802.1x (in)Security
GTER 19

Luiz Eduardo Dos Santos
CISSP, CWSP, CWAP
Principal Network & Security Engineer

ARUBA

802.1x in 10 seconds (okay 2 minutes)

Not originally a wireless protocol

Usually, depends on some sort of RADIUS server on the back-end

EAP – Extensible Authentication Protocol (basically, extention to PPP)

Extensible Authentication Protocol over LANs - Layer 2 (and ½) authentication protocol

Used on wireless LANs to provide authentication without PPP

Properly implemented improves security in wireless networks since it not only provides authentication but also encryption key rotation

EAP Types

EAP TLS

EAP TTLS

EAP PEAP

EAP LEAP

EAP MD5

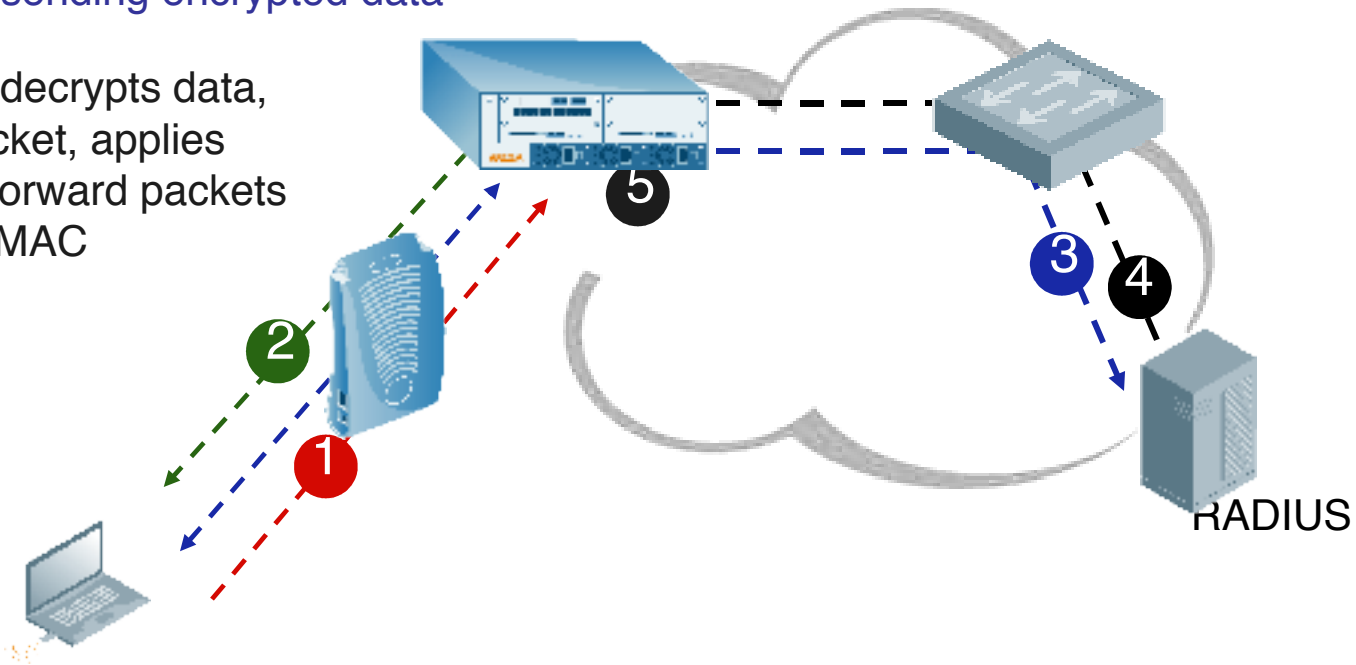
EAP SIM

...

Plus, authentication methods inside EAP (pap, chap, ms-chapv2)

802.1x process

1. Client sends 802.11 association request that is automatically forwarded by AP to WLAN switch
2. WLAN switch responds with association acknowledgement
3. Client and WLAN switch start 802.1x authentication conversation along with RADIUS server
4. Encryption keys pass to the WLAN switch and user derives own encryption keys…begins sending encrypted data
5. WLAN switch decrypts data, processes packet, applies services and forward packets based on .11 MAC



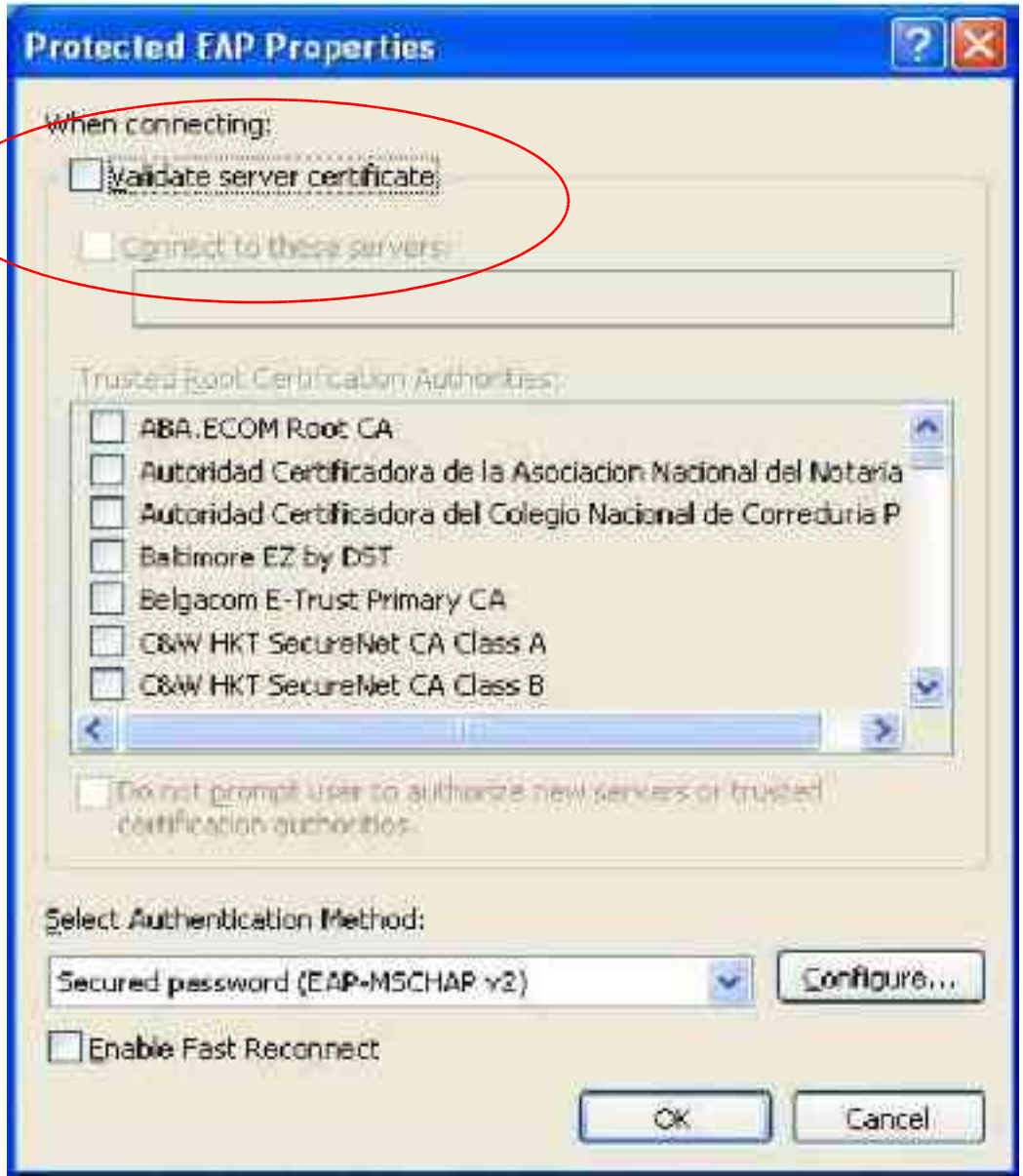
Certificates

Depending on the EAP, certificates can be used, on both the server or client sides

Through the use of certificates a tunnel is created and then pass the user credentials

But...

Validate Certificates



What else?

Depending on the EAP implementation, some usernames are sent out “in clear” in the outer tunnel

Good thing is that some implementations allow “fake” usernames (or simply anonymous) to be sent out in the outer tunnel

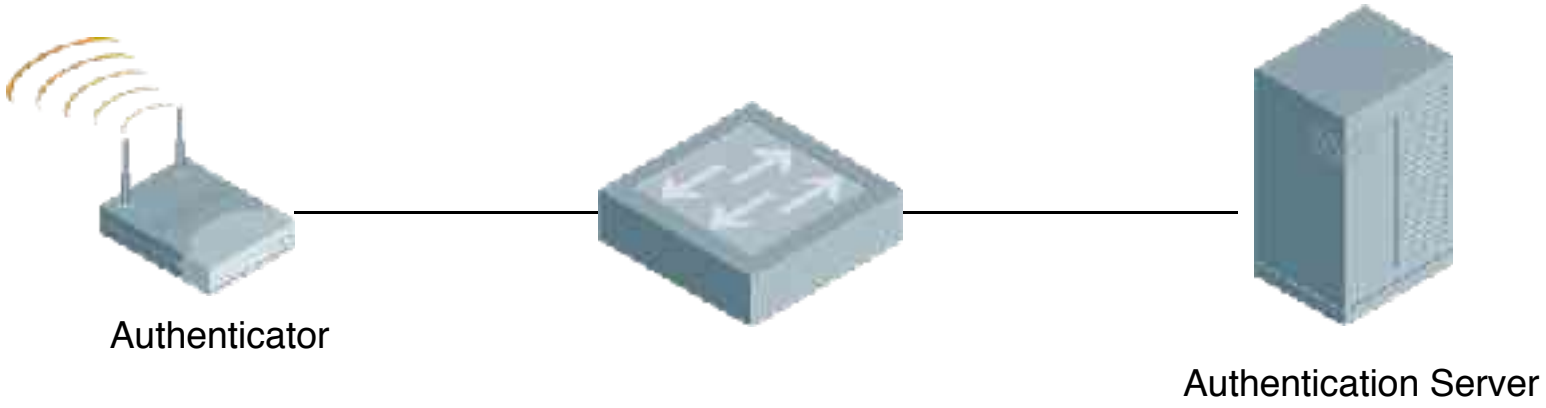
But...

RADIUS

Sometimes people worry too much about the “wireless side” of the security...

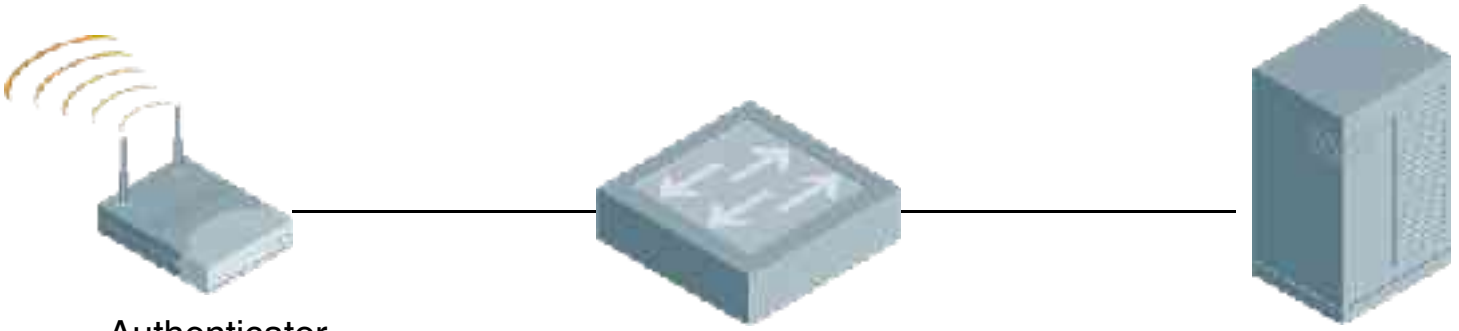
How about the RADIUS security?

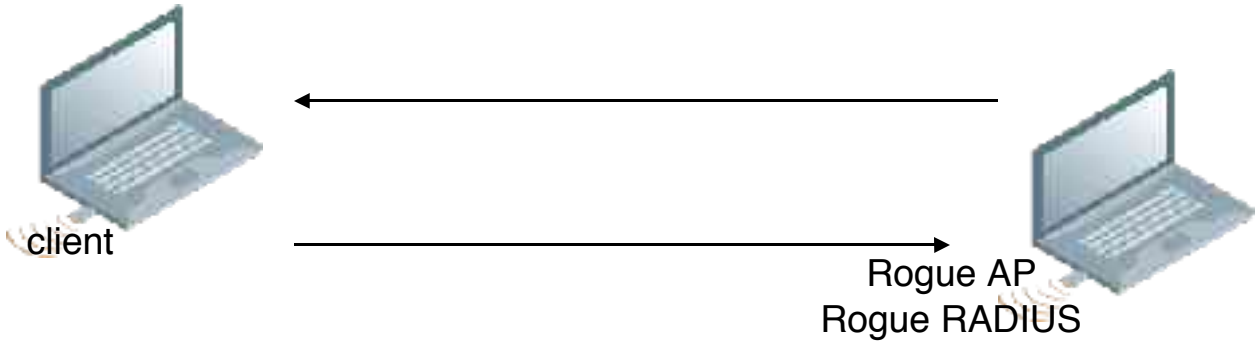
How about the RADIUS traffic security?



Attack Options

Rogue AP + Rogue RADIUS server





Then impersonate victim

How?

Adversary captures request and response authenticators

Mounts brute-force/dictionary attack against secret

Adversary uses secret to:

- Forge Access-Accept frames
- Decrypt MPPE for EAP keys

Others

TTLS using PAP as inner authentication method and no certificate verification

Brute force attacks

People don’t enable certificates because it’s complicated

Some people enable 802.1x with TKIP but don’t have key rotation enabled by default

Some other people enable 802.1x for RADIUS auth, but have the SSID configured as WEP

(as mentioned before) Some 802.1x supplicants allow Server Validation to be optional

WPA will “DoS itself” if a MIC failure occurs

So, is 802.1x bad?

NO! It's your friend.

Just configure it properly.

Make sure the wired connection from the Authenticator (APs or switch) to the RADIUS is secure OR make sure the RADIUS implementation conforms to RFC 3579 and RFC 2865.

Implement a mutual authentication method

Avoid early 802.1x implementations that do not provide per-session keys, but only encrypt packets using the "default-keys"

Good Security Thinking

1. Don’t talk to anyone you don’t know
2. Accept nothing without a guarantee
3. Treat everyone as an enemy until proved otherwise
4. Don’t trust your friends for long
5. Use well-tried solutions
6. Watch the ground you are standing on for cracks

Obrigado!

luiz (at) arubanetworks.com