WPA2-Enterprise Authentication Protocols Comparison

Securely authenticating network users is a fundamental aspect of network security and is the source of significant challenges for many network administrators.

An 802.1x network authentication method is one of the first lines of defense that protect users and the network against outside attacks. As a user connects to the network, they are prompted to provide identifying information that is compared against the stored identities of all network users.

Protecting this process is of utmost importance because it’s the most consistent instance of compromising information being sent over-the-air. Many data theft attacks target the authentication method because some are significantly less secure than others.

**Table Of Contents**

* [**Security**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#cyber)
  + [**PEAP-MSCHAPv2**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#peap3)
  + [**EAP-TTLS/PAP**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#ttls3)
  + [**EAP-TLS**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#tls3)
* [**User Experience**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#user)
  + [**PEAP-MSCHAPv2**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#peap2)
  + [**EAP-TTLS/PAP**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#ttls2)
  + [**EAP-TLS**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#tls2)
* [**Identity Management**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#access)
  + [**PEAP-MSCHAPv2**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#peap1)
  + [**EAP-TTLS/PAP**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#ttls1)
  + [**EAP-TLS**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#tls1)
* [**EAP-TLS Surpasses The Rest**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#surpass)
* [**Authentication Processes In Detail**](https://www.securew2.com/blog/wpa2-enterprise-authentication-protocols-comparison/#detail)

Below is the criteria by which we judged the effectiveness of each 802.1x authentication type. Each authentication type was individually judged and represent a complete picture of their attributes and effectiveness.

| **WPA2-Enterprise Protocols** | Level of Encryption | Authentication Speed | Directory Support | User Experience |
| --- | --- | --- | --- | --- |
| EAP-TLS | Public-Private Key Cryptography | Fast – 12 Steps | SAML/LDAP/MFA Servers | Best |
| PEAP-MSCHAPV2 | [**Encrypted Credentials**](https://www.securew2.com/blog/peap-mschapv2-vulnerability/) | Slow – 22 Steps | Active Directory | Acceptable |
| EAP-TTLS/PAP | Non-Encrypted Credentials | Slowest – 25 Steps | Non-AD LDAP Servers | Poor |

A comparison of the WPA2-Enterprise protocols on Encryption, Speed, Support and User Experience.

From this criteria, we set out to compare each type and evaluate their how successful each is as an authentication method. Each method will be evaluated based on the effectiveness of it’s cybersecurity measures, the user experience, and how it manages network access.

**Security**

**PEAP-MSCHAPv2**

PEAP’s primary vulnerability is its requirement to use credentials to authenticate users. Credentials do not give a clear picture of who is connected to a network because they can be stolen or given to another user. An ill-intentioned user on the network can operate without being properly identified if they have obtained a valid set of credentials.

There are several methods that can be used to obtain credentials. One such way is to use a [**Man-In-The-Middle**](https://www.securew2.com/blog/what-man-in-the-middle-attack/) attack to intercept credentials while they are being sent for authentication. Another is a dictionary attack, or brute-force attack, which simply involves a hacker attempting to login with nearly endless combinations of letters, numbers, and symbols to guess a user’s password. This can be frighteningly effective as common passwords, patterns in human behavior, and cooperation among hackers has resulted in sophisticated programs and lists of passwords to attempt when conducting a brute-force attack. What’s worse is that PEAP-MSCHAPv2 has been in use for many years and is [**revealing vulnerabilities that can be exploited**](https://www.securew2.com/blog/peap-mschapv2-vulnerability/).

But an important aspect of PEAP that is not often highlighted is how much the security depends upon your network users. The integrity of the network depends on users: never losing their credentials, never writing them down, never sharing them, always using password best practices, never connecting to the wrong SSID, and more.

Network security is also dependent on end users configuring their devices properly. One of the most important methods for [**preventing over-the-air credential theft**](https://www.securew2.com/solutions/preventing-over-the-air-credential-theft/) is server certificate validation. When onboarding software is used, it significantly reduces the risk of users not properly configuring their devices for server certificate validation. However, your network will always remain vulnerable. Any end user can choose to bypass the onboarding software provided to them and manually configure their device for network access. The potential for misconfiguration is high, and the costs are an exploitable flaw in your network security.

As a result of this level of dependence, human error is often the primary cause of data breaches. According to [**Experian’s Managing Insider Risk Through Training and Culture Report**](https://www.secureworldexpo.com/industry-news/weakest-link-human-error-in-cybersecurity), data protection professionals labeled employees as the weakest link in an organization’s cybersecurity system 66% of the time. As a general rule of thumb in cybersecurity, the more the user is involved, the less secure the system is.

**EAP-TTLS/PAP**

Considering both EAP-TTLS/PAP and PEAP-MSCHAPv2 are credential-based, they suffer from many of the same problems. EAP-TTLS/PAP is vulnerable to Man-In-The-Middle attacks and credential-based phishing. It depends on users to be vigilant in their security best practices and assumes they are not allowing others to use their credentials.

The primary difference between the two is that EAP-TTLS/PAP sends its credentials in cleartext through the EAP tunnel. Cleartext is an unencrypted format that can be read plainly.

In a normal environment, the EAP tunnel prevents anyone from observing the communication going on during the authentication process. But circumstances are not always normal, and if the user falls victim to a Man-In-The-Middle attack, they end up sending their cleartext credentials to a data thief.

Encrypted credentials are not a security measure to depend upon; it’s relatively easy to decrypt credentials and many tools exist that can do this. If an attacker obtains encrypted credentials, they experience a delay before they are able to use the credentials and offer an opportunity for the organization to discover the attack and take the necessary steps to prevent further damage. When authenticating with EAP-TTLS/PAP, an attacker who obtains cleartext credentials is able to immediately log into the network. Allowing such important information to be sent over-the-air in cleartext is risky and presents an opportunity for data breaches.

**EAP-TLS**

Certificate-based authentication prevents many of the attacks other authentication methods are vulnerable to because it eliminates the need for credentials. Certificates can’t be duplicated, transferred, or stolen off a device, eliminating the risks of many phishing and over-the-air attacks. Credentials can be repurposed and used on any device, but a certificate is explicitly tied to the identity of a particular person and device.

When observing the certificate authentication process, it becomes apparent that the user has minimal involvement. The certificate-equipped device auto-detects the secure network and is automatically authenticated for access. For the entire life of the certificate, the only time the user should have to interact with the certificate is during configuration, which is recommended to supplement with onboarding software that correctly configures every device.

**User Experience**

A risky mistake that some organizations make is allowing users to self-configure their devices for secure 802.1x network access. Configuring a device for network access is not a simple process and requires the user to complete many steps that require high-level IT knowledge to understand. There are ample opportunities to misconfigure, which can leave the network vulnerable to outside attacks.

SecureW2 provides onboarding software that automatically configures the user’s device for secure network access. The onboarding solution can be completed in minutes and guarantees that all network users are properly configured for secure network access. Additionally, our solution allows for both PEAP-MSCHAPv2 and EAP-TLS to be run simultaneously. Learn more about our dynamic solution provided to [**College of William & Mary**](https://www.securew2.com/customers/education-customer-stories/college-willam-mary-eduroam/).

Given the dangers and poor user experience of allowing self-configuration, this “User Experience” evaluation section will assume that each user has gone through onboarding software that has successfully configured their device for the appropriate authentication type.

We’ll focus on the user’s experience during the average network authentication session.

**PEAP-MSCHAPv2**

PEAP authentication requires a valid set of credentials to connect to the secure network. Each user must memorize and manually enter their credentials to connect. This creates reliance on the user to maintain overall network security. Furthermore, it can be annoyingly repetitive for the user considering that the process occurs each time they attempt to authenticate.

Password-reset policies are a necessity when using credentials to guarantee that an outdated set of credentials are not used by an unapproved user. These policies are a significant burden for users. They often lead to IT support ticket requests because, when the policy is enacted, every network-connected device is disconnected. Most users have multiple network-connected devices and resetting each one is a burden that could be avoided.

**EAP-TTLS/PAP**

The EAP-TTLS/PAP authentication process is near identical to PEAPSCHAPv2 from the user experience perspective.

Considering it is also a credential-based 802.1x authentication method, the user follows the same authentication process by entering their valid credentials. It also suffers from the inconvenience caused by password reset policies and the need for manual authentication. Overall, the process is rather involved from the user’s perspective and is not convenient for long-term use.

**EAP-TLS**

Enrolling for a certificate results in the user’s device being equipped with a certificate that is directly tied to the secure network. When a user wants to reconnect to the secure network, the process is entirely hands-off for the user.

Once their device is within the vicinity of the network, it will attempt to establish a connection and authenticate the certificate. The user doesn’t have to memorize a password to enter, and their connection is never disrupted by password disconnect policies. Essentially, once a user has a certificate, their job is done. The certificate is tied to the user and device and automatically authenticates them for secure network access.

A relatively minor but occasionally impactful advantage of certificate-based authentication is its faster authentication speeds. The number of steps required to authenticate a certificate is fewer than that of PEAP-MSCHAPv2 and EAP-TTLS/PAP.

At the individual level, this is such a small amount of time that it is basically negligible. But when a situation occurs where a mass amount of devices attempt to authenticate at the same time, those few steps become much more important and lead to significant differences in authentication speeds.

**Identity Management**

The primary purpose of network authentication is to control who is able to use your network. To separate network users from non-network users, network users’ identities are securely stored, and when someone connects to the network, their identity is compared against known users. If they are an approved user, they are able to successfully connect.

How does each authentication type regulate network access?

**PEAP-MSCHAPv2**

PEAP-MSCHAPv2 is a credential-based authentication system that requires a valid set of credentials to connect. To authenticate, an approved network user will connect to the secure SSID and promptly send their username and password. The user’s credentials are then tied to their identity and stored securely in Active Directory. During the authentication process, PEAP-MSCHAPv2 encrypts the credential data and shields it within an encrypted EAP tunnel. The intended result is end-to-end encryption and authentication of the network user, but the process does not always operate smoothly when variables are introduced.

A glaring issue with credentials is that, although they are tied to a user’s identity, any person that obtains those credentials can connect with anonymity. The Ponemon Institute’s 2019 State of Password and Authentication Security Behaviors found that [**69% of survey respondents admit they share passwords with colleagues**](https://www.intellisuite.com/blog/2019-password-policy-best-practices). There are no countermeasures in place to determine if the person behind the credentials is the approved user, and the more people that know the credentials, the greater the risk.

If an irresponsible user shares their credentials, it can end up in the hands of someone with nefarious goals of data theft.

**EAP-TTLS/PAP**

Similar to PEAP, EAP-TTLS/PAP is a credential-based authentication protocol and is susceptible to the same credential-based identity issues. To be authorized for network use, the onboarding process associates a particular user with the credentials they provide. Contrary to PEAP, EAP-TTLS/PAP credentials are stored in non-AD LDAP servers. With updates in technology, there exists multiple cloud-based, directory-as-a-service, open source providers.  Unfortunately, those credentials can be lost, stolen, or given to another person – who could use them to authenticate and access the network identified as someone else.

**EAP-TLS**

[**EAP-TLS authentication**](https://www.securew2.com/solutions/eap-tls-authentication/) is a certificate-based authentication system, meaning users’ identities are authenticated by digital certificates instead of credentials.

When users enroll to be onboarded to the secure network, they are distributed a certificate that is tied to the identity of the user and their device. With SecureW2’s onboarding solution, the user’s identity can be stored in Active Directory, or any LDAP or SAML based directory.

Once distributed, certificates are designed to not be removed from the device until they expire. Some tools exist online that can make a certificate exportable if they are not properly protected. Counter that with a tool called Certlock that eliminates the risk and makes it impossible for a user or hacker to remove the certificate tied to the device. Unlike credentials, each time a user authenticates to the network with certificates, they are exactly who the network identifies them as.

The identity context provided is paramount to maintaining network security because it puts unwavering control of who has network access in the hands of network administrators. The worry of credentials being obtained by a data thief is eliminated because they would be unable to obtain a certificate.

In addition, admins can easily revoke certificates before expiration if need be. The revoked-access user’s certificate is added to the Certificate Revocation List (CRL). When a user on the CRL attempts to connect, they are identified as unapproved and will not be authenticated. With certificate-based security, administrators can be confident in their ability to regulate who is approved for network access.

**EAP-TLS Surpasses The Rest**

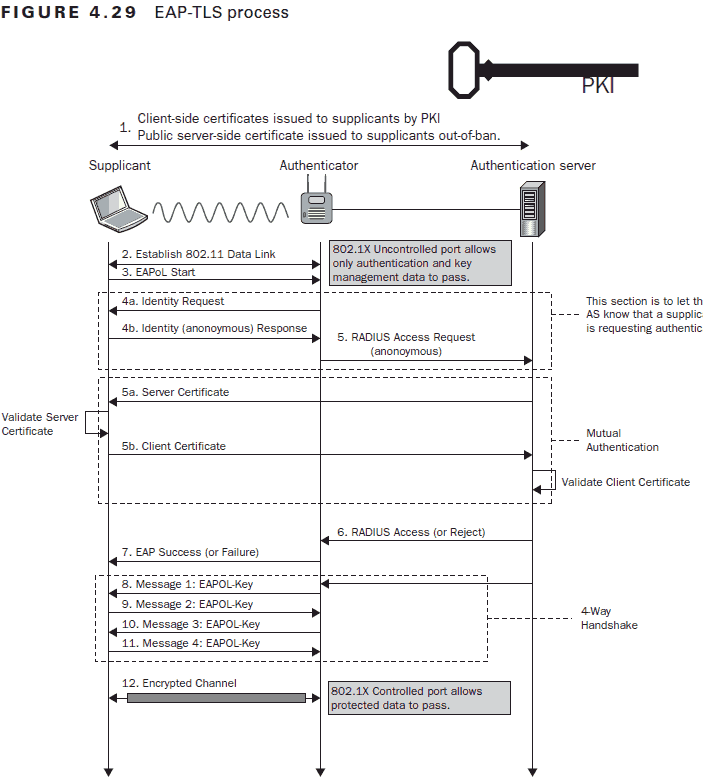
When evaluating an authentication method for your own organization, it’s important to take into account the attributes of your network. A large enterprise may require the highest level of security available while a small organization may value convenience for its employees. Be sure to look ahead and evaluate what will work best for your organization in the long term. Maintaining a secure and easily accessible wireless network is a key to longevity for any organization.

SecureW2 specializes in deploying and maintaining EAP-TLS networks to maximize security and user experience. We have affordable options for organizations of every size. To streamline the transition period, we have supported PEAP-MSCHAPv2 alongside EAP-TLS in the past. Some organizations wish to authenticate new incoming users with certificates while phasing out credential-based authentication in stages. Click [**here**](https://www.securew2.com/pricing/) to inquire about pricing.

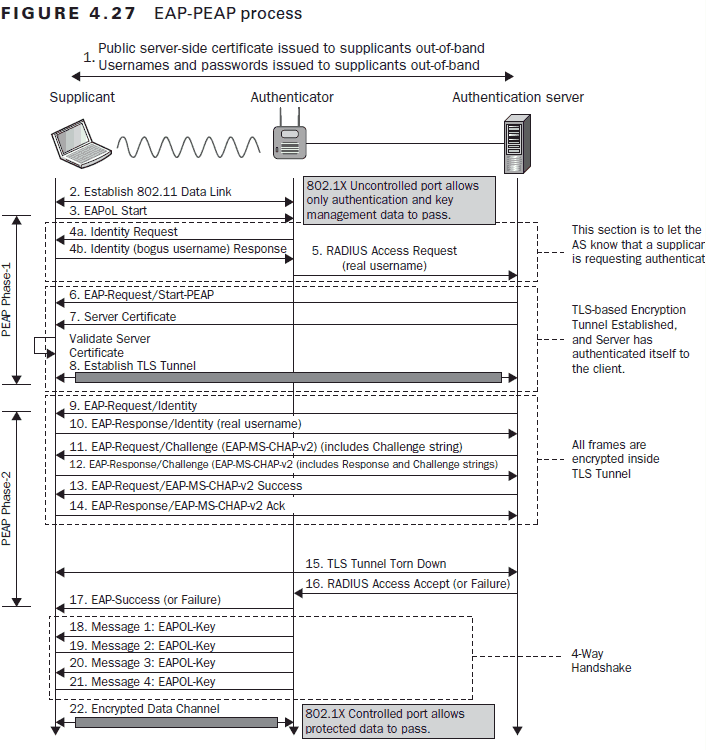
**802.1x Authentication Processes In Detail**

The images below come from the CWSP Certified Wireless Security Professional Study Guide

**EAP-TLS**



**PEAP-MSCHAPv2**



**EAP-TTLS/PAP**

