WPA2

Attacks on Enterprise Networks

Robin Meis
https://robin.meis.space/

16.06.2019

Agenda

Missing Certificate Checks

Using Public CAs

Bypassing “Connect to these servers“

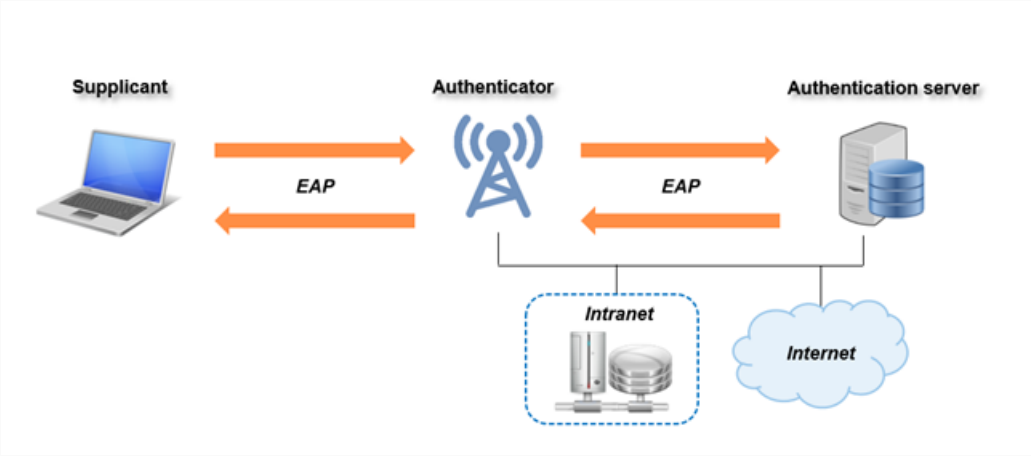
Revealing Domain Credentials

Wardriving

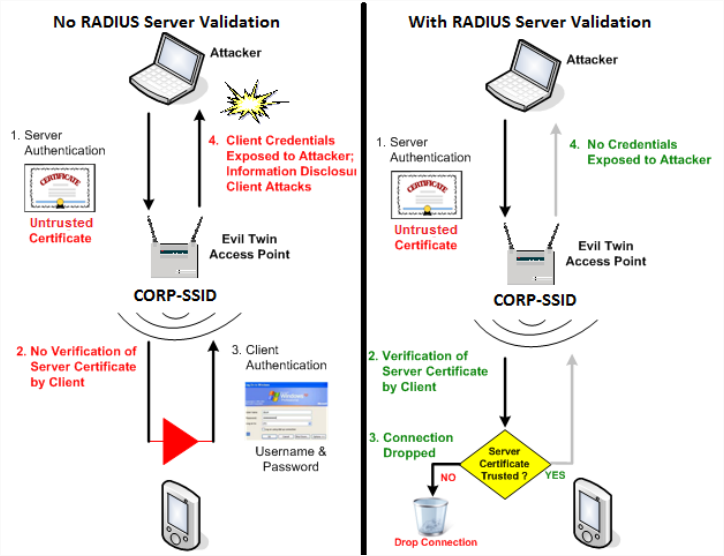

Laurensberg
Soers
Sportpark Soers
Lousberg 262 m
Salvatorberg 229 m
Wingertsberg 195 m
Gewerbegebiet Gruner Weg
Aachen West
Ostfriedhof
Westfriedhof II
Rothe Erde
Continental
Forst
Viertel
Aachen Hauptbahnhof
Haarener Gracht
Berliner Ring
Madrider Ring
Huttenstraße
Pariser Ring
Campus-Boulevard
Schurzelter Straße
Süsterfeldstraße
Soerser Weg
Passstraße
Grüner Weg
Am Gut Wolf
Auf der Hüls
Montzenroute
L 232
L 260
B 57
B 1
B 1a
B 258
B 264
A 544

Missing certificate checks

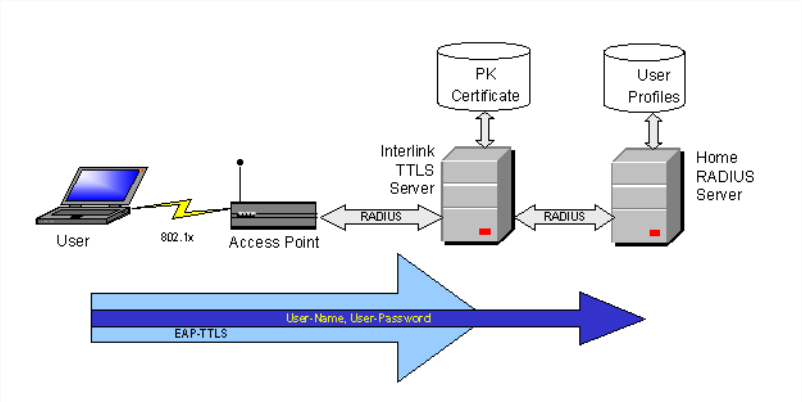
Authentication



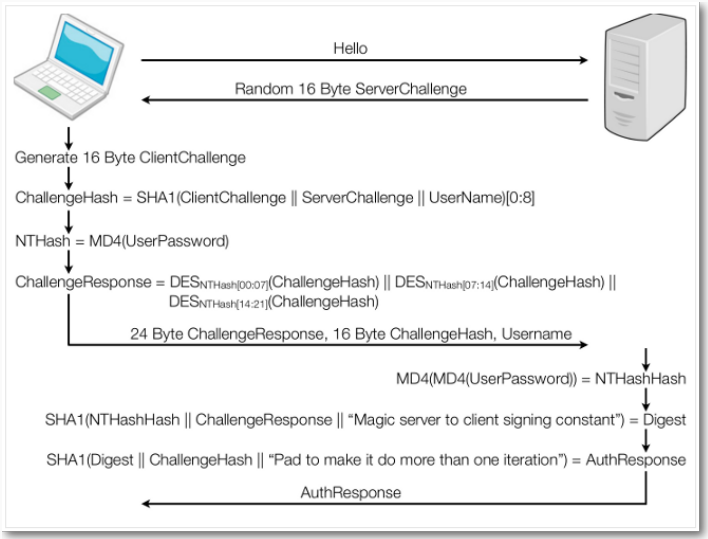
Evil Twin / Rogue Access Point



TTLS / PAP


PK
Certificate
User
Profiles
Interlink
TTLS
Server
Home
RADIUS
Server
RADIUS
RADIUS
User
802.1x
Access Point
User-Name, User-Password
EAP-TTLS

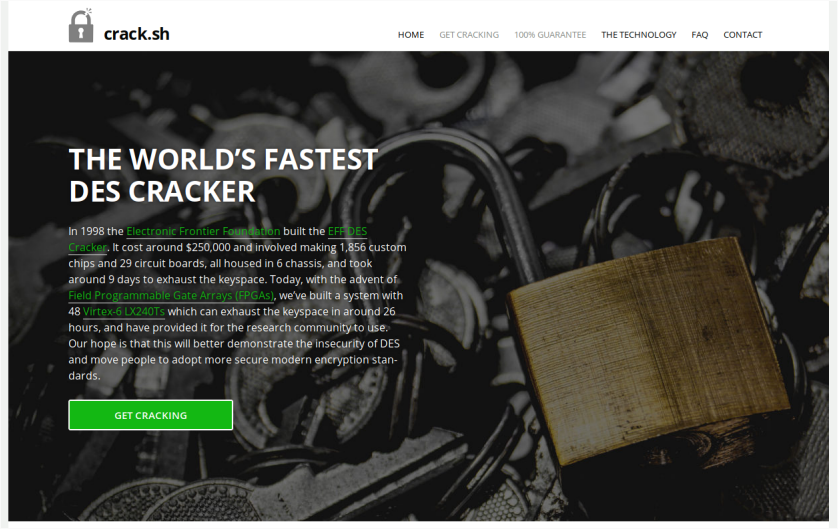
MS-CHAP


Hello
Random 16 Byte ServerChallenge
Generate 16 Byte ClientChallenge
ChallengeHash = SHA1(ClientChallenge || ServerChallenge || UserName)[0:8]
NTHash = MD4(UserPassword)
ChallengeResponse = DES NTHash[00:07](ChallengeHash) || DES NTHash[07:14](ChallengeHash) || DES NTHash[14:21](ChallengeHash)
24 Byte ChallengeResponse, 16 Byte ChallengeHash, Username
MD4(MD4(UserPassword)) = NTHashHash
SHA1(NTHashHash || ChallengeResponse || "Magic server to client signing constant") = Digest
SHA1(Digest || ChallengeHash || "Pad to make it do more than one iteration") = AuthResponse
AuthResponse

Challenge-Resonse (hostapd-wpe)

```
mschapv2
username : domain.de\username
challenge: e5:cf:89:93:7b:83:d7:ee
response : 93:c9:5a:ec:ca:48...
```

crack.sh


crack.sh
HOME
GET CRACKING
100% GUARANTEE
THE TECHNOLOGY
FAQ
CONTACT
THE WORLD'S FASTEST DES CRACKER
In 1998 the Electronic Frontier Foundation built the EFF DES Cracker. It cost around $250,000 and involved making 1,856 custom chips and 29 circuit boards, all housed in 6 chassis, and took around 9 days to exhaust the keyspace. Today, with the advent of Field Programmable Gate Arrays (FPGAs), we've built a system with 48 Virtex-6 LX240Ts which can exhaust the keyspace in around 26 hours, and have provided it for the research community to use. Our hope is that this will better demonstrate the insecurity of DES and move people to adopt more secure modern encryption standards.
GET CRACKING

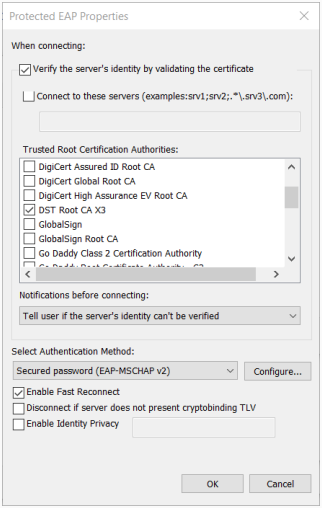
Credentials

```
username: domain.de\username
NT-Hash : 08869782B4E851F9C42DF6B6A6737913
```

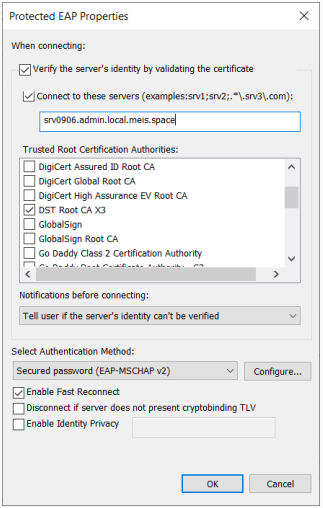
Demo…

Public CAs

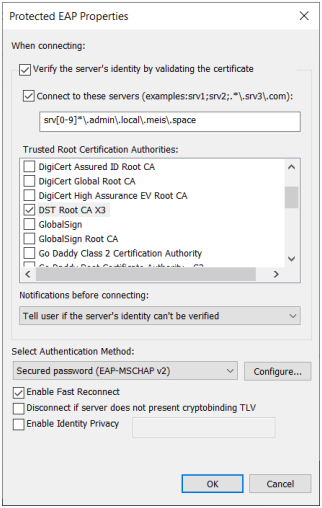
Public CA


Protected EAP Properties
When connecting:
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert High Assurance EV Root CA
DST Root CA X3
GlobalSign
GlobalSign Root CA
Go Daddy Class 2 Certification Authority
Notifications before connecting:
Tell user if the server's identity can't be verified
Select Authentication Method:
Secured password (EAP-MSCHAP v2)
Configure...
Enable Fast Reconnect
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

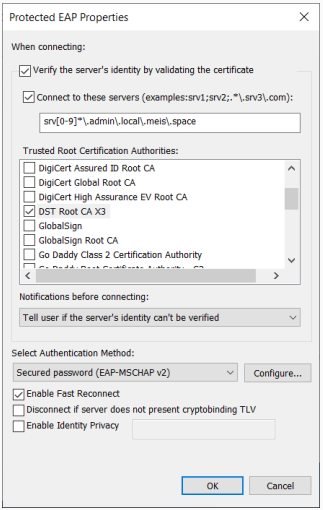
Public CA + Common Name



Public CA + Common Name + Regex

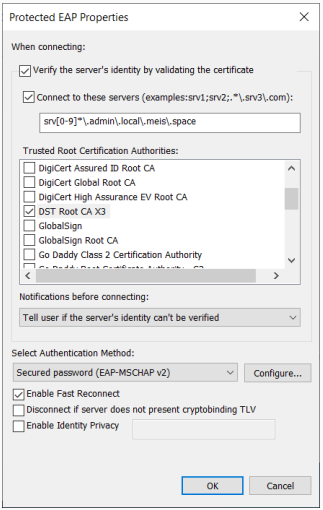


Public CA + Common Name + Regex



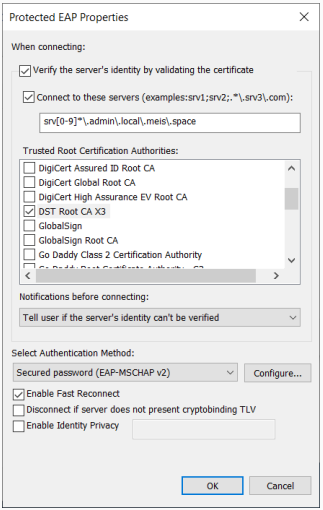
srv1234.admin.local.meis.space

Public CA + Common Name + Regex



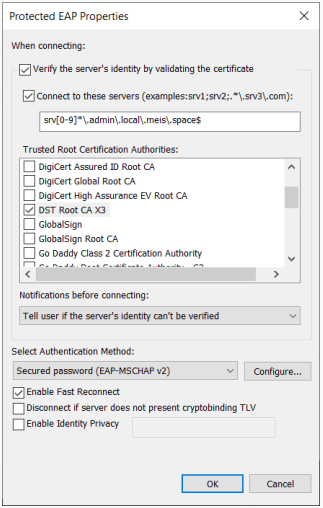
srv12345.admin.local.meis.space

Public CA + Common Name + Regex

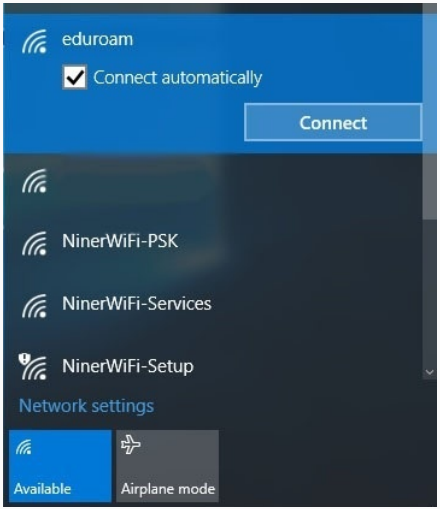


srv1234.admin.local.meis.space.smartnoob.de

Public CA + Common Name + Regex



Revealing Domain Credentials on first connect



Conclusion

Usage of WPA2 Enterprise might reveal domain credentials

Not limited to wireless network, also on 802.1X

Documentation partly insufficient

Default client behaviour is dangerous

Similar attacks in local network using NTLM

Further information

https://robin.meis.space/2018/12/17/
wpa2-enterprise-and-common-security-issues/

https://robin.meis.space/2019/06/09/
connect-to-these-servers-peap

https://docs.microsoft.com/en-us/previous-versions/
windows/it-pro/windows-server-2012-r2-and-2012/
hh994701(v%3Dws.11)

https://docs.microsoft.com/en-us/windows-server/
networking/technologies/nps/nps-crp-reg-expressions