SEGSI

CIBERSEGURANÇA E ADMINISTRAÇÃO DE SISTEMAS

DCR

Authentication Protocols - 1st phase

When referring to this authentication, the protocol is divided in two phases.
The first phase establishes the protocol to be used, for instances:

- **PEAP** (Protected AP)
- **TTLS** (Tunneled TLS)
- **TLS** (Certificate)
- **FAST** - https://www.cisco.com/en/US/docs/wireless/wlan_adapter/eap_types/fast/admin/guide/EF_ovrvw.pdf

- **PWD** (Password)
- **LEAP** (Lightweight Extensible Authentication Protocol)

Authentication Protocols - PEAP

- PEAP or Protected EAP is one of the most common protocols protocols to see in the wild.
- It’s use creates a tunnel between the client and Access Point so it can connect “securely”.
- “Security” since often there are problems with the PKI infrastructure. Either the certificate is a self-signed one and can easily be forged due to lack of validation of the client. This is rare, but often happens.
- Or the implementation is flawed that the client sends credentials even when a certificate is configured (Android 5.0)

Authentication Protocols - TLS

- This is one of the most secure phase one protocols.
- Essentially it uses certificates to provide identity of the client (supplicant) to the authenticator.
- However, since it involves certificates its adoption rate is very low.

Authentication Protocols - 2nd Phase

The second phase, also known as inner authentication, differs from the first phase.
The most known protocols are:

- **PAP** - Protected AP, ClearText
- **MSCHAP** – Microsoft Challenge Protocol
- **MSCHAPv2** - (Microsoft Challenge Protocol)^2
- **CHAP** - Challenge Authentication Protocol
- **MD5** - Well…
- **GTC** - Token

Authentication Protocols - PAP

- PAP - Protected AP is an inner authentication method that passes the authentication in a cleartext form.
- Meaning that no secure tunnel is made to exchange information.
- An attacker that is able to impersonate an access point can easily capture credentials.
- Even with a sniffer it is possible to do that so.

Authentication Protocols - MSCHAP(v2)

- **MSCHAP** or Microsoft Challenge Handshake Authentication Protocol is a protocol that, by itself, doesn’t transmit the credential.
- This is similar to other Microsoft technologies that allow replay attacks.
- They all suffer from the same flaws, either replayability (with **scyophant**) or the ability to crack them.
- Yes, it depends on the password complexity, but the hash is not that strong and with GPU acceleration nowadays this hash cipher is easily crackable (Good luck enforcing complex passwords on your whole IT park).

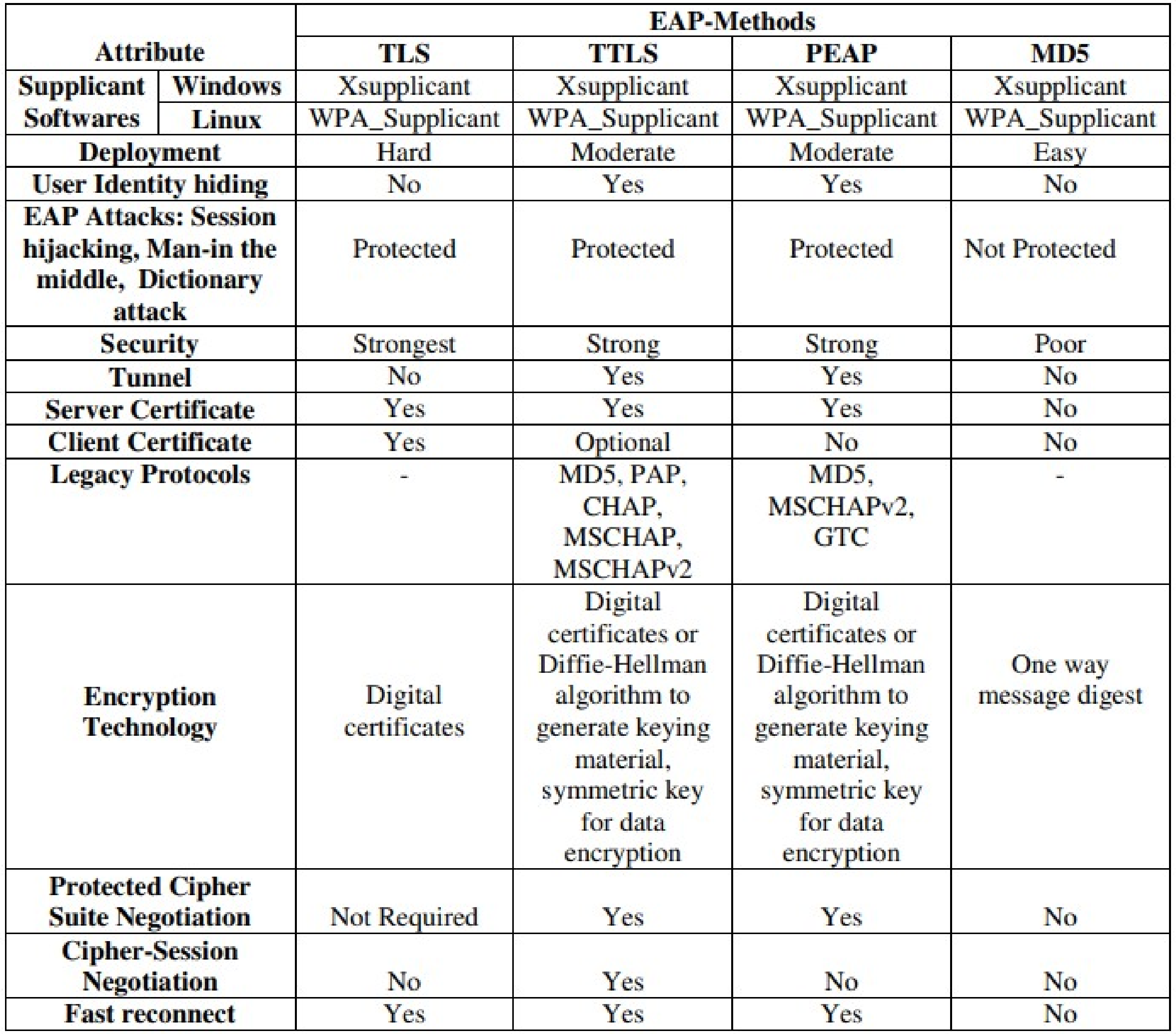
Authentication Protocols - MD5

- It’s MD5! All over again. Your identity is provided by a MD5 Hash of your password and passed to the authenticator. If one person is able to capture this request it is able to crack it either by brute forcing or finding a collision in the MD5 itself.
- With GPUs nowadays it’s considered trivial to do so and this is considered an insecure method of authentication.

Authentication Protocols - GTC

- This is an implementation of a Generic Token challenge. This can be secured, as long as the token is correctly implemented. Not as widespread as other authentication methods.

Authentication Protocols - Summary



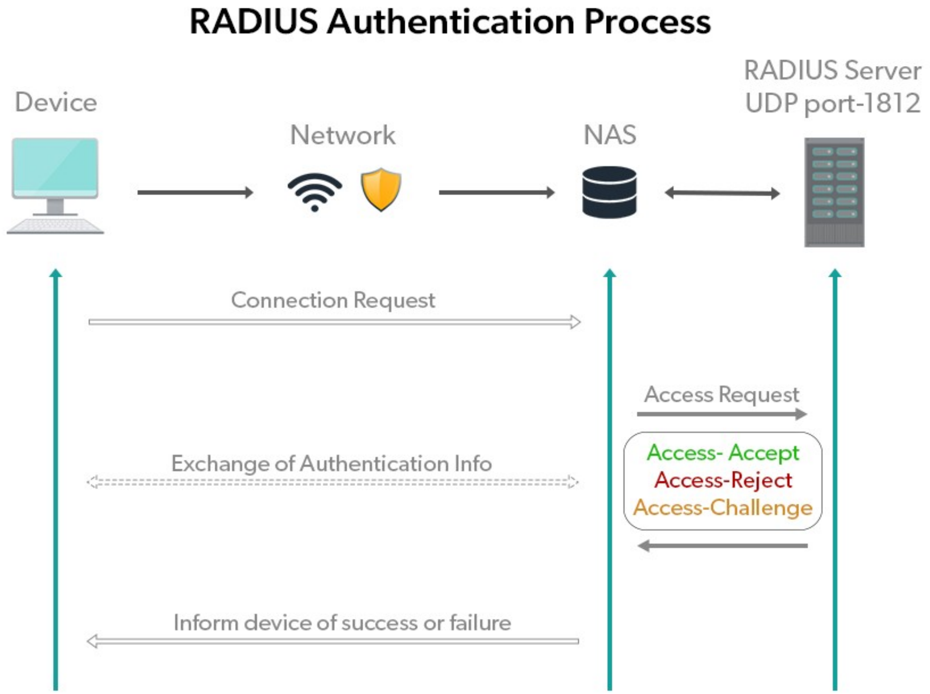
Attribute		EAP-Methods			
		TLS	TTLS	PEAP	MD5
Supplicant Softwares	Windows	Xsupplicant	Xsupplicant	Xsupplicant	Xsupplicant
	Linux	WPA_Supplicant	WPA_Supplicant	WPA_Supplicant	WPA_Supplicant
Deployment		Hard	Moderate	Moderate	Easy
User Identity hiding		No	Yes	Yes	No
EAP Attacks: Session hijacking, Man-in the middle, Dictionary attack		Protected	Protected	Protected	Not Protected
Security		Strongest	Strong	Strong	Poor
Tunnel		No	Yes	Yes	No
Server Certificate		Yes	Yes	Yes	No
Client Certificate		Yes	Optional	No	No
Legacy Protocols		-	MD5, PAP, CHAP, MSCHAP, MSCHAPv2	MD5, MSCHAPv2, GTC	-
Encryption Technology		Digital certificates	Digital certificates or Diffie-Hellman algorithm to generate keying material, symmetric key for data encryption	Digital certificates or Diffie-Hellman algorithm to generate keying material, symmetric key for data encryption	One way message digest
Protected Cipher Suite Negotiation		Not Required	Yes	Yes	No
Cipher-Session Negotiation		No	Yes	No	No
Fast reconnect		Yes	Yes	Yes	No

https://www.diva-portal.org/smash/get/diva2:831569/FULLTEXT01.pdf

Radius

Standard protocol to interconnect clients to several domains

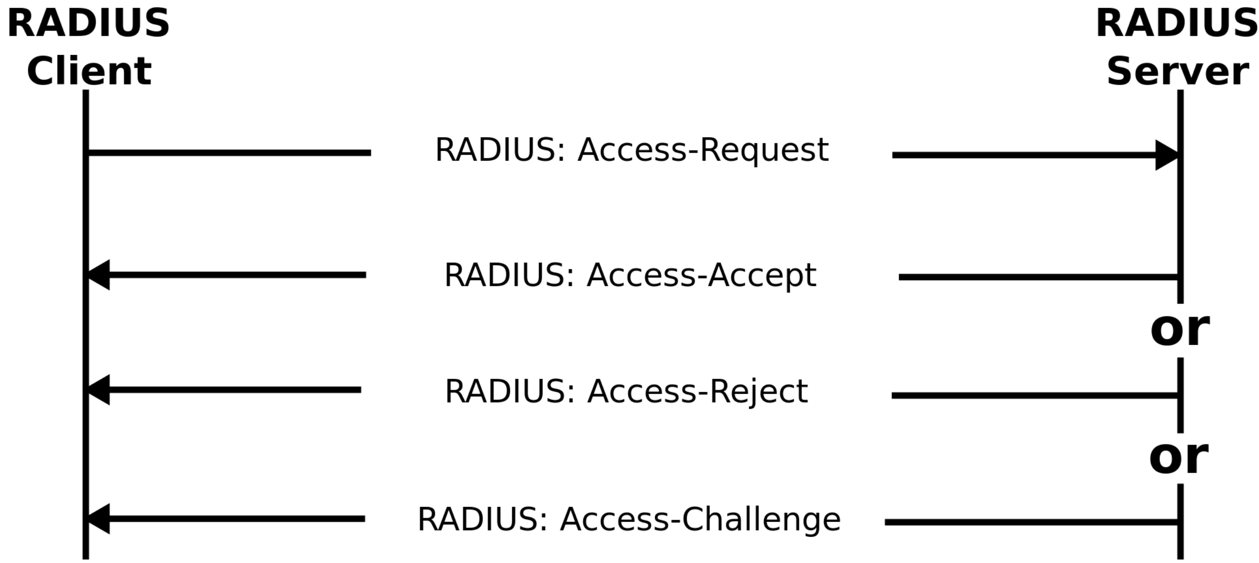
- It can interconnect with different providers;
- The standard case is the Eduroam Network where AAA requests are sent to the respective institutions;
- The Supplicant requests the authenticator to connect; The authenticator forwards the request to the Radius server; Based on the **Realm** of the user.
- Often a shared key is used to avoid rogue clients to connect to the server.



Radius

Radius Authentication steps:

- A client requests User Access providing the necessary information
- One of the following:
  - Accepted
  - Rejected
  - Challenge

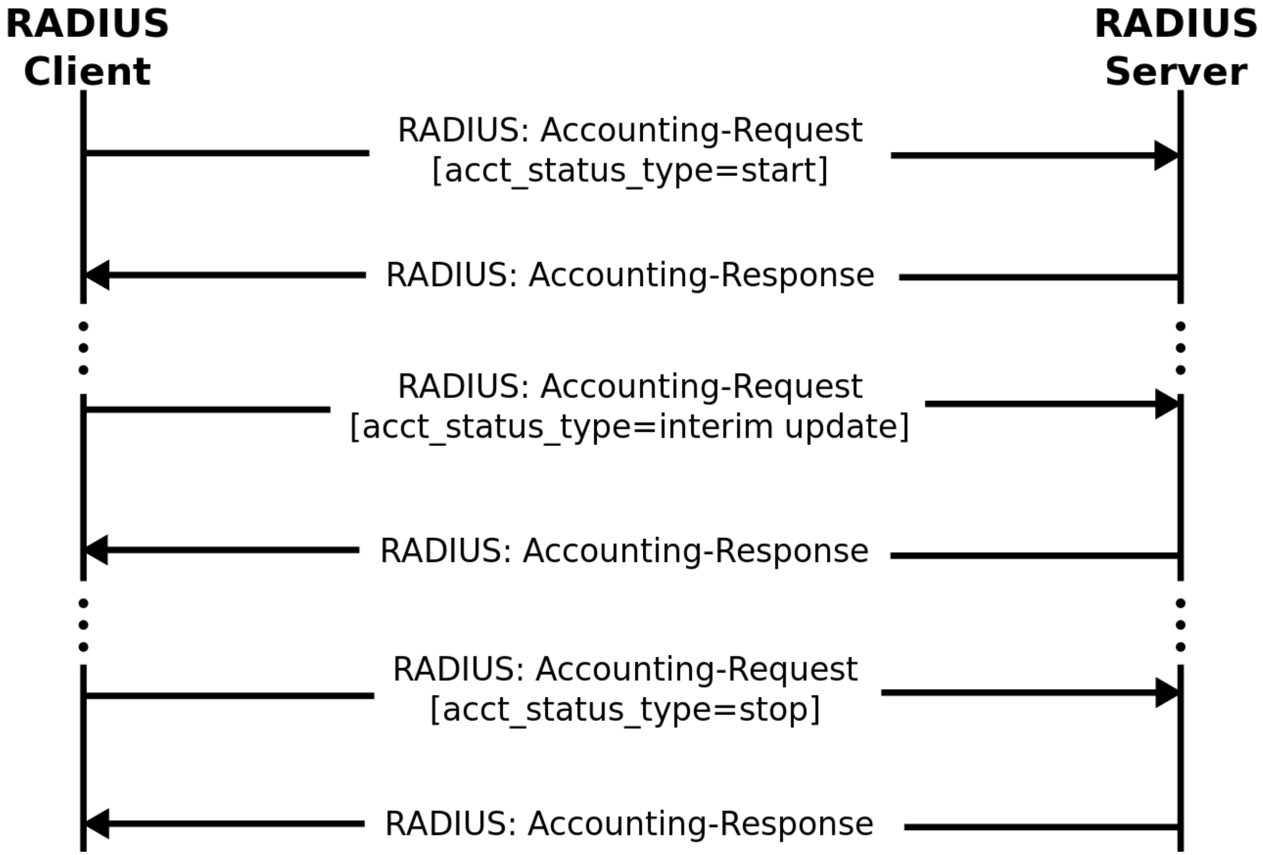


Radius

Radius Accounting

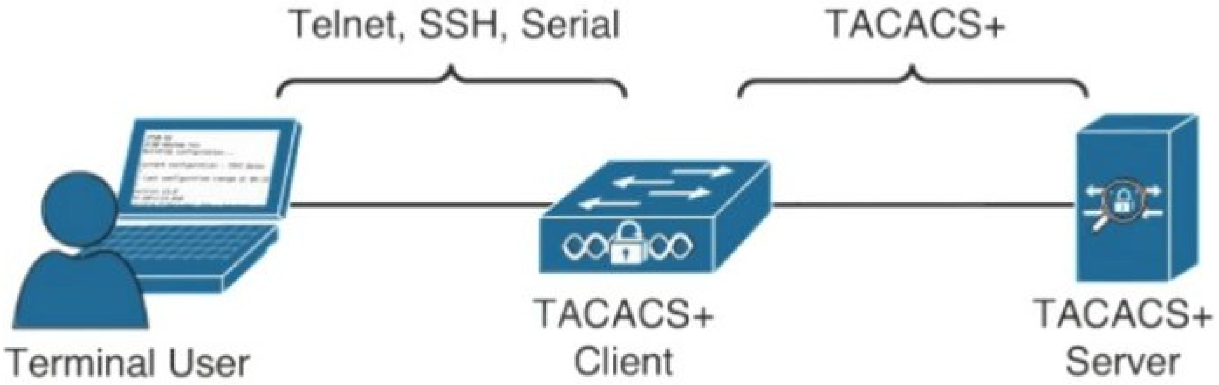
- If the Accounting is done by the **NAS Accounting** is done by the following flow.

Accounting might be done in a different place if an external provider is set up i.e.: Kerberos, LDAP..


RADIUS Client
RADIUS Server
RADIUS: Accounting-Request [acct_status_type=start]
RADIUS: Accounting-Response
RADIUS: Accounting-Request [acct_status_type=interim update]
RADIUS: Accounting-Response
RADIUS: Accounting-Request [acct_status_type=stop]
RADIUS: Accounting-Response

TACACS

- Often used in Cisco Network Devices for **AAA**.
- Configured in the Device itself we can set the AAA server and enable what can the user do in the device
- Legacy protocol with some security concerns. https://www.openwall.com/articles/TACACS+-Protocol-Security

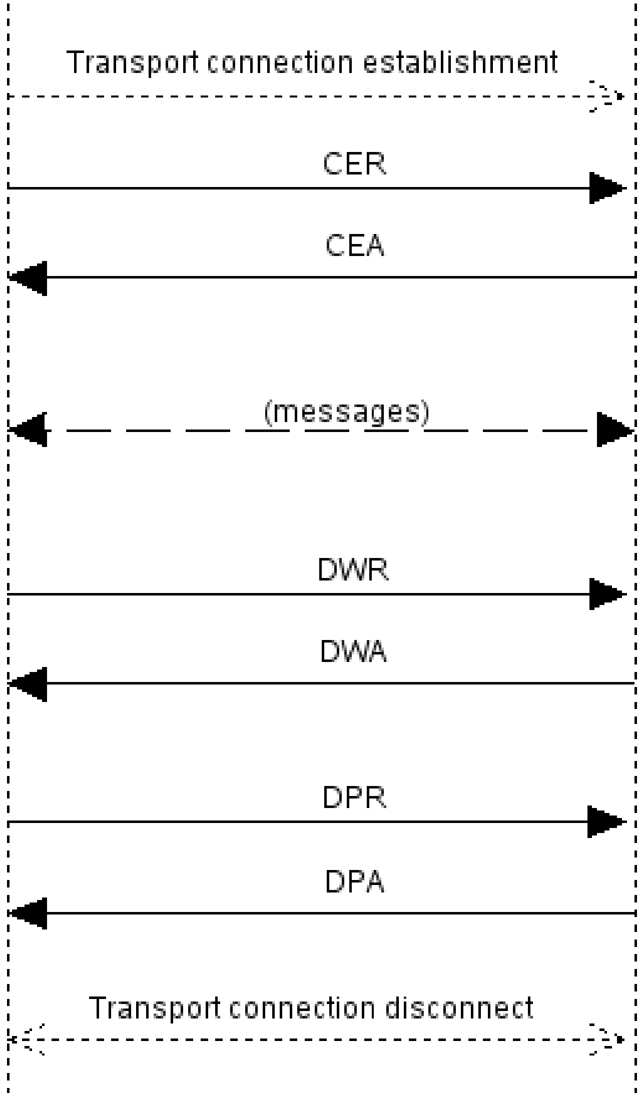


DIAMETER

- 2x the Radius=Diameter
- It brings additional solutions to AAA protocols:
  - TLS certificates;
  - End-2-End encryption;
  - Scalability;
  - Resilience;
- With more capabilities it brings additional complexity to the environment making it a not so adopted solution, apart from the 5G integration

DIAMETER

The connection is Session Oriented;
Roaming is possible and intended;


Transport connection establishment
CER
CEA
(messages)
DWR
DWA
DPR
DPA
Transport connection disconnect