AIRHEADS meetup

aruba
a Hewlett Packard Enterprise company

The risks off using EAP-PEAP-MSCHAPv2

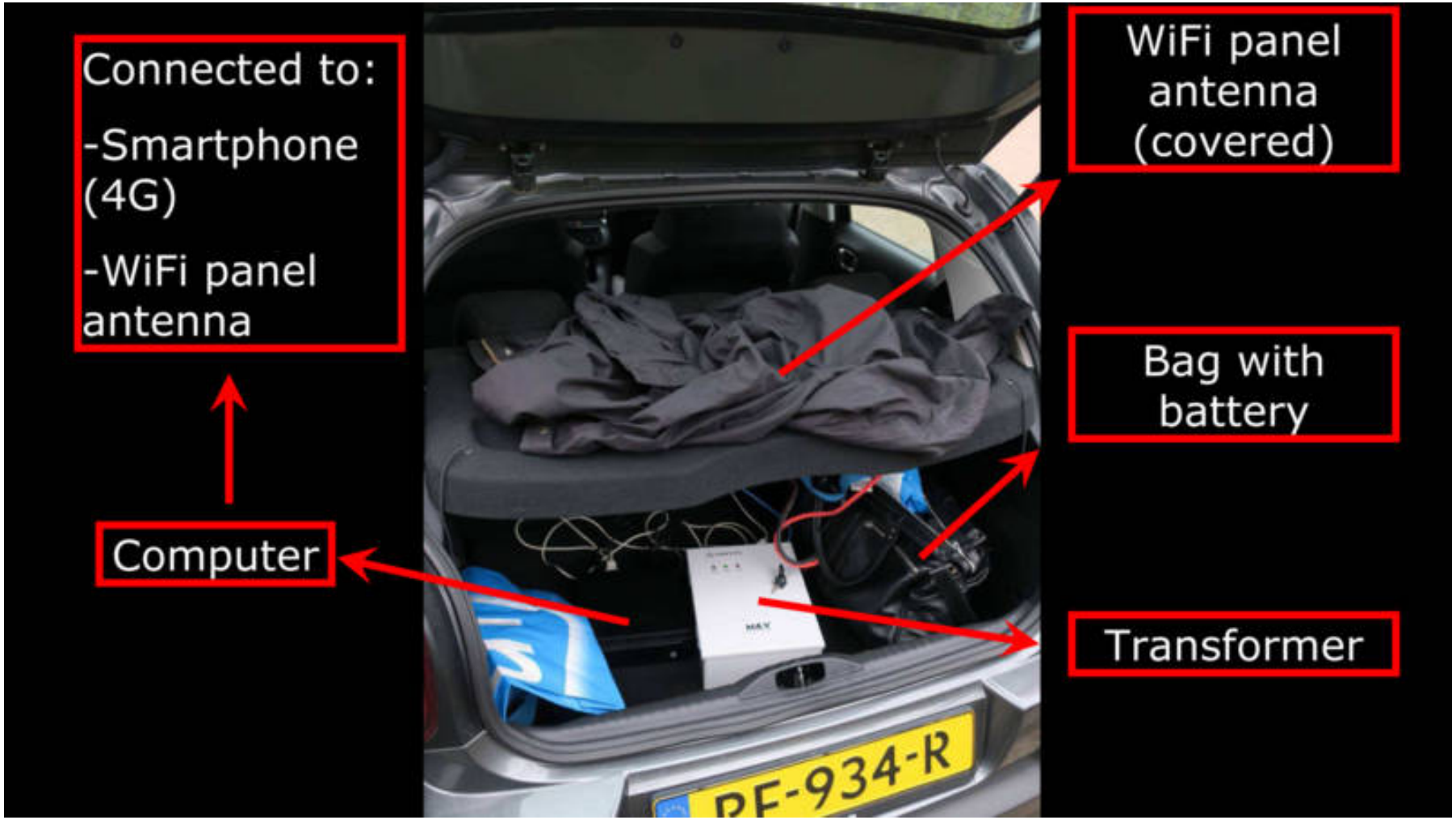
14 November 2018

Willem Bargeman
Security Engineer @ SecureLink

#ArubaAirheads

OPCW Hack

OPCW Hack – ‘Evil Twin’ Attack



What is EAP-PEAP-MSCHAPv2

- Widely used for 802.1x authentication (wired and wireless)
- Developed by Cisco Systems, Microsoft and RSA Security
  RFC: https://tools.ietf.org/html/draft-kamath-pppext-peapv0-00
- First included in Windows XP, but now widely supported (iOS, OSX, Android etc.)
- Outer method: EAP-PEAP (TLS)
- Inner method: MSCHAPv2 (username / password)

EAP-PEAP inner / outer method

What is the problem?

–Biggest issue: MS-CHAPv2 is broken

–(No) Server Certificate validation

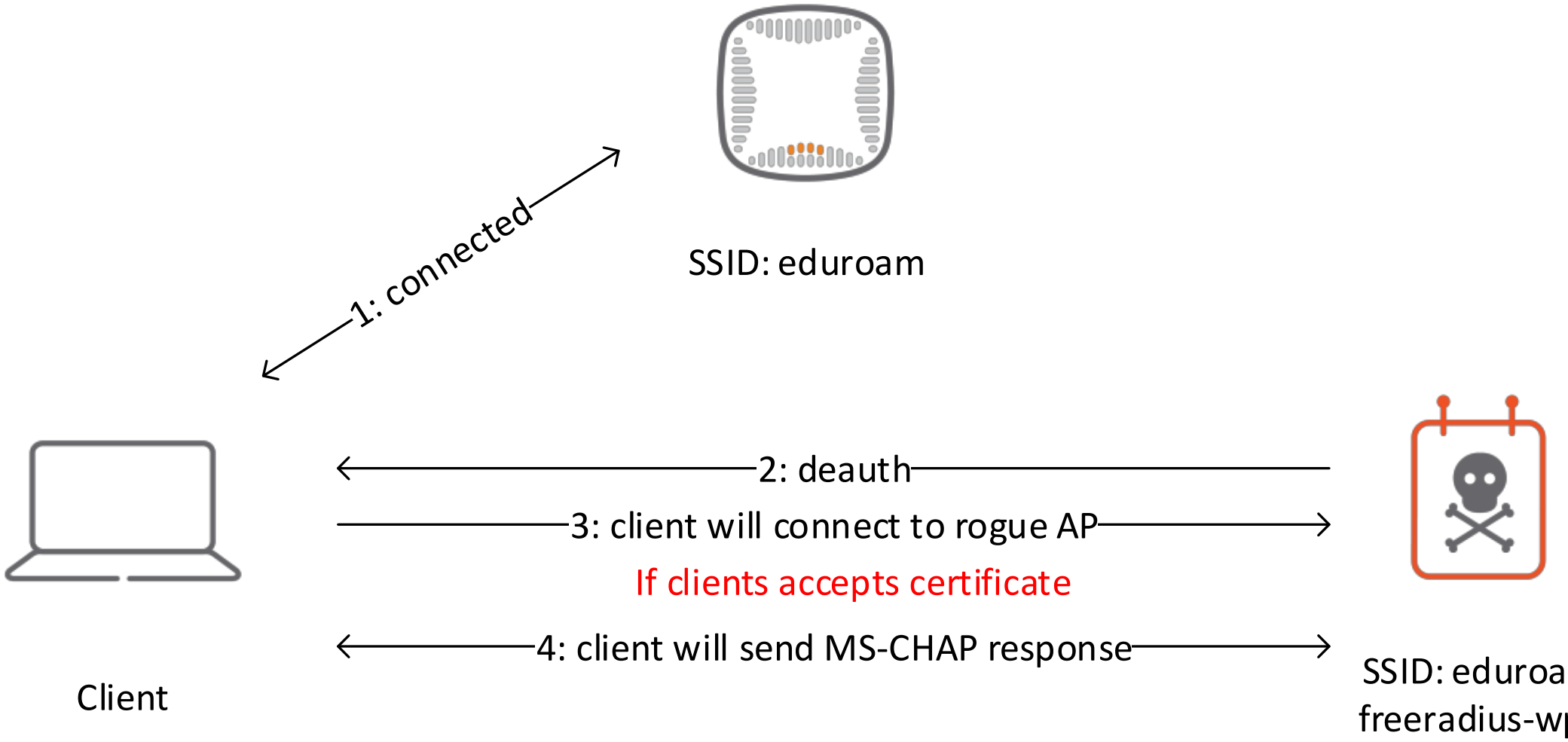
MS-CHAPv2

- MS-CHAPv2 has been proven weak (broken) back in 1999:
  - Dictionary attack
  - https://www.schneier.com/academic/archives/1999/09/cryptanalysis_of_mic_1.html
- Divide and Conquer Attack (Moxie Marlinspike and David Hulton, 2012)
  - 100% success rate in less than 24 hours when using an FPGA cracking such as Crack.sh (previously Cloudcracker)

How does the attack work?

- Force client to authenticate using evil twin attack
- Server side is running freeradius-wpe or eaphammer
  - Will log authentication credentials:
  - TTLS/PAP: Username/password
  - TTLS/CHAP: Challenge/response
  - PEAP/MS-CHAPv2: Challenge/response
  - Returns success for any credentials where possible
- Many clients will automatically connect to a (Rogue) SSID without certificate validation
- MS-CHAPv2 challenge response will be send to attacker

Example


1: connected
SSID: eduroam
2: deauth
3: client will connect to rogue AP
If clients accepts certificate
4: client will send MS-CHAP response
Client
SSID: eduroam
freeradius-wpe

What's next?

- We have the NTLM hash
  - Try to see if the password is listed in a dictionary
  - Or use crack.sh
  - But we could also authenticate with the hash to the network

Pricing & Formats

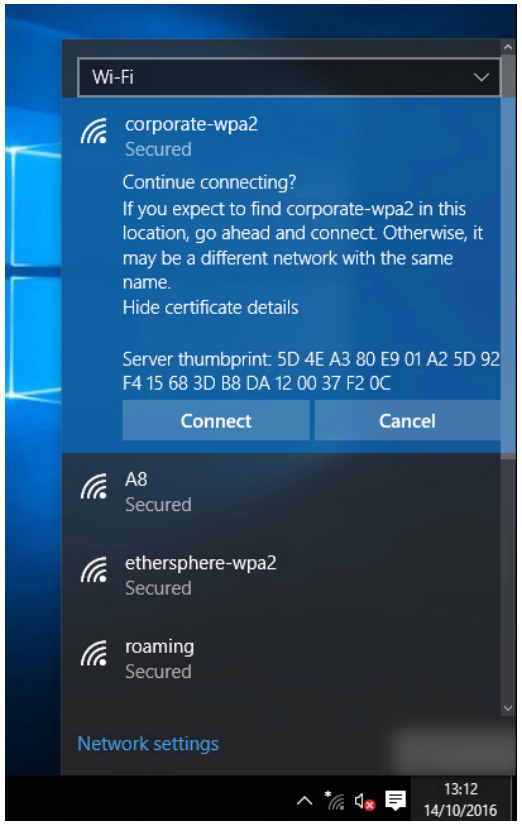
Here's our basic pricing model:

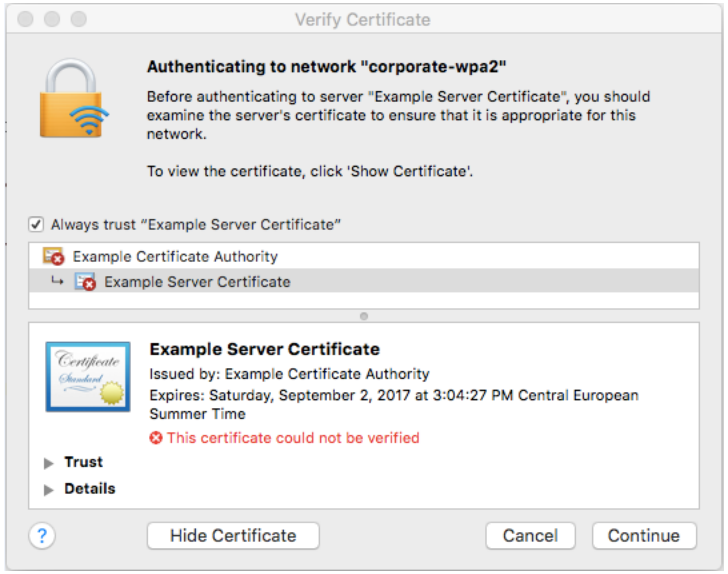
TOKEN FORMAT	TYPE	NORMAL PRICE	ASAP PRICE	DESCRIPTION
(LM|NT)HASH:[0-9a-fA-F]{48}	NET(NT)LM	FREE	N/A	NET(NT)LM hashes captured with the 1122334455667788 challenge (like with SMB Capture or Responder)
$NET(NT)?LM$[0-9a-fA-F]{16}$[0-9a-fA-F]{48}	NET(NT)LM	$20	$200	NET(NT)LM hashes captured with a random challenge
99[a-zA-Z0-9\+/]{35}=	chapcrack	$20	$200	PPTP VPN and WPA-Enterprise MSCHAPv2 authentication captures
$9[78]$[a-zA-Z0-9\+/]{32}	des_kpt	$30	$300	Custom Known-Plaintext DES Cracking or Kerberos5
[0-9a-zA-Z/\.]{13}	des_crypt()	$100	$1000	/etc/passwd 25-round DES hashes full keyspace search

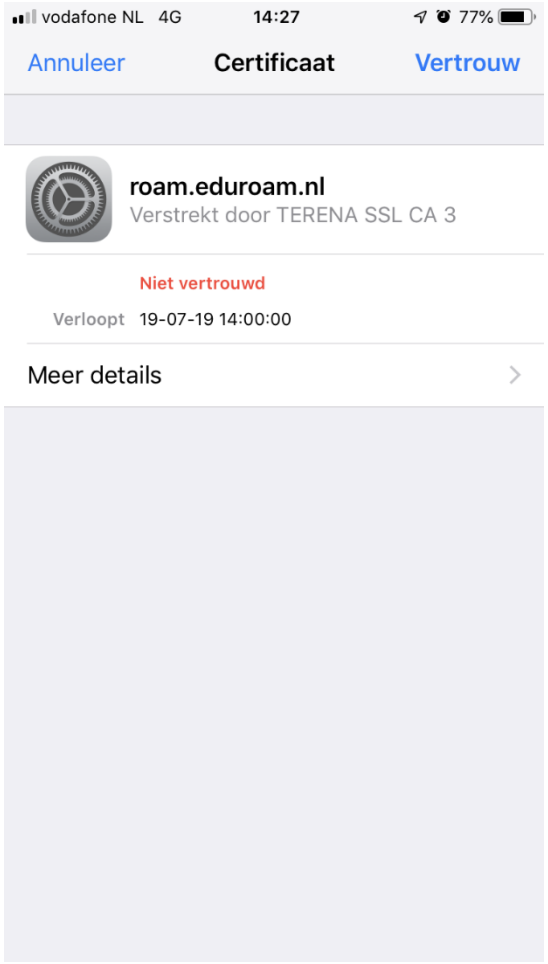
Who are affected?

- Every device that is using EAP-PEAP without (correctly configured) certificate validation
- Without validation the device will send the MS-CHAPv2 challenge without any user interaction to a Rogue AP
- But also EAP-TTLS

User experience







User experience

- Windows / OSX / iOS will generate a certificate warning
- Android by default will automatically connect….
  - But can be configured correctly since Android 7
- But what about the users? Are they ignoring the certificate warning?

Eduroam and govroam institutions, be careful!

EAP-PEAP and locked out accounts

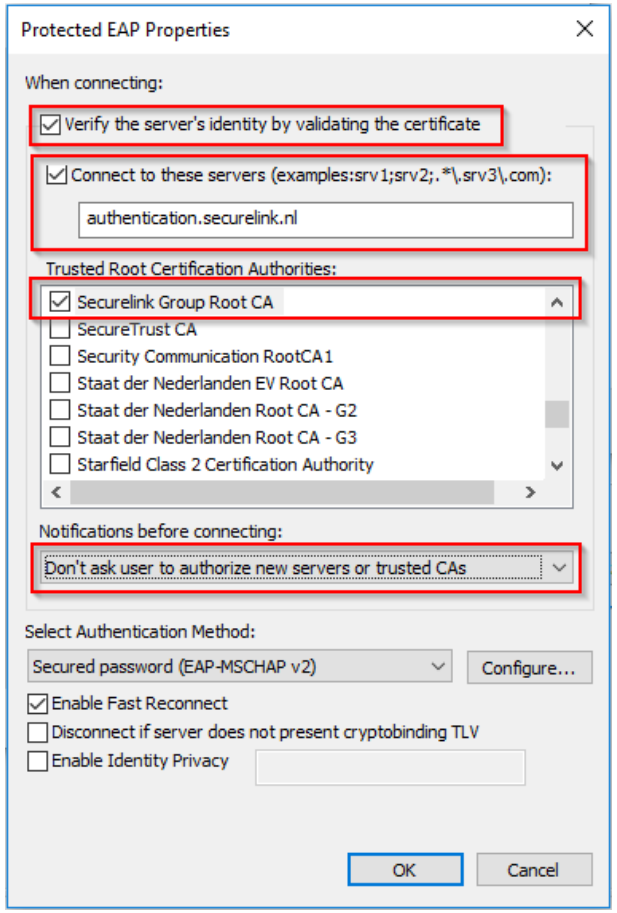
- Devices will automatically connect to network using old password after password change
- This can result in locked out AD account

What now?

- Move to EAP-TLS
- For managed devices it's really simple
  - Even for managed mobile devices with a MDM solution
- EAP-PEAP/EAP-TTLS can be secure if correctly configured
- How to deal with BYOD devices?
  - Onboard (ClearPass onboarding)
  - or….
  - Use a different username/password for 802.1x than the AD password (pseudo ID)

Correctly configured client

– Also configure validation for wired clients and EAP-TLS clients



aruba
a Hewlett Packard Enterprise company

AIRHEADS meetup

Thank you

Willem Bargeman
SecureLink