A Survey of 802.1X: Securing Network Access in the Modern Age

Vignesh Kumar S
Information Science and EngineeringRV College of Engineering
Bangalore, India
vigneshkumars1090@gmail.com

SG Raghavendra Prasad
Information Science and EngineeringRV College of Engineering
Bangalore, India
raghavendrap@rvce.edu.in

Abstract

The advent of wireless and wired net- works has revolutionized the way we communicate and access information, yet it has also introduced new security challenges. Among the various pro- tocols designed to mitigate these chal- lenges, 802.1X stands out as a corner- stone for securing network access. This paper presents a comprehensive survey of the 802.1X protocol, focusing on its role in modern networking, the types of Extensible Authentication Proto- col (EAP) methods it supports, and the security vulnerabilities and mitigation strategies associated with its implemen- tation. Through an examination of com- mon security vulnerabilities, such as de- nial of service (DoS) attacks, man-in-the- middle (MitM) attacks, and session hi- jacking, the paper highlights the importance of robust authentication mecha- nisms in safeguarding network integrity. Furthermore, the paper delves into real- world applications and case studies, il- lustrating the practical implications of 802.1X in securing critical infrastructure like silent clients. As technology contin- ues to evolve, the paper also explores fu- ture directions and research opportuni- ties, emphasizing the need for ongoing innovation to address emerging threats and leverage new technologies effec- tively. This survey serves as a valuable re- source for network administrators, secu- rity professionals, and researchers inter- ested in understanding the current state of 802.1X and its significance in securing network access in the modern age.

1. Introduction

In the rapidly evolving landscape of network technologies, securing network access has become paramount. With the proliferation of wireless local area networks (WLANs) and the increasing reliance on network connectivity, the need for robust security measures has never been more critical. Among the various protocols designed to enhance network security, 802.1X stands out as a foundational standard for secur- ing network access. This paper aims to delve into the background and importance of 802.1X in modern networking, highlighting its role in ad- dressing key security concerns associated with WLANs.

1.1 Background and Importance of 802.1X in Modern Networking

The emergence of 802.1X was a response to the growing security threats and risks associ- ated with network access. Initially, the absence of a comprehensive security protocol left net- works vulnerable to unauthorized access, net- work intrusion, data interception, and man-in- the-middle attacks. These vulnerabilities posed significant risks to data integrity and confidentiality, necessitating the development of a proto- col that could effectively mitigate these threats. 802.1X was designed to address these concerns by requiring devices to authenticate before gain- ing access to the network, thereby preventing unauthorized devices from participating in network communication. This authentication process not only secures the network against exter- nal threats but also allows for the enforcement of security policies based on the authentication status of devices, thereby enhancing the overall security posture of the network.

1.2 Overview of Wireless Local Area Networks (WLANs) and Their Security Concerns

Wireless Local Area Networks (WLANs) have revolutionized the way we access and share information, offering unparalleled convenience and mobility. However, the open nature of WLANs introduces unique security challenges, including unauthorized access, network intrusion, data interception, and the risk of rogue device connections. These challenges are exacerbated in environments with multiple access points or network ports, where the risk of an attacker exploit- ing vulnerabilities to gain unauthorized access is heightened. Moreover, the provision of guest access further complicates network security, as it requires mechanisms to control and secure guest access without compromising the integrity of the main corporate network.

The introduction of 802.1X has been instrumental in addressing these security concerns by providing a standardized method for authenticating and authorizing devices on WLANs. By requiring devices to authenticate before access- ing the network, 802.1X significantly reduces the risk of unauthorized access and network intru- sion. Additionally, its ability to dynamically as- sign VLANs based on authentication status al- lows for effective isolation of devices, further en- hancing network security.

As networks continue to evolve and become more complex, the need for robust security protocols like 802.1X remains critical. This paper will explore the various aspects of 802.1X, its implementation, and its impact on network secu- rity, providing a comprehensive overview of its role in securing network access in the modern age.

2 IEEE 802.1X Standard Overview

The IEEE 802.1X standard is a protocol for network port security, specifically designed to pre- vent unauthorized access to a LAN or WLAN. It operates by requiring devices (supplicants) to authenticate themselves before they can access the network. This authentication process en- sures that only authorized devices can commu- nicate over the network, thereby enhancing net- work security.

Key Components: Supplicant, Authenticator, and Authentication Server

- **Supplicant:** The device attempting to con- nect to the network. This could be a laptop, smartphone, or any other device capable of network communication.
- **Authenticator:** The network device (e.g., switch or access point) that controls access to the network. It is responsible for re- ceiving the authentication request from the supplicant and forwarding it to the authen-tication server.
- **Authentication Server:** A server that holds the credentials of authorized devices. It verifies the supplicant's identity and, upon successful authentication, sends an autho- rization message back to the authenticator, which then grants or denies network access.

Authentication Process and Message Sequence

The authentication process involves several steps, typically using the Extensible Authentica- tion Protocol (EAP):

- EAPOL-Start (Client -> Access Device): The client initiates the EAP authentication pro- cess by sending an EAPOL-Start message to the access device.
- EAP-Request/Identity (Access Device -> Client): The access device sends an EAP- Request message prompting the client for its identity.
- EAP-Response/Identity (Client -> Access Device): The client responds with an EAP- Response message containing its identity (e.g., username).
- RADIUS Access-Request (Access Device -> RADIUS Server): The access device forwards the EAP-Response/Identity message to the RADIUS server for authentication.
- RADIUS Access-Challenge (RADIUS Server -> Access Device): The RADIUS server sends an Access-Challenge message back to the access device. This challenge may contain additional authentication require- ments for the client (e.g., password).
- EAP-Request/MD5 Challenge (Access De- vice -> Client): The access device sends an EAP-Request message containing the RA- DIUS Access-Challenge to the client.

- EAP-Response/MD5 Challenge (Client -> Access Device): The client responds with an EAP-Response message containing its cre- dentials (e.g., encrypted password) to ad- dress the challenge.

- RADIUS Access-Request (Access Device -> RADIUS Server): The access device for- wards the EAP-Response/MD5 Challenge message to the RADIUS server.

- RADIUS Access-Accept (RADIUS Server -> Access Device): If the RADIUS server val- idates the client's credentials, it sends an Access-Accept message back to the access device.

- EAP-Success (Access Device -> Client): The access device sends an EAP-Success mes- sage to the client, indicating successful au-thentication.

- Handshake Request (Client -> Access De- vice) (Optional): The client may send a Handshake Request message to initiate additional communication (e.g., key ex-change).

- Handshake Response (Access Device -> Client) (Optional): The access device re- sponds with a Handshake Response mes- sage to complete the handshake.

- EAPOL-Logoff (Client -> Access Device): When the client disconnects from the net- work, it sends an EAPOL-Logoff message tothe access device.

- EAP-Failure (Access Device -> Client) (Op- tional): If the RADIUS server rejects the client's credentials or any other error oc- curs, the access device may send an EAP- Failure message to the client.

  In essence, the EAP authentication process in- volves the client and access device exchanging messages to prove the client's identity to the RA- DIUS server. If successful, the client is granted access to the network.

3 Types of 802.1x Protocols and its usecases

- **EAP-Transport Layer Security (EAP-TLS)** Provides mutual authentication between

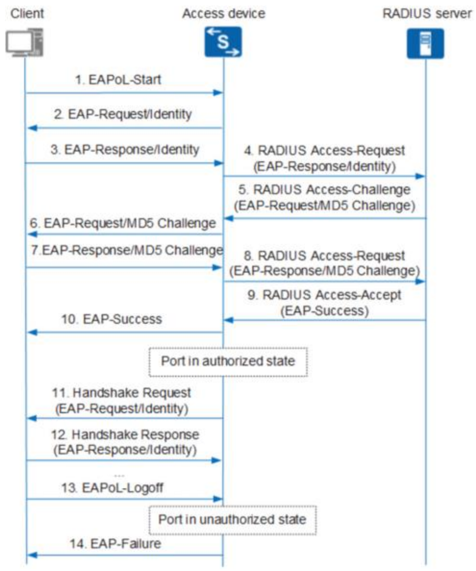

Figure 2.1: Sequence Diagram showing Dot1x authentication

the client and the server using TLS. It is con- sidered one of the most secure methods due to its use of SSL/TLS encryption. Ideal for environments requiring high levels of secu- rity, such as financial institutions or govern-ment agencies.

- **EAP-Protected Access Credential (EAP- PAE)** Offers mutual authentication using a pre-shared secret key. It is simpler to implement than EAP-TLS but less secure. Suitable for environments where simplicity and ease of deployment are prioritized overmaximum security.

- **EAP-Message Digest 5 (EAP-MD5)** Uses MD5 hashing for authentication. It is sus- ceptible to replay attacks due to the lack of a nonce. Best avoided in environments where security is a concern due to its vulnerabili-ties.

- **EAP-Subscriber Identity Module (EAP- SIM)** Utilizes SIM cards for authentication, similar to GSM networks. It is designed for mobile networks and IoT devices. Ideal for mobile networks and IoT devices that require authentication based on SIM cards.

- **EAP-Authentication and Key Agreement (EAP-AKA)** Similar to EAP-SIM but uses stronger encryption algorithms. It is com- monly used in 3GPP networks for mobile authentication. Best suited for mobile net- works and environments requiring strong encryption.

- **EAP-Tunneled Transport Layer Security (EAP-TTLS)** Allows EAP to be tunneled within a TLS session, providing mutual au- thentication. It is versatile and can support multiple EAP methods. Suitable for envi- ronments transitioning from unsecured to secured networks.

- **EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)** Designed to replace LEAP, offering better security and flexibil- ity. It uses a fast re-authentication mech- anism. Recommended for environments moving away from LEAP and requiring fastre-authentication.

- **EAP-Generic Token Card (EAP-GTC)** Uses token-based authentication, similar to smart cards. It is secure but requires physical tokens. Suitable for environments requiring strong authentication mech- anisms and where physical tokens are acceptable.

4 Security Vulnerabilities in 802.1X and Mitigation Strategies

The IEEE 802.1X standard, while a cornerstone in network security, is not immune to vulnera- bilities and attacks. Understanding these vulner- abilities is crucial for implementing effective se- curity measures and mitigating potential threats.

4.1 Common Security Vulnerabilities in802.1X

- **Masquerading and Malicious Access Points (APs):**The plaintext MAC addresses used in wireless communications can be intercepted by adversaries, who can then masquerade as any wireless station or AP by spoofing their MAC addresses. This allows attackers to intercept, modify, or inject packets into the network, compromising data integrity and confidentiality.
- **Session Hijacking:** After successful authen- tication, an adversary can hijack a ses- sion by disconnecting a device and mas- querading as it to establish new connec- tions. This attack can bypass authentication mechanisms unless robust data con- fidentiality and integrity protocols are in place.

- **Man-in-the-Middle (MitM) Attacks:** In these attacks, the adversary intercepts and possibly alters the communication between two parties without their knowledge. To execute a MitM attack, the adversary must first break the connection between the le- gitimate station and the AP, then masquer- ade as both the station and the AP to fool the other party into communicating with them. This attack undermines the trust be- tween the communicating parties.

- **Denial-of-Service (DoS) Attacks:** WLAN systems are susceptible to DoS attacks, which can render the entire Basic Service Set (BSS) unavailable or disrupt connec- tions between legitimate peers. Adversaries can launch DoS attacks by forging man- agement frames, exploiting protocol weak- nesses, or jamming the frequency band. These attacks aim to degrade the availabil- ity of the network service.

4.2 Mitigation Strategies and Countermeasures

Use of 802.1X for Wired and Wireless Networks: Applying 802.1X authentication to both wired and wireless networks ensures that all devices at- tempting to connect to the network are strongly authenticated. This prevents unauthorized de- vices from becoming insecure backdoors.

Secure Configuration of Authorized Access Points: Organizations must ensure that all au- thorized wireless access points are securely con- figured. Changing default settings, which are well- known and can be exploited by attackers, is crucial for enhancing network security

Elimination of Rogue Access Points: Using 802.1X on the wired network to authenticate all devices plugged into the network can prevent unauthorized devices from connecting to the network, thus eliminating the threat of rogue ac- cess points.

Securing Wireless Client Devices: Protecting wireless client devices from loss, theft, and com- promise is essential. This includes implement- ing strong authentication and encryption mech- anisms on the devices themselves, as well as se- curing the data stored on them .

Encryption of Wireless Communications: Encrypting communications over the wireless network is the most effective way to secure the network from intruders. Most wireless routers, access points, and base stations have built-in en- cryption mechanisms that should be enabled.

4.3 Addressing Security Vulnerabilities in802.1X

User-Based Authentication: Ensuring that au- thentication is based on individual user creden- tials rather than just device identification helps in preventing unauthorized access.

Dynamic Cryptographic Keys: Generating dynamic, per-session, and per-user crypto- graphic keys enhances security by limiting the window of opportunity for attackers to exploit static keys .

Stronger Cryptographic Algorithms: Moving away from weaker algorithms like RC4 towards stronger ones, such as those based on AES, improves the resilience of the network against cryptographic attacks .

Message Integrity Checks: Implementing strong message integrity checks protects mes- sages in transit from tampering, ensuring the integrity of the data being transmitted .

5 Silent Clients: A Challenge to Network Security

In today's interconnected world, network secu- rity is paramount, especially in environments where unauthorized access can lead to sig- nificant disruptions. One emerging challenge in network security is the presence of "silent" clients—devices that do not actively participate in the 802.1X authentication process, potentially bypassing security measures. Silent clients can compromise the integrity of the network, expos- ing it to unauthorized access and potential secu- rity breaches.

5.1 Proactive Solution: Engaging SilentClients

To counteract the threat posed by silent clients, a proactive solution was developed, involving three key steps: detection, storage, and en- gagement. First, network monitoring tools are utilized to identify devices that do not initiate the 802.1X authentication process. Detected silent clients are then stored in a remote server database, including their MAC addresses and other relevant network identifiers. Finally, periodic probes are initiated towards these clients to encourage them to participate in the 802.1X authentication process, thereby ensuring compliance with network security policies. This ap-

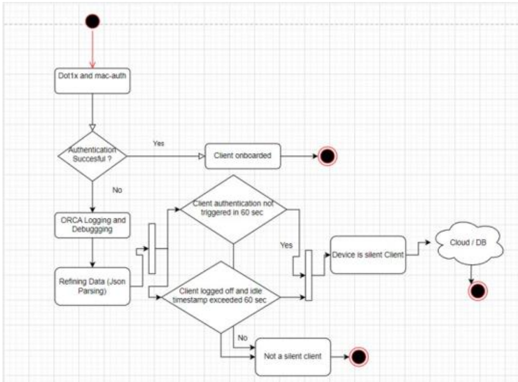

Figure 5.1: Activity Diagram for detecting silent clients

proach not only helps in identifying previously silent clients but also ensures that they are en- gaged in the authentication process, enhancing the overall security posture of the network.

6 Conclusion

The exploration of silent clients and their impact on network security, particularly in the context of the 802.1X protocol, underscores the evolv- ing landscape of cybersecurity challenges. Silent clients represent a unique threat to network security, capable of bypassing traditional au- thentication mechanisms and potentially gain- ing unauthorized access to network resources. The case studies and real-world applications of 802.1X, coupled with the innovative solutions aimed at detecting and engaging silent clients, highlight the dynamic nature of network security threats and the necessity for proactive, adaptivesecurity measures.

The 802.1X protocol, while foundational in providing secure network access, faces new challenges as network architectures evolve and cyber threats become increasingly sophisticated. The ongoing development and refinement of 802.1X, alongside advancements in network monitoring and analysis tools, are crucial for maintaining network security in the face of these challenges.

7 Future Scope

As networks become more complex and reliant on secure access, the demand for enhanced authentication mechanisms grows. This in- cludes the adoption of multi-factor authentica- tion (MFA) and biometric verification, which of- fer higher levels of security by requiring users to prove their identity through multiple means. Furthermore, the integration of artificial intelli- gence (AI) and machine learning (ML) technolo- gies promises to revolutionize network security, enabling real-time anomaly detection and pre- dictive analytics. These technologies can iden- tify and respond to security threats before they materialize, significantly reducing the risk of breaches. Secure device management is an- other area ripe for innovation, with develop- ments aimed at detecting and engaging silent clients to ensure all devices on the network com- ply with security policies. Standardization and compliance efforts will continue to play a cru- cial role, ensuring that network security proto- cols and practices are universally recognized and adhered to. Lastly, user education and aware- ness campaigns will become increasingly impor- tant, as they empower individuals to understand and follow best practices for network security, including the dangers posed by silent clients. To- gether, these advancements promise to shape the future of 802.1X and network security, ensur- ing that networks remain secure and resilient inthe face of evolving threats.

References

[1] Kachhara, Shaleen Anil Kumar, Kakelli. (2018). Implementation of IEEE 802.1X Port-based Authentication Mechanism for Ethernet. International Journal of Com- puter Trends and Technology. 64. 17-23.10.14445/22312803/IJCTT-V64P105.

[2] "IEEE Standard for Local and Metropolitan Area Networks–Port-Based Network Access Control," in IEEE Std 802.1X-2020 (Revision of IEEE Std 802.1X-2010 Incorporating IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck- 2018) , vol., no., pp.1-289, 28 Feb. 2020, doi: 10.1109/IEEESTD.2020.9018454.

[3] I. V. Araújo, S. R. Lima and A. D. Brízido, "IEEE 802.1X Virtual Network Function Development for NG-PON Architecture," 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2022, pp. 1-6, doi: 10.23919/Soft-COM55329.2022.9911396.

[4] Jabbar, A Ayoub, Harith. (2014). Analy- sis and Implementation of the Authentica- tion Protocol 802.1x. International Journal of Computer Applications. 87.

[5] Cisco, "OpenFlow," in Consolidated Plat- form Configuration Guide, Cisco IOS Re- lease 15.2(5)E (Catalyst 2960-X Switches), 2017.

[6] B. Shojaie, I. Saberi, and M. Salleh, "En- hancing EAP-TLS authentication protocol for IEEE 802.11i," Wireless Networks, 2017

[7] A. E. Maslov, S. L. Katuntsev, and A. A. Maliavko, "Study and implementa- tion of authentication mechanism by RADIUS-server in switches and routers using NETCONF protocol," in Interna- tional Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices, EDM, 2017.

[8] K. W. Kim, Y. H. Han, and S. G. Min, "An Au- thentication and Key Management Mecha- nism for Resource Constrained Devices in IEEE 802.11-based IoT Access Networks," Sensors (Switzerland), 2017.

[9] C. Rigney, A. Rubens,W. Simpson and S.Willens. RFC 2865: Remote Authentica- tion Dial In User Service (RADIUS).

[10] Cisco, "Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(25)EW - Understanding and Con- figuring VLANs [Cisco Catalyst 4500 Series Switches] - Cisco," February 15, 2018, 2018.

[11] YongYu, Qun Wang, Van Jiang, "Research on Security of the WLAN Campus Network" International Conference on E-Health Net- working, Digital Ecosystems and Technolo-gies, 2010.

[12] M. Hasbullah Mazlan, Sharifah H.S. Ar- iffin, Mohammed Balfaqih, S.Norhaizum M.Hasnan, Shariq Haseeb, "Latency eval- uation ofauthentication protocols incen- tralized 802.11 architecture", Universiti Teknologi Malaysia (UTM), 2012

[13] Snehasish Parhi, "Attacks Due to Flaw of Protocols Used In Network Access Control (NAC) ", Their Solutions and Issues: A Sur- vey, I. J. Computer Network and Informa- tion Security, 2012

[14] Alexandra Chiornita, Laura Gheorghe, Daniel Rosner, "A Practical Analysis of EAP Authentication

Methods, Faculty of Automatic Control and Computers", IEEE International Conference ,2010

[15] IEEE Standards, "IEEE Standard for Local and Metropolitan Area Networks - Port-Based Network Access Control", 2010

[16] Snehasish Parhi, "Attacks Due to Flaw of Protocols Used In Network Access Control (NAC) ", Their Solutions and Issues: A Sur- vey, I. J. Computer Network and Informa- tion Security, 2012.

[17] M. Hasbullah Mazlan, Sharifah H.S. Ar- iffin, Mohammed Balfaqih, S.Norhaizum M.Hasnan, Shariq Haseeb, "Latency eval- uation ofauthentication protocols incen- tralized 802.11 architecture", Universiti Teknologi Malaysia (UTM), 2012

[18] YongYu, Qun Wang, Van Jiang, "Research on Security of the WLAN Campus Network" International Conference on E-Health Net- working, Digital Ecosystems and Technolo-gies, 2010.