedia Computer Science, 169: 51-56. https://doi.org/10.1016/j.procs.2020.02.113

Naman D, Abdulwahab M, and Ibrahim A (2020). RADIUS authentication on Unifi enterprise system controller using zero-handoff roaming in wireless communication. Journal of Applied Science and Technology Trends, 1(3): 118-124. https://doi.org/10.38094/jastt1427

Park J and Jung S (2017). Shared secret key update scheme between RADIUS server and access point using PUFs. In the 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), IEEE, Kuta Bali, Indonesia: 1-5. https://doi.org/10.1109/CAIPT.2017.8320725

Petrosyan AS, Petrosyan GS, Tadevosyan RN, and Arsalanian KK (2019). Identity infrastructure boost concept for eduroam service. Mathematical Problems of Computer Science, 52: 61-65. https://doi.org/10.51408/1963-0045

Pisa C, Caponi A, Dargahi T, Bianchi G, and Blefari-Melazzi N (2016). WI-FAB: Attribute-based WLAN access control, without pre-shared keys and backend infrastructures. In Proceedings of the 8th ACM International Workshop on Hot Topics in Planet-Scale Mobile Computing and Online Social Networking: 31-36. https://doi.org/10.1145/2944789.2949546

PTSC (2019). Penetration testing of corporate information systems: statistics and findings, 2019. Positive Technologies Software Company Moscow, Russia.

PTSC (2020). Top cybersecurity threats on enterprise networks. Positive Technologies Software Company Moscow, Russia.

PTSC (2021). Cybersecurity threatscape: Q1 2021. Positive Technologies Software Company Moscow, Russia.

Rigney C, Willens S, Rubens A, and Simpson W (2000). Remote authentication dial in user service (RADIUS) (No. rfc2865). https://doi.org/10.17487/rfc2865

Saharkhizan M, Azmoodeh A, Dehghantanha A, Choo KKR, and Parizi RM (2020). An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic. IEEE Internet of Things Journal, 7(9): 8852-8859. https://doi.org/10.1109/JIOT.2020.2996425