WPA2 – Enterprise

WPA2-Enterprise
or
How to hack it

TuxCoder
2016-09-23

About Me

- Norbert Summer
- Bachelor student for Software & Information Engineering at the TU-Vienna

norbert@o-g.at
@tuxcoder
tuxcoder@jabber.o-g.at

Table of Contents

Connection Methods

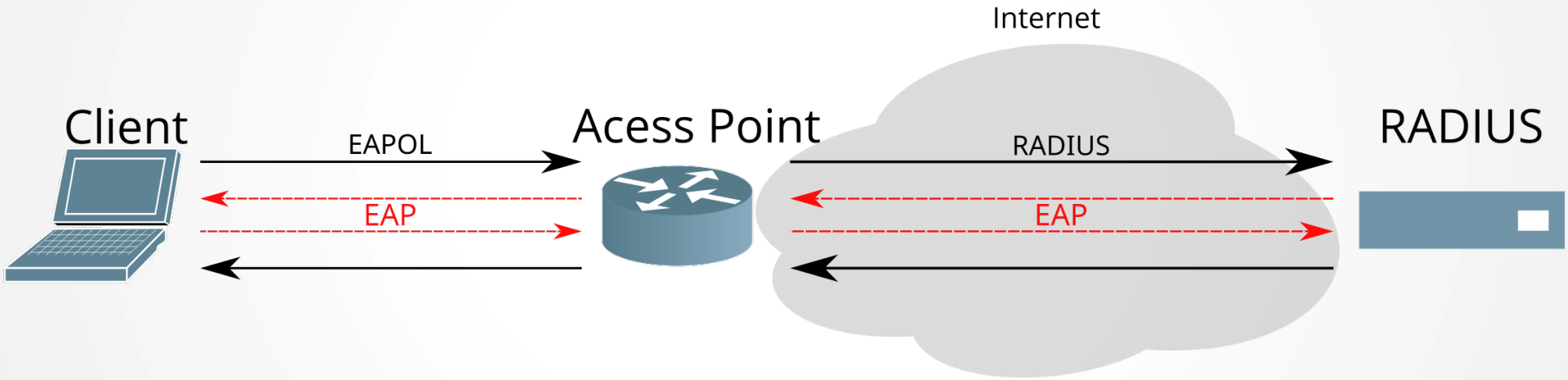
- OPEN – not encrypted
- WEP – cracked in minutes
- WPA(1,2) PSK – partial broken

  51.8kH/s (GTX 660Ti)
- WPA2 Enterprise – deemed to be secure

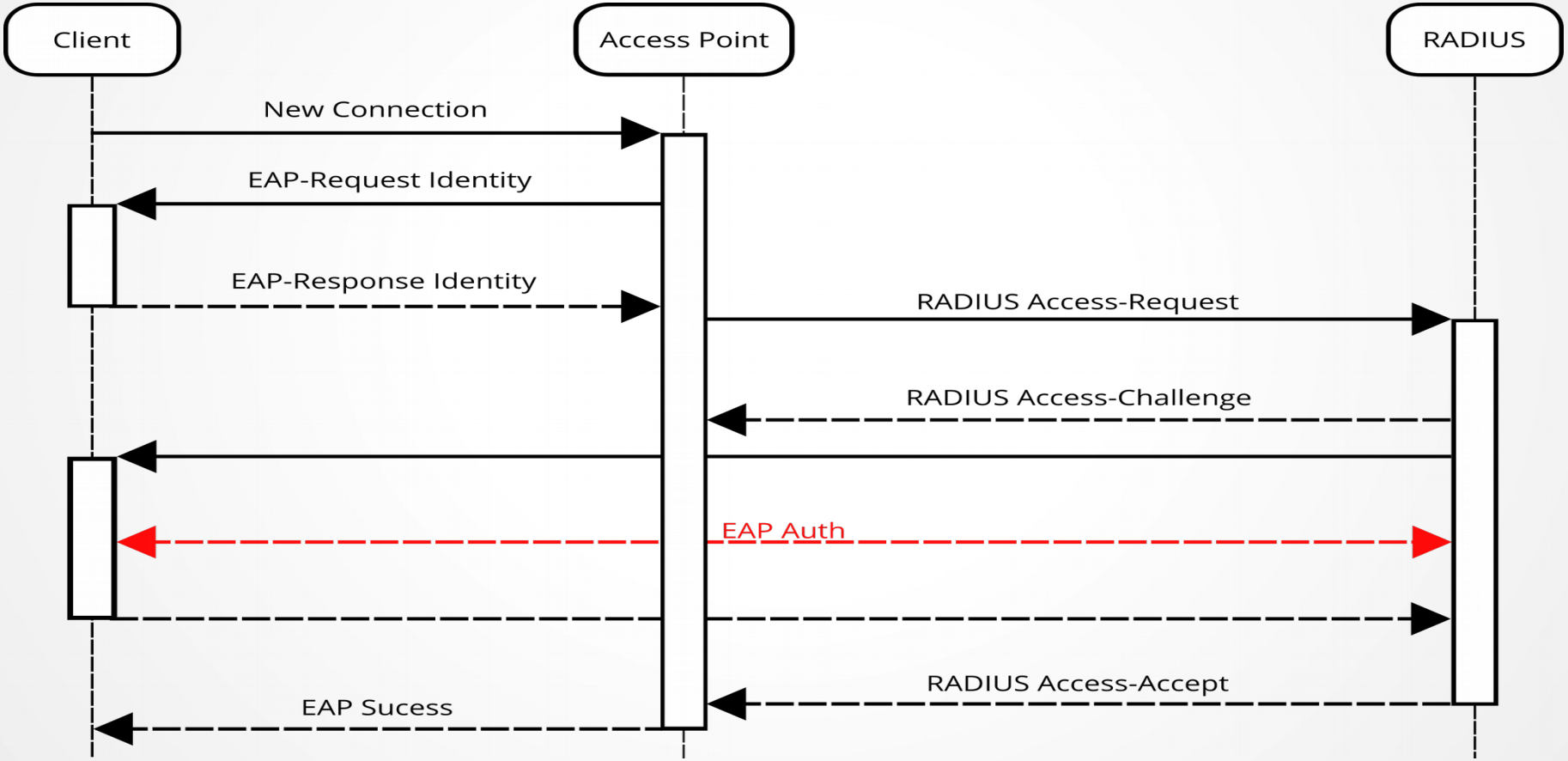
Benefits of WPA2-Enterprise

- Multiple users
- V-LAN (access restriction)
- Different authentication methods
- Used by companies, universities and ISPs

Overview



Workflow


Client
Access Point
RADIUS
New Connection
EAP-Request Identity
EAP-Response Identity
RADIUS Access-Request
RADIUS Access-Challenge
EAP Auth
RADIUS Access-Accept
EAP Sucess

Authentication (Phase 1)

- **PEAP**
- **Tunneled TLS** – (similar to PEAP but a open standard**)**
- **TLS** – client side certificate (only one phase)
- PWD – PSK (only one phase)
- FAST – Cisco
- ….

Authentication (Phase 2)

- **MSCHAPv2**
- **PAP** (Password Authentication Protocol)
- GTC (Generic Token Card)
- MD5-Challenge
- MSCHAPv1
- OTP (One Time Password)
- …..

What could possibly go wrong?

- Problems of a PKI (certificate exchange)
- No good key-exchanges are common
- Whole TLS stuff

Client Problems

- Lots of clients ignore missing certificate check
- Most clients can not validate the CN attribute
  (auth. capture possible)
- IOS does not check the returned hash while MSCHAPv2 auth.
  (MITM posible)
- Some Clients accept expired certificates

Hostapd-wpe

- Patched Hostapd
- JTR

  foo:$NETNTLM$afb7dc907a3a2dd4$
  bfc13c5d4fc4a24127e82ff13df6a9660608d58b2a6df990
- User: foo
- Challenge: afb7dc907a3a2dd4
- Response:
  bfc13c5d4fc4a24127e82ff13df6a9660608d58b2a6df990

Hostapd-wpe on Android

- Rooted Android
- Lil' Debi – chroot debian
- git, gcc, make,…
- W-LAN off

  # modprobe wlan

  # ./hostapd-wpe hostapd.conf

PoC – John The Ripper

- John the Ripper Jumbo
  https://github.com/magnumripper/JohnTheRipper

  # john --format=netntlm-naive hash.txt –fork=8
- ~ 17 MH/s (i7-920@2.6GHz)
- [a-zA-Z0-9]{1,6} ~ 1h worst case

PoC – oclHashcat

- OclHashcat https://github.com/hashcat/oclHashcat
- foo::::bfc13c5d4fc4a24127e82ff13df6a9660608d58b2a6df990:afb7dc907a3a2dd4

  # sed 's/\([^:]*\):\?\$NETNTLM\$\([^$]*\)\$\([^\$]*\)/\1::::\3:\2/'

  # ./oclHashcat -m 5500 hash.txt wordlist.txt
- 2.1GH/s (GTX 660Ti)

PoC – Moxie

- Moxie Marlinspikes, Defcon 20 (2012)
- Cracking MSCHAPv2 100%
- DES cracker based on FPGAs
- https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/ (offline see archive.org)

POC - sensepost

- By Dominic White & Ian de Villiers @ Defcon 22
- Full automatic sniffing, cracking, MiTM
- https://github.com/sensepost/hostapd-mana

How good does it work

- ~5 days
- 2 GPUs (GTX 660Ti,AMD HDxxxx)
- 200 Hashes captured
- 43 of them cracked
- Wordlist and hybrid attack

Consequences

- Liability of ISPs
- Access to services with the linked passwords
- Access to private networks
- Record and manipulate traffic

Possible Solutions

- Self signed certificates and validation
- Different passwords for WIFI access and other services, better password policy (12+ characters)
- Better Clients (or apps to configure it right) https://cat.eduroam.org/

- Better WIFI standards with current hash functions
  - **EAP-SRP-256** (better with TTLS/PEAP)

Thank you for your attention

TuxCoder

Mail: norbert@o-g.at

PGP: DE76 DC79 727D ED71 3C60 5393 A50A E759 388A 158E