Authentication Protocol Risk Scoring: A Classification Approach

Rania BLIBEK, Yasmine ZAHEM, Jiahui XIANG, Osman SALEM and Ahmed MEHAOUA
Centre Borelli UMR 9010
Université Paris Cité
Paris, France
firstname.lastname@u-paris.fr

***Abstract*—Abstract — Authentication is a fundamental component of cybersecurity, responsible for verifying the identity of users and devices before granting access to critical resources. Despite its importance, many widely adopted authentication protocols continue to exhibit significant security flaws. This paper presents a risk-based analysis of commonly used protocols, including PAP, CHAP, RADIUS, LDAP, and modern multi-factor authentication systems.**

Using public vulnerability data (CVEs, CVSS scores, and CWE classifications), we propose a classification model that evaluates each protocol based on the severity and nature of its known weaknesses. Our findings highlight recurring vulnerabilities such as unencrypted credential transmission, weak cryptographic practices, and susceptibility to replay and impersonation attacks.

The study also discusses evolving approaches for improving authentication security, including the adoption of robust encryption standards, biometric verification, and AI-driven anomaly detection. Ultimately, this work aims to guide organizations in making informed decisions about protocol selection and to promote a more resilient and adaptive authentication infrastructure.

***Index Terms*—Authentication protocols, network security, vulnerabilities, cryptography.**

I. Introduction

As digital technologies become increasingly embedded in our daily lives, the protection of networked systems and digital infrastructures is more critical than ever. Among the foundational elements of cybersecurity, authentication protocols play a central role: they verify the identity of users, devices, and services, and govern access to sensitive data and resources.

Despite their importance, many widely used authentication protocols—particularly legacy ones such as PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol)—are still vulnerable to attacks. PAP sends credentials in cleartext, making it susceptible to interception, while CHAP remains exposed to brute-force and hash-recovery techniques. These weaknesses open the door to unauthorized access, impersonation, and manipulation of data exchanges.

The introduction of modern techniques such as Multi-Factor Authentication (MFA) has improved resilience by requiring multiple forms of identity verification. However, these systems also come with new challenges, including increased complexity, synchronization issues, and privacy concerns related to biometric or token-based data.

To address the need for a clearer understanding and prioritization of these vulnerabilities, we propose a risk-based classification model. It combines data from public vulnerability databases—specifically CVSS (Common Vulnerability Scoring System) and CWE (Common Weakness Enumeration)—to produce a composite risk score for each protocol. Unlike traditional models that focus on a single metric, ours incorporates both severity and structural flaw type, offering a more complete evaluation of each protocol's real-world risk.

This paper is organized as follows: Section II reviews existing literature on authentication vulnerabilities. Section III introduces our methodology and scoring model. Section IV discusses the results across several protocols, and Section V concludes with recommendations for improving authentication security in practice.

II. Related Work

Authentication plays a crucial role in network security, ensuring that only legitimate users can access systems and services. Numerous studies have focused on authentication protocols, whether simple, centralized, scalable, or based on multifactor mechanisms. The following diagram illustrates the interaction between the user, the service provider, and the identity provider, showcasing the authentication and identity verification process in a federated authentication system.

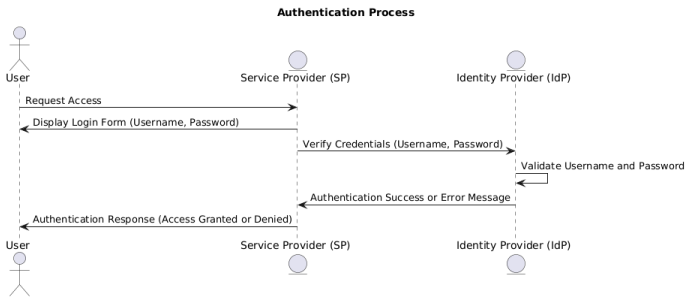

Fig. 1. Authentication Process Diagram

Numerous studies have examined in depth the security, performance,,, and scalability of authentication protocols, whether simple, centralized, decentralized, or multifactor. This section presents a critical overview of the main approaches described

in the literature, highlighting the trade-offs between security, ease of deployment, and compatibility with existing infrastructures.

A. Password Authentication Protocol (PAP)

The Password Authentication Protocol (PAP) is an authentication protocol that transmits credentials (username and password) to the authenticator in clear text, without encryption. Although it is one of the oldest protocols for packet verification in communication systems, PAP presents major vulnerabilities. It uses a two-step handshake, in which the user sends his or her credentials at the start of the connection. However, the absence of encryption makes this protocol vulnerable to eavesdropping and man-in-the-middle (MITM) attacks, where an attacker can intercept data packets to retrieve the user's credentials. Another important vulnerability of PAP is its susceptibility to replay attacks. Since information is sent in clear text, an attacker can capture and replay authentication packets in an attempt to log in using the same credentials. Because of these weaknesses, PAP is no longer recommended in sensitive environments where data security is essential.

However, PAP remains compatible with many servers and operating systems, and can still be used in remote access environments where additional security mechanisms (such as network layer encryption) are in place.[1]

B. Challenge Handshake Authentication Protocol (CHAP)

The Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol based on a three-stage challenge-response mechanism. When a server sends a challenge to a client in the form of a random character string, the client uses this string and its password to calculate an MD5 hash, which it sends back to the server. The server performs the same operation and compares the two results. If the hashes match, authentication is successful.

Although CHAP improves security over PAP by avoiding the sending of clear text passwords, it also presents vulnerabilities. The MD5 hash used by CHAP may be vulnerable to brute-force attacks, particularly if an attacker manages to capture the challenge and response, and then test possible passwords. Furthermore, although CHAP prevents replay attacks by varying the challenge at each authentication, it is not invulnerable to brute force or dictionary attacks if the chosen password is weak.

CHAP is still widely used, but more secure protocols such as EAP-TLS are now preferred in environments requiring a higher level of security. [1]

C. Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

The Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is a variant of CHAP, which encrypts password information before transmitting it via a PPP (Point-to-Point Protocol) link, using MD5 encryption. MS-CHAPv2, the most common version, supports bidirectional authentication, enabling the identity of both parties to the connection to be verified. This protocol generates separate keys for each session, offering a higher level of security than MS-CHAPv1.

However, despite these improvements, MS-CHAPv2 still presents significant vulnerabilities, notably due to the inherent weakness of MD5 encryption. Studies have demonstrated that dictionary or brute-force attacks can successfully break MD5 hashes, allowing attackers to recover user passwords. Additionally, vulnerabilities have been identified in the protocol's mutual authentication process, enabling potential man-in-the-middle attacks under certain conditions.

Because of these vulnerabilities, Microsoft recommends the use of more secure protocols, such as EAP-TLS, for environments requiring a high level of security.[1]

D. Extensible Authentication Protocol (EAP)

The Extensible Authentication Protocol (EAP) was designed to meet the growing security needs of mobile users, particularly with the widespread use of PPP and remote connections. To enhance security, systems have integrated mechanisms such as challenge authentication, PPP message encryption, and key distribution via the RADIUS protocol.

EAP provides a flexible framework for transporting different authentication methods, regardless of their complexity. It is based on a simple message format consisting of four types: Request, Response, Success and Failure.

Each method is identified by a number:[2]
Type 1: EAP-Identity (user identification),
Type 4: EAP-MD5 (challenge authentication),
Type 13: EAP-TLS (authentication via TLS),
Type 18: EAP-SIM (via SIM card),
Type 26: EAP-MSCHAPv2 (Windows environments).

An EAP session begins with an identity request (EAP-Request.Identity), followed by an exchange of messages according to the selected method. It ends with a success or failure response.

Despite its flexibility, EAP does present certain vulnerabilities, particularly with regard to denial-of-service attacks: an attacker can interrupt a session by sending a false EAP-Failure message. However, they cannot access the encryption keys, which are protected by robust cryptographic mechanisms.[3]

E. Centralized protocols: a solution for distributed environments

Centralized authentication protocols such as RADIUS and TACACS+ are widely used to simplify access management in distributed architectures. By externalizing authentication decisions to dedicated servers, they enable centralized control of identities and access rights, particularly suited to large-scale enterprise environments.

Despite their similar functions, RADIUS and TACACS+ differ considerably in terms of security. RADIUS encrypts only passwords in communications, which can leave other sensitive data exposed to interception attacks[4]. In contrast, TACACS+ encrypts all exchanges between client and server, offering more comprehensive protection against sniffing or Man-in-the-Middle attacks. This makes it a preferred choice in environments where confidentiality of exchanges is essential.

F. Strong authentication and TOTP/HOTP mechanisms

Faced with an upsurge in targeted attacks, security systems have turned to strong authentication, notably via multi-factor authentication (MFA). This is based on the combined use of several independent identity factors: something the user knows (password), possesses (smartphone, token), or embodies (biometrics). This combination makes identity theft by a malicious third party much more difficult.[5]

Among the most widely used mechanisms in this context are the TOTP (Time-based One-Time Password) and HOTP (HMAC-based One-Time Password) protocols.

TOTP generates a temporary password based on the current time, generally valid for 30 seconds, thus limiting the risk of interception or reuse.

HOTP, on the other hand, is based on an incremental counter. It is useful in contexts where time synchronization is difficult to guarantee, such as in certain industrial or low-connectivity environments. However, it is vulnerable to desynchronization, which can block legitimate access or, on the contrary, weaken security if the system accepts a wide tolerance window. Despite their effectiveness, these mechanisms are not free of flaws:

They remain vulnerable to phishing attacks, where users are tricked into entering their one-time password on a fake site.

Malware can intercept OTPs on compromised terminals, particularly poorly secured smartphones.

And, in the case of poorly managed synchronization between server and client, replay attacks are still possible, especially with HOTP.

More recently, work has been done to reinforce these approaches with the Moving Target Defense (MTD) concept[6]. For example, the TOTP protocol is used to dynamically synchronize sensitive network parameters, such as access ports or communication paths. The aim is to disrupt automated or directed attacks, by regularly modifying the "attack surface". However, even this strategy has its limitations:

It complicates network management and requires strict synchronization between devices.

It can lead to availability problems if a legitimate user is not perfectly synchronized with the system.

And it does not totally prevent attacks if the attacker has local or already intrusive access to the system.

G. LDAP (Lightweight Directory Access Protocol) and its vulnerabilities

LDAP is a protocol used to manage and access authentication information in a centralized directory. Although it is widely used for authentication and identity management in enterprise environments, it presents a number of vulnerabilities.

Main LDAP vulnerabilities:[7] Clear text transmission: By default, LDAP sends sensitive information (such as passwords) in clear text. This exposes data to interception, unless secure versions such as LDAPS (LDAP over SSL/TLS) are used.

Man-in-the-Middle (MITM) attacks: The absence of encryption in conventional exchanges exposes LDAP to MITM attacks, where an attacker can intercept and alter the data exchanged.

LDAP injection: Like SQL injections, poorly validated LDAP queries can be manipulated by attackers, compromising directory security.

Denial of Service (DoS): LDAP can be targeted by DoS attacks aimed at overloading the server and making authentication unavailable.

With the evolution of threats and cybersecurity requirements, new authentication protocols have emerged, aimed at correcting the shortcomings of traditional solutions. Among them, WebAuthn, developed by the W3C and FIDO Alliance, enables password-less authentication based on robust cryptographic methods and the use of physical devices such as security keys.Finally, Passwordless Authentication approaches are gaining in popularity, eliminating dependence on passwords altogether by favoring biometric or trusted device authentication.

Real-world incidents continue to demonstrate the limitations of traditional authentication protocols. For example, a sophisticated breach of RSA's SecurID token system exposed numerous corporate accounts. Insecure LDAP implementations have also been exploited, particularly in university and healthcare environments, leading to the exposure of thousands of sensitive credentials. Additionally, weaknesses in MS-CHAPv2 have been successfully leveraged by researchers to compromise VPN sessions using GPU-assisted brute-force attacks.

The following table provides an overview of common protocols and their main security vulnerabilities. This information enables you to quickly identify the most vulnerable protocols and assess the risks associated with their use in different network environments.

Protocol	**Main Vulnerability**
PAP	Clear text transmission, interception, replay
CHAP	Brute-force on MD5, dictionary attack
MS-CHAPv2	Brute-force MD5, Man-in-the-Middle (MITM)
EAP	Denial-of-service (DoS) attacks
RADIUS	Partial encryption, exposure of metadata
TACACS+	Misconfiguration
TOTP	Phishing, OTP code interception
HOTP	Desynchronization, replay risk
LDAP (non-secured)	Clear text transmission, LDAP injection, MITM

TABLE I
PROTOCOL VULNERABILITIES

III. METHODOLOGY

To evaluate the security of commonly used authentication protocols, we developed a classification model based on publicly documented vulnerabilities. This model combines multiple sources of vulnerability data—CVE (Common Vulnerabilities and Exposures), CVSS (Common Vulnerability Scoring System), and CWE (Common Weakness Enumeration)—to quantify and compare the relative risk of different protocols. The following steps describe the analysis process in detail.

A. Vulnerability Collection

The first step in our methodology consisted of collecting known vulnerabilities associated with each authentication protocol. We began by identifying commonly used software and systems that implement the studied protocols (e.g., PAP, CHAP, RADIUS, LDAP). Then, for each protocol, we retrieved all related CVEs from public vulnerability databases. This data acquisition step ensures that our analysis is based on empirical evidence and reflects real-world risks.

Justification: By relying on official vulnerability repositories such as NIST's NVD and MITRE's CVE database, we ensured objectivity and comprehensiveness in our dataset. This approach also allows reproducibility and future updates.

B. Attribute Extraction

For each identified CVE, we extracted a set of descriptive and quantitative attributes. These included the CVSS base score (measuring severity), the CWE classification (indicating the nature of the weakness), the year of publication, and the scope of impact (confidentiality, integrity, availability).

Justification: These attributes offer both technical and contextual insights. The CVSS score quantifies how dangerous a vulnerability is, while CWEs help group similar types of weaknesses. The year of publication reveals the temporal evolution of risk exposure, and the impact scope highlights the nature of potential damage.

C. CWE Grouping

In order to make the data more manageable and meaningful, we grouped CWEs into broader categories of vulnerability types. These included: memory safety violations, injection flaws, authentication issues, data exposure, cryptographic weaknesses, and configuration errors.

Justification: Grouping CWEs into general categories simplifies interpretation and allows for cross-protocol comparison. This categorization also helps identify structural weaknesses common to multiple protocols, guiding targeted mitigation strategies.

D. Vulnerability Score Calculation

We calculated a global vulnerability score V for each protocol using the formula:

$$V = \alpha \cdot S + \beta \cdot C$$

Where S is the average CVSS severity score for the protocol and C is the proportion of critical CWEs among its vulnerabilities. The weighting coefficients were set to $\alpha = 0.7$ and $\beta = 0.3$, emphasizing severity while still considering the concentration of critical flaws.

Justification: This formula offers a balanced view of both the intensity and the nature of the vulnerabilities. By assigning greater weight to CVSS severity, we prioritize real-world exploitability, while the inclusion of CWE criticality provides a qualitative dimension.

E. Risk Level Classification

Based on the calculated vulnerability score V, each protocol was assigned to a risk category:

$$\text{Critical if } V \geq 8, \quad \text{Moderate if } 5 \leq V < 8, \quad \text{Low if } V < 5$$

Justification: This classification enables security professionals to prioritize their focus on higher-risk protocols. It also provides a simplified, actionable output from the model, facilitating integration into decision-making processes for protocol selection or system hardening.

IV. Experimental Results

Based on the methodology described in the previous section, we conducted experiments to evaluate the security of different authentication protocols. This section presents the results of our analysis, focusing on the vulnerability scores of the protocols studied. By applying the classification model, we were able to identify critical vulnerabilities and determine the level of risk associated with each protocol.

As part of our analysis, we produced detailed presentations for each product studied, to examine the number of vulnerabilities associated with each authentication technology. For each product, we extracted and presented the relevant data, enabling us to visualize the impact of vulnerabilities according to the specific characteristics of each product.

In addition, we also presented the evolution of the number of vulnerabilities over the years, by analyzing temporal trends. This has enabled us to observe the evolution of authentication protocol security, and to better understand the periods when major vulnerabilities were identified, as well as the impact of updates and fixes on security over time.

Vulnerability analysis has enabled us to gain a better understanding of the evolution of risks associated with authentication protocols. To this end, we have used several visualizations, which we present below to illustrate the results obtained.

Firstly,fig: Number of vulnerabilities listed by year shows the evolution of the number of vulnerabilities identified each year. We can see a steady progression until 2017, a year marked by a significant peak, before a gradual decline. This phenomenon can be interpreted as reflecting the intensification of security audits and improved reporting of CVEs, followed by corrective actions that have limited the appearance of new vulnerabilities.

We then looked at the distribution of vulnerabilities by product (excluding MFA).fig:Distribution of vulnerabilities by product/technology (excluding MFA) shows that certain mission-critical systems, such as Windows Server or network equipment from Cisco and Juniper, account for a significant proportion of vulnerabilities. This underlines their strategic importance in infrastructures, but also their attractiveness as

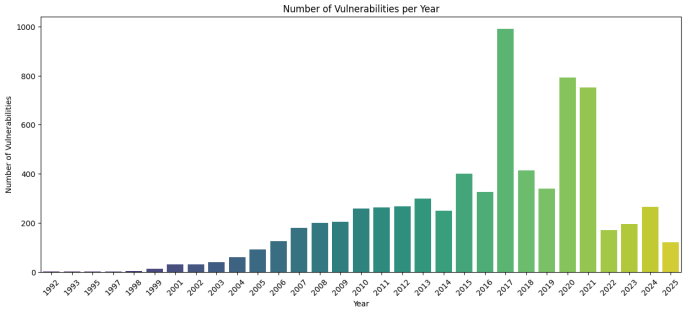

Fig. 2. Number of vulnerabilities listed by year

potential targets for attackers.

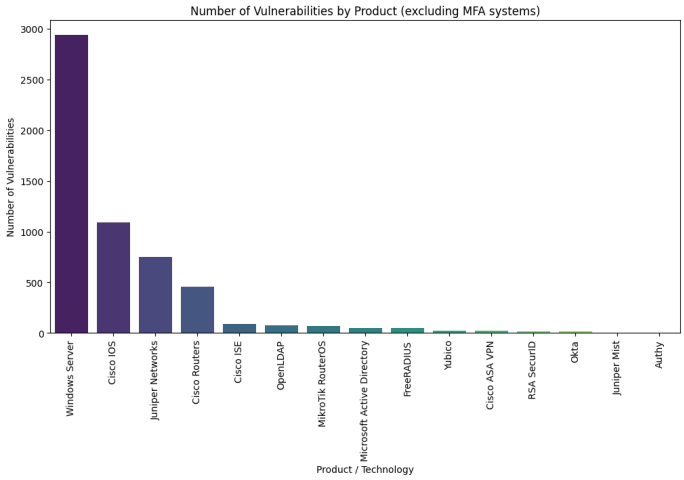

Fig. 3. Distribution of vulnerabilities by product/technology (excluding MFA)

Finally, we have isolated the vulnerabilities specifically affecting multi-factor authentication (MFA) systems. As shown in fig:Number of vulnerabilities by MFA product, these technologies generally present a more contained level of risk. However, certain solutions such as *Yubico* or *RSA SecurID* deserve extra vigilance due to their presence in sensitive environments.

Taken together, these results enable us to better target high-risk technologies, and to focus security efforts on the most critical components of authentication chains.

To assess the security of the main authentication protocols, we applied our classification model based on the average CVSS score (S) and the proportion of critical flaws (C). The weighting used is $\alpha = 0.7$ for severity (S) and $\beta = 0.3$ for the critical flaw proportion (C), in line with our methodology.

For each protocol, we calculated an overall risk score (V) using the formula:

$$V = \alpha \cdot S + \beta \cdot C$$

The numerical results obtained by applying the classification model provide an overview of the overall risk associated with

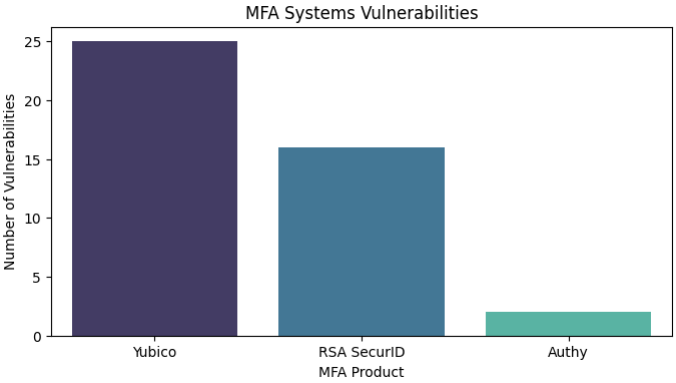

Fig. 4. Number of vulnerabilities by MFA product

each authentication protocol. To further illustrate these results, we have used visualizations that help to better understand the risk distribution for each protocol studied.

Firstly, Figure 5 presents the overall risk score V calculated for each protocol based on our weighted model. This score takes into account both the average severity of vulnerabilities (S) and the proportion of critical flaws (C). As the visualization shows, all the protocols studied fall within the moderate risk range, although there are significant differences between some of them. The LDAP and TACACS+ protocols stand out with higher risk scores, suggesting that they present more severe or critical vulnerabilities.

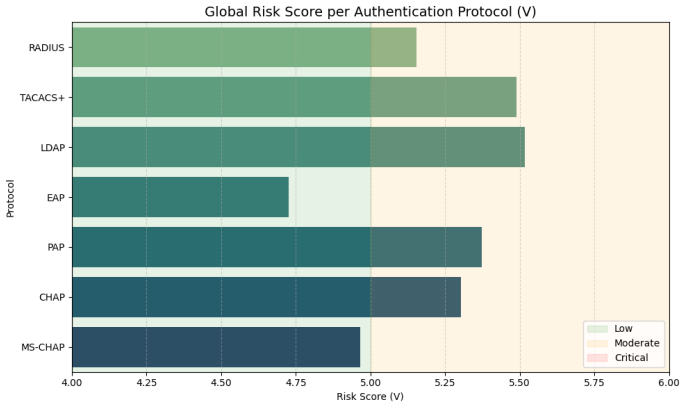

Fig. 5. Global Risk Score by Authentication Protocol (V)

Complementing this analysis, we have also studied the proportion of critical CWEs associated with each protocol, providing a better understanding of the concentration of particularly serious flaws in each technology. Figure 6 presents this distribution, where we can see that certain protocols, such as LDAP and TACACS+, are associated with a high proportion of critical flaws, highlighting their vulnerability to potentially devastating attacks.

These visualizations give a clearer picture of the relative risks of different authentication protocols. They reinforce the importance of adopting a targeted approach to vulnerability management, particularly for protocols with higher risk scores.

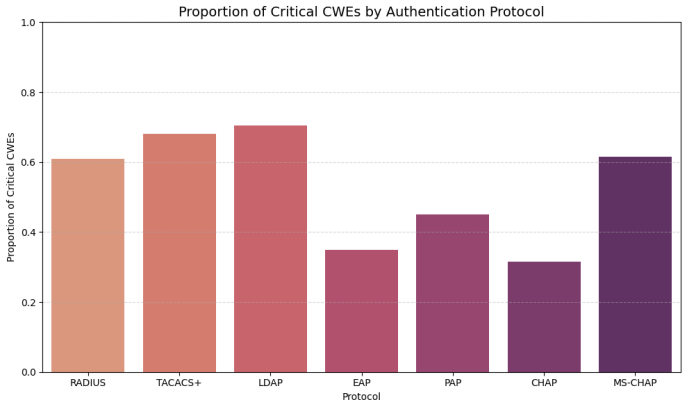

Fig. 6. Proportion of Critical CWEs by Authentication Protocol

In this way, these analyses provide a more detailed overview of high-risk authentication protocols, and help to define more precisely the priorities for security hardening efforts, particularly for technologies such as LDAP, which are widely deployed and show both a high severity and a significant proportion of critical vulnerabilities.

V. Conclusion

User and device authentication is a fundamental pillar of information systems security. However, as this study has shown, the authentication protocols used in modern infrastructures are often vulnerable to a wide range of attacks. Although long-standing protocols such as PAP and CHAP have contributed to network security in the past, they now have serious flaws, particularly in the transmission of unencrypted data, making them susceptible to interception and replay attacks. These vulnerabilities underline the need for more secure solutions to protect access to sensitive information. With this in mind, more advanced protocols such as RADIUS and TACACS+ offer better centralized access management, but they are not without their risks. RADIUS, for example, only encrypts passwords, exposing other sensitive information during transmission. By contrast, TACACS+ offers superior protection by encrypting all exchanges between client and server, making it a preferable option in environments where confidentiality of exchanges is paramount. However, the management complexity and costs associated with implementing TACACS+ can be an obstacle in some organizations. In addition, both protocols present potential vulnerabilities, such as man-in-the-middle attacks or configuration errors, which can compromise the security of the entire system.

Modern multi-factor authentication (MFA) protocols, such as those using TOTP and HOTP, also offer a partial answer to these vulnerabilities by adding an extra layer of security. However, these mechanisms are not immune to phishing attacks, malware and synchronization problems, which underlines the fact that no solution is totally invulnerable. The integration of biometrics and artificial intelligence into authentication systems represents a promising step forward, although significant challenges remain in terms of personal data management and privacy.

In addition, protocols such as LDAP, used for centralized management of identity information, also present significant risks. The absence of encryption in default transmission exposes sensitive data to man-in-the-middle attacks. LDAP injection attacks and denial-of-service (DoS) attacks are also possible, underlining the importance of adopting secure versions of LDAP, such as LDAPS, to avoid such threats.

By applying a risk classification model, we were able to assess the vulnerabilities of the protocols studied and measure the level of risk associated with each of them. Our results showed that, while most protocols present a moderate risk, some, such as LDAP and TACACS+, display higher risk scores, indicating that they require special attention to avoid serious consequences linked to uncorrected security flaws. The results of this analysis highlight the need for proactive vulnerability management and regular updating of authentication protocols to reduce their exposure to attacks. Finally, although many solutions exist to reinforce the security of authentication protocols, the constant evolution of threats and attack techniques makes it imperative to adopt a dynamic approach to security. This involves not only the implementation of robust technical solutions, but also the ongoing training of administrators and users to minimize the risks associated with human error or poor management of authentication systems. By combining advanced authentication protocols, rigorous vulnerability management and proactive defense strategies, organizations can be better prepared to face the complex challenges of modern cybersecurity.

References

[1] S. Szymoniak and S. Kesar, *Key Agreement and Authentication Protocols in the Internet of Things: A Survey*, Applied Sciences, vol. 13, no. 1, p. 404, Dec. 2022.

[2] M. Kovtsur, A. Minyaev, D. Khramtsov, and G. Abramenko, “Investigation of Attacks and Methods of Protection of Wireless Networks During Authorization Using the IEEE 802.1x Protocol,” in *Proceedings of the 5th International Conference on Future Networks and Distributed Systems* , 2022, pp. 555–561.

[3] M. Kovtsur, A. Minyaev, D. Khramtsov, and G. Abramenko, “Investigation of Attacks and Methods of Protection of Wireless Networks During Authorization Using the IEEE 802.1X Protocol,” in *Proceedings of the 5th International Conference on Future Networks and Distributed Systems*, 2022, pp. 555–561.

[4] H. Mutaher and P. Kumar, “Security-Enhanced SDN Controller Based Kerberos Authentication Protocol,” in 11th International Conference on Cloud Computing, Data Science & Engineering , 2021.

[5] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-Factor Authentication: A Survey,” 2021.

[6] Z. Yang, C. Jin, J. Ning, Z. Li, A. Dinh, and J. Zhou, “Group Time-based One-time Passwords and its Application to Efficient Privacy-Preserving Proof of Location,” in Proceedings of the 37th Annual Computer Security Applications Conference , 2021, pp. 497–512.

[7] S. Srinivasa, J. M. Pedersen, and E. Vasilomanolakis, “Deceptive directories and ‘vulnerable’ logs: a honeypot study of the LDAP and log4j attack landscape,” in Proceedings of the IEEE Conference, 2022.