Survey of Authentication Vulnerabilities and Classification Model

Presented by :

- Rania BLIBEK
- Yasmine ZAHEM

02/06/2025

Presentation Plan Overview

1. **Introduction:** Define authentication and its cybersecurity role.
2. **Authentication Process:** Steps from identification to session management and inherent risks.
3. **Protocols & Vulnerabilities:** Overview of common protocols and their key security flaws.
4. **Classification Methodology:** Data collection, attribute extraction, scoring, and risk categorization.
5. **Results & Conclusion:** Risk scores, critical vulnerabilities, and future cybersecurity directions.

Introduction:

Authentication is the process of verifying the identity of a user, device, or system before granting access to sensitive resources.

Why is it important?

- It protects systems from **unauthorized access**.
- It ensures that **only trusted users or devices** can access data or perform actions.
- It is a **first line of defense** in cybersecurity — without secure authentication, even strong systems are vulnerable.

Authentication Process Cycle

User Identification

The user provides credentials such as username or biometric data.

Session Management

Active sessions are monitored and renewed to maintain security.

Verification

Credentials are checked against stored data to verify identity.

Authentication

Successful verification grants access and initiates secure session.

Authorization

Access rights are assigned based on authenticated identity.

A successful authentication doesn’t always mean it’s secure

Sometimes, the system says **“Access Granted”**, but it’s **not the real user**.

Commonly Used Authentication Protocols

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)
LDAP	Clear text transmission, LDAP injection, MITM
RADIUS	Partial encryption, exposure of metadata
TACACS+	Misconfiguration
EAP-TLS	Denial-of-service (DoS) attacks
TOTP/HOTP	Phishing, OTP code interception/Desynchronization, replay risk

Classification Methodology

1

Data Collection

Gathered CVEs from public databases for protocols like PAP, CHAP, RADIUS, and LDAP.

2

Attribute Extraction

Extracted CVSS scores, CWE classifications, impact scope, and publication year.

3

Grouping & Scoring

Grouped CWEs into categories and calculated a global vulnerability score combining severity and critical flaw proportion.

4

Risk Classification

Protocols categorized as Critical, Moderate, or Low risk based on the global score.

Data Collection & Attribute Extraction

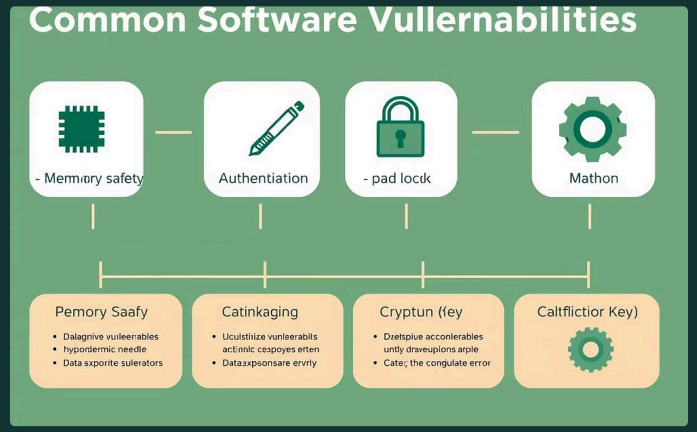
Data Collection

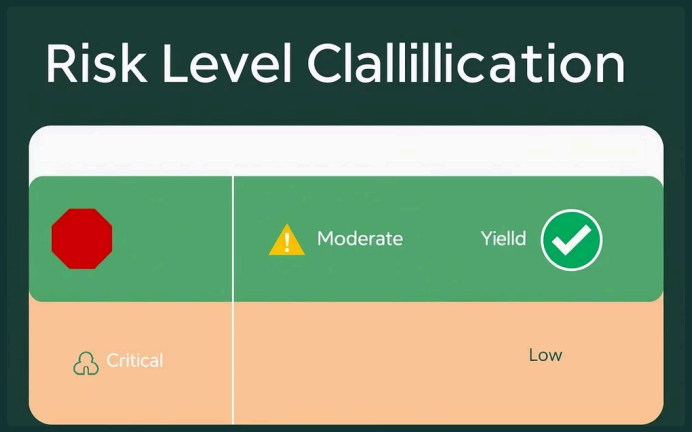
Gathered CVEs from NVD, MITRE databases for protocols PAP, CHAP, RADIUS, LDAP.....

Attribute Extraction

Extracted CVSS scores, CWE types, publication year, and impact on confidentiality, integrity, availability.

Grouping, Scoring & Risk Classification





CWE Grouping

Groups simplify threat analysis and reveal common protocol weaknesses.

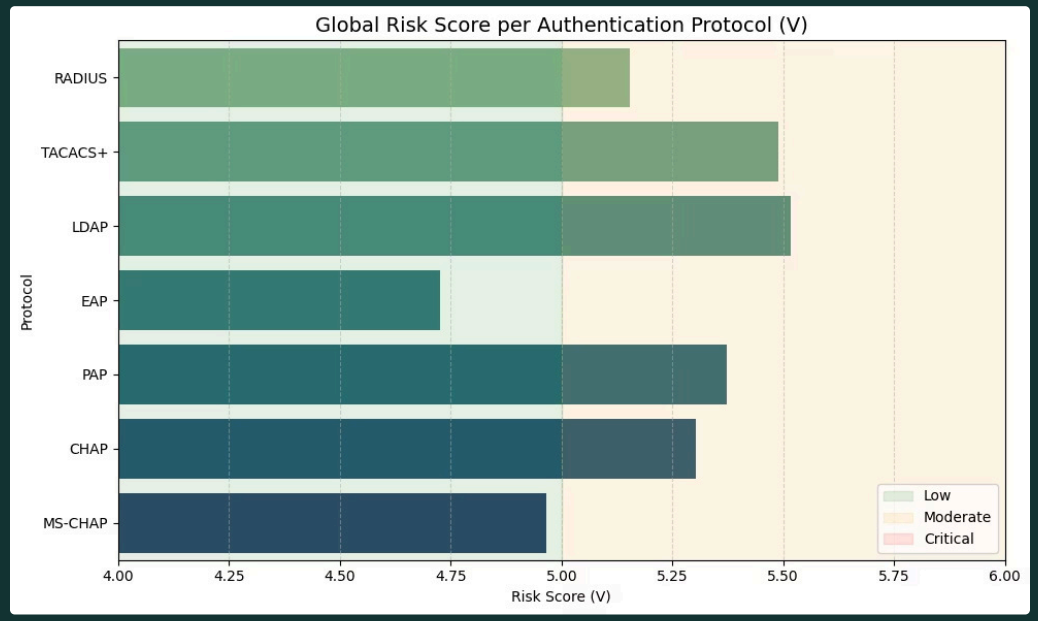
Vulnerability Score

Score = 0.7 × average CVSS + 0.3 × critical CWE share balances risk.

Risk Classification

- Critical: $V \geqslant 8$
- Moderate: $5 \leqslant V < 8$
- Low: $V < 5$

Results and Analysis



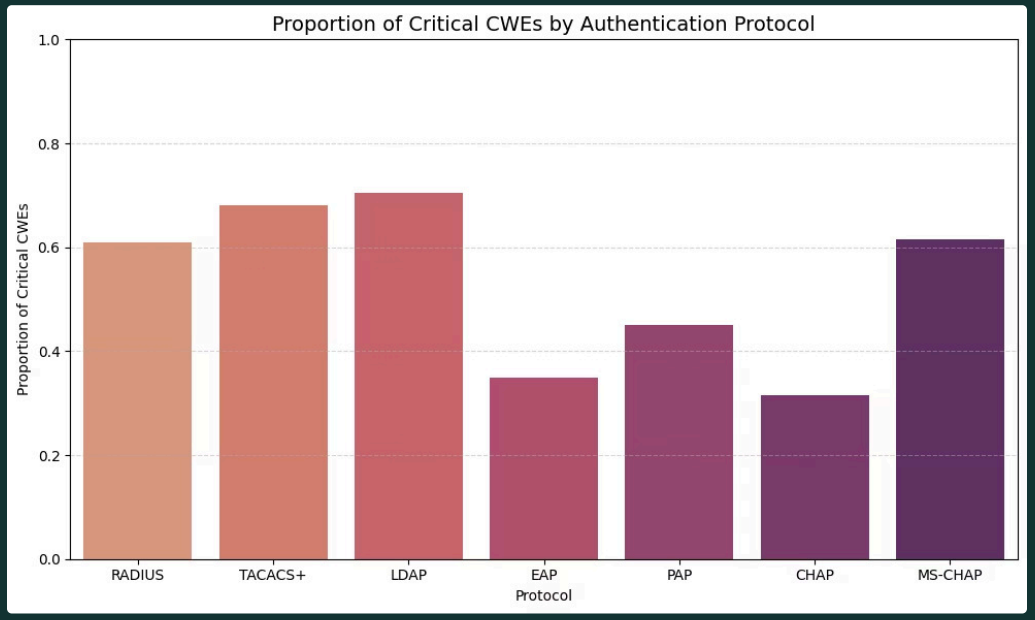
This graph displays the global risk score (V) calculated for each authentication protocol.

The score is based on both the **severity (CVSS)** and the **proportion of critical weaknesses (CWE)**.

🔴 **LDAP**, **TACACS+**, and **PAP** show the **highest risk levels**, indicating a significant exposure to attacks.

🟢 **EAP** stands out as the **only low-risk protocol**, reflecting strong cryptographic properties and better implementation standards.

This comparison helps identify which protocols should be prioritized for replacement or reinforcement.



This chart highlights how many of the vulnerabilities found in each protocol are considered **critical** (according to CWE classification).

🚨 **LDAP** and **TACACS+** again top the chart, with over **70% of their weaknesses classified as critical**.

🟣 **CHAP** and **EAP** show a **lower concentration of severe flaws**, indicating comparatively better security structures.

🔍 This perspective complements the global risk score by focusing on **how dangerous the flaws actually are**.

Conclusion and Future Directions

Protocol Vulnerabilities Persist

Many protocols still expose data to interception and attacks.

Advanced Protocols Improve Security

TACACS+ encrypts all exchanges but may bring management complexity.

Multi-Factor and Biometrics

MFA adds layers but faces phishing and sync challenges; biometrics hold promise despite privacy concerns.

Ongoing Risk Management Needed

Frequent updates and user training are crucial to counter evolving threats.

✨Thank you for your attention