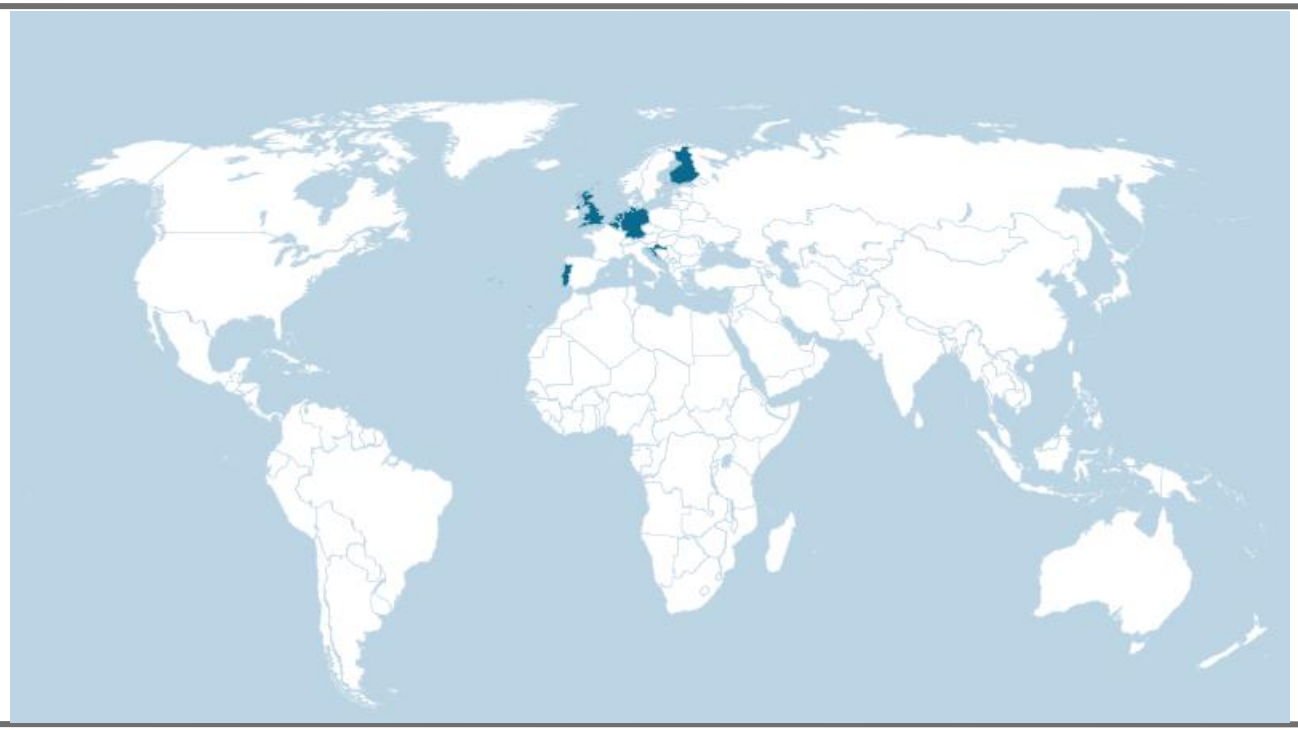
HRVATSKI CENTAR KOMPETENCIJA ZA HPC

Primjer korištenja HPC-a u nastavi: Analiza sigurnosti lozinka

Toni Perkovic

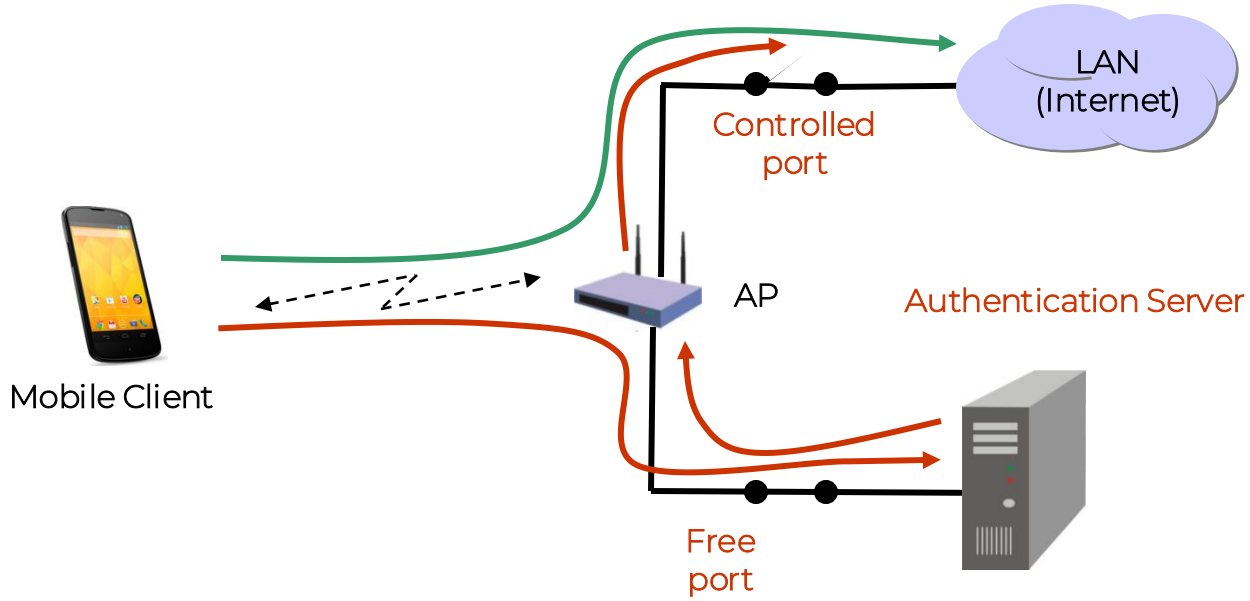
EURO²
Financira Europska unija
EuroHPC Joint Undertaking
srce
Sveučilište u Zagrebu
Sveučilišni računski centar

WPA2-Enterprise: eduroam



eduroam (**edu**cation **roam**ing) je sigurna, svjetska usluga roaming pristupa razvijena za međunarodnu istraživačku i obrazovnu zajednicu. Omogućuje internetsku povezivost diljem kampusa

WPA2-Enterprise: IEEE 802.1X



- Mobilni klijent šalje zahtjev (želi se spojiti na mrežu)
- AP kontrolira pristup uslugama (Controlled port)
- Autentifikacijski poslužitelj (AS):
  - Mobilni klijent i AS međusobno se autentificiraju
  - Nakon uspješne autentifikacije, AS obavještava AP da otvori Controlled port za mobilnog klijenta

WPA2-Enterprise: EAP in 802.1X

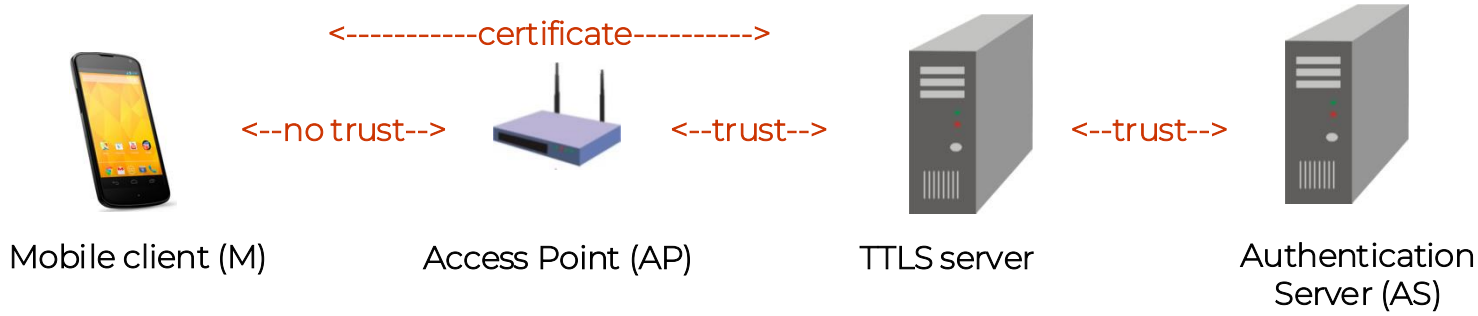
EAP Type	Upotreba u svijetu
PEAP	Najviša
EAP-TTLS	Visoka
EAP-TLS	Srednja
LEAP	Niska
EAP-FAST	Niska
…	…

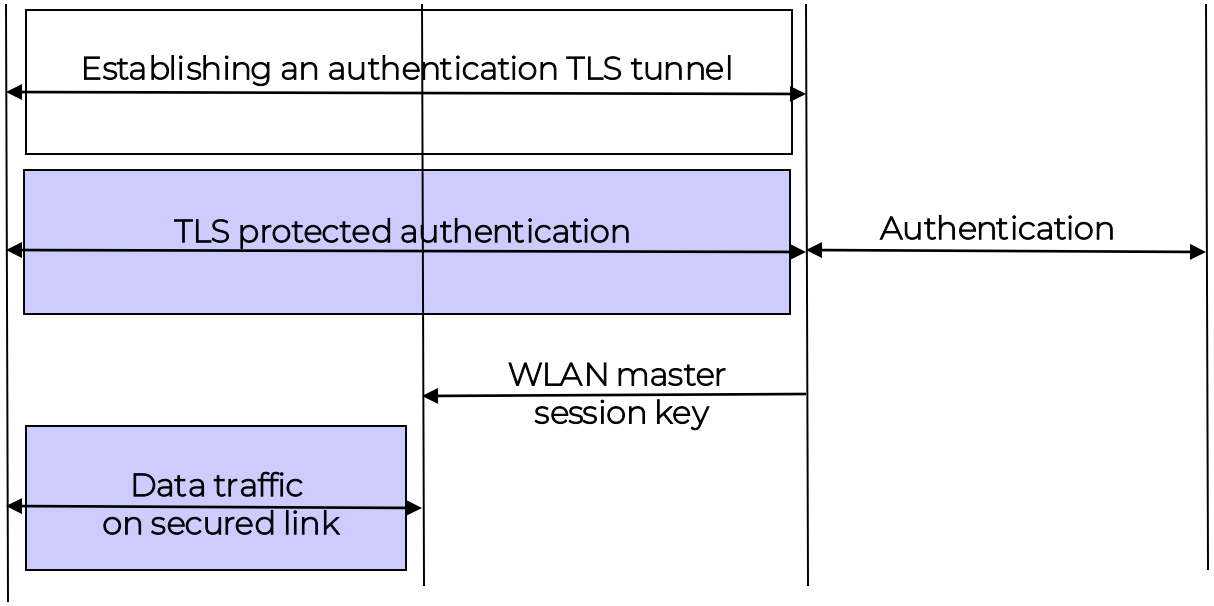
Eduroam's WiFi

- EAP-TTLS (+ PAP: Password Authentication Protocol)
  U 802.1X/EAP mreži postoje mnogi oblici autentifikacije, a jedan od sigurnijih oblika je EAP-TTLS. EAP-TTLS poznat je kao tunelirana metoda autentifikacije. Njegova sigurnost leži u činjenici da se prije slanja korisničkih vjerodajnica autentifikacijskom poslužitelju, između korisničkog klijenta i autentifikacijskog poslužitelja na koji se vjerodajnice prenose, postavlja TLS tunel. Prednosti korištenja takvog tunela su da se ne samo štite vjerodajnice korisnika,
  već se omogućuje i provjera autentifikacijskog poslužitelja na temelju njegovog TLS certifikata.

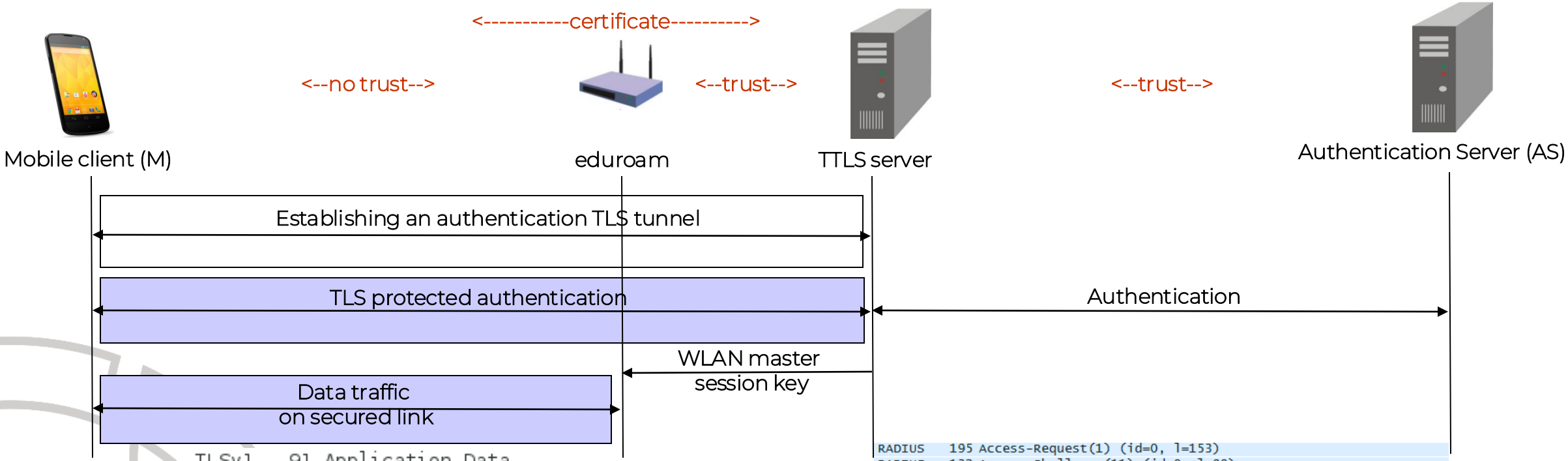
WPA2-Enterprise: EAP–TTLS

- Tunneled TLS over Extensible Authentication Protocol (EAP-TTLS)
  - Pruža zaštitu za početne poruke za autentifikaciju (lozinke u običnom tekstu, npr. PAP koje koristi **eduroam**) koje se prenose putem javnog bežičnog kanala.
  - Početne poruke za autentifikaciju razmjenjuju se putem SSL/TLS tunela.





WPA2-Enterprise: EAP–TTLS

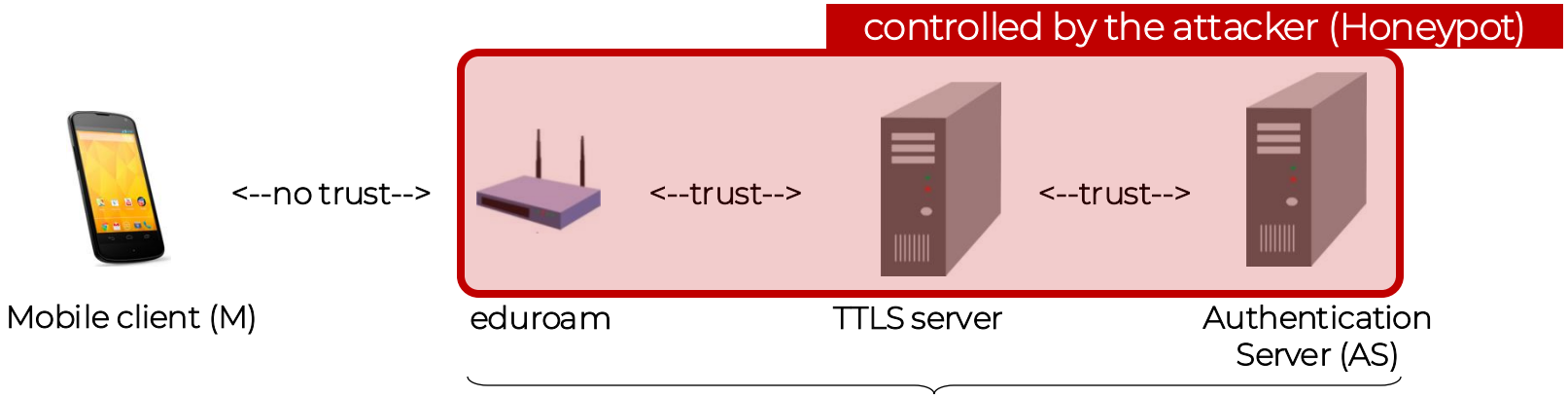



```
TLSv1    91 Application Data
TLSv1   115 Application Data
TLSv1   107 Application Data
TLSv1    91 Application Data
TLSv1   131 Application Data
TLSv1   163 Application Data
TLSv1   139 Application Data
TLSv1    91 Application Data
TLSv1   163 Application Data
TLSv1    99 Application Data
```

```
RADIUS   195 Access-Request(1) (id=0, l=153)
RADIUS   132 Access-Challenge(11) (id=0, l=90)
RADIUS   264 Access-Request(1) (id=0, l=222), Duplicate Request ID:0
RADIUS    52 Access-Challenge(11) (id=0, l=1490), Duplicate Response ID:0
RADIUS   214 Access-Request(1) (id=0, l=172), Duplicate Request ID:0
RADIUS  1453 Access-Challenge(11) (id=0, l=1411), Duplicate Response ID:0
RADIUS   546 Access-Request(1) (id=0, l=504), Duplicate Request ID:0
RADIUS   187 Access-Challenge(11) (id=0, l=145)
RADIUS   214 Access-Request(1) (id=0, l=172), Duplicate Request ID:0
RADIUS   161 Access-Challenge(11) (id=0, l=119), Duplicate Response ID:0
RADIUS   267 Access-Request(1) (id=0, l=225), Duplicate Request ID:0
RADIUS   177 Access-Challenge(11) (id=0, l=135), Duplicate Response ID:0
RADIUS   243 Access-Request(1) (id=0, l=201), Duplicate Request ID:0
RADIUS   201 Access-Challenge(11) (id=0, l=159), Duplicate Response ID:0
RADIUS   315 Access-Request(1) (id=0, l=273), Duplicate Request ID:0
RADIUS   209 Access-Challenge(11) (id=0, l=167), Duplicate Response ID:0
RADIUS   243 Access-Request(1) (id=0, l=201), Duplicate Request ID:0
RADIUS   233 Access-Challenge(11) (id=0, l=191), Duplicate Response ID:0
RADIUS   251 Access-Request(1) (id=0, l=209), Duplicate Request ID:0
RADIUS   354 Access-Accept(2) (id=0, l=312)
```

Sigurnosni problem eduroam WiFi mreže

- Eduroam nije siguran od aktivnih napada

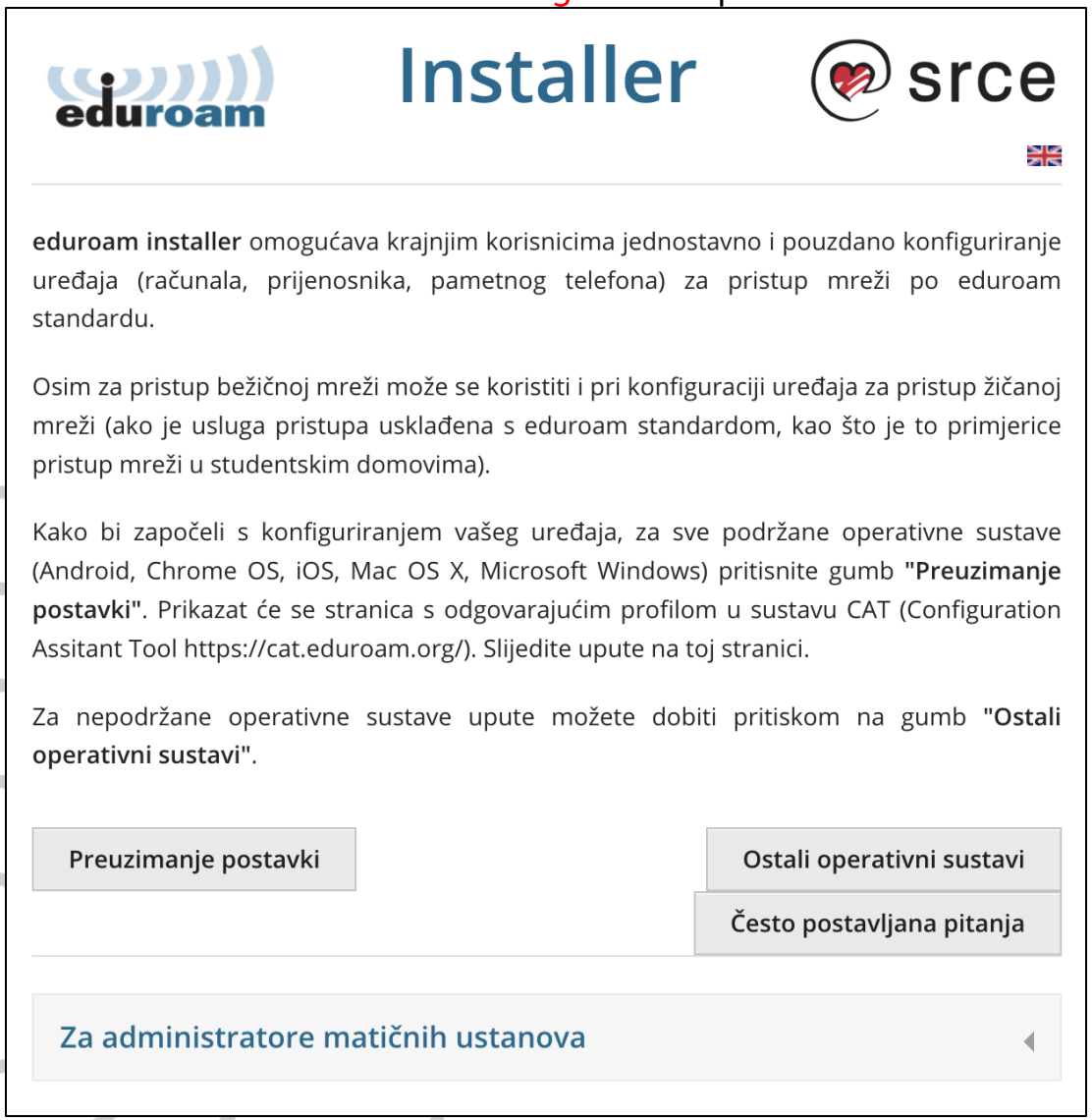


Kali Linux

WiFi card

WPA2-Enterprise: Upotrebljivost vs. Sigurnost

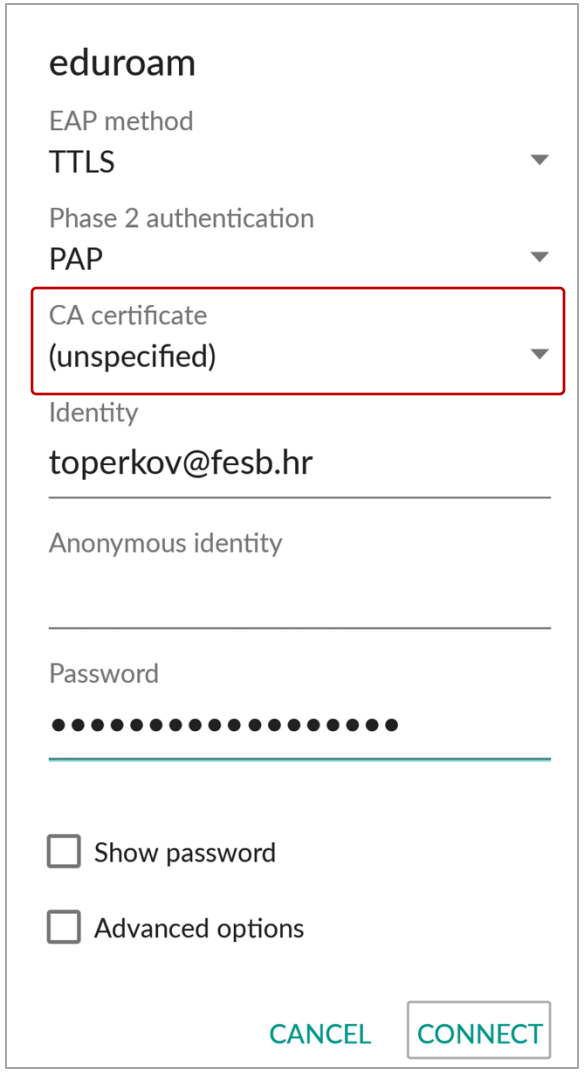
- Što korisnici moraju napraviti



SSID	eduroam
key-management	WPA-EAP (WPA2 i WPA3)
kripto-komunikacija	AES
CA root certifikat	ca.fesb.hr.der
ime radius servera	freeradius.fesb.hr
EAP algoritam	EAP-TTLS
autentikacija	PAP
korisnička oznaka	[uid]@fesb.hr (pero@fesb.hr) *ista s vanjskom korisničkom oznakom*

WPA2-Enterprise: Upotrebljivost vs. Sigurnost

- Što korisnici zapravo rade



Klijent NE provjerava autentifikacijski poslužitelj (AS)

SSID	eduroam
key-management	WPA-EAP (WPA2 i WPA3)
kripto-komunikacija	AES
CA root certifikat	ca.fesb.hr.der
ime radius servera	freeradius.fesb.hr
EAP algoritam	EAP-TTLS
autentikacija	PAP
korisnička oznaka	[uid]@fesb.hr (pero@fesb.hr) *ista s vanjskom korisničkom oznakom*

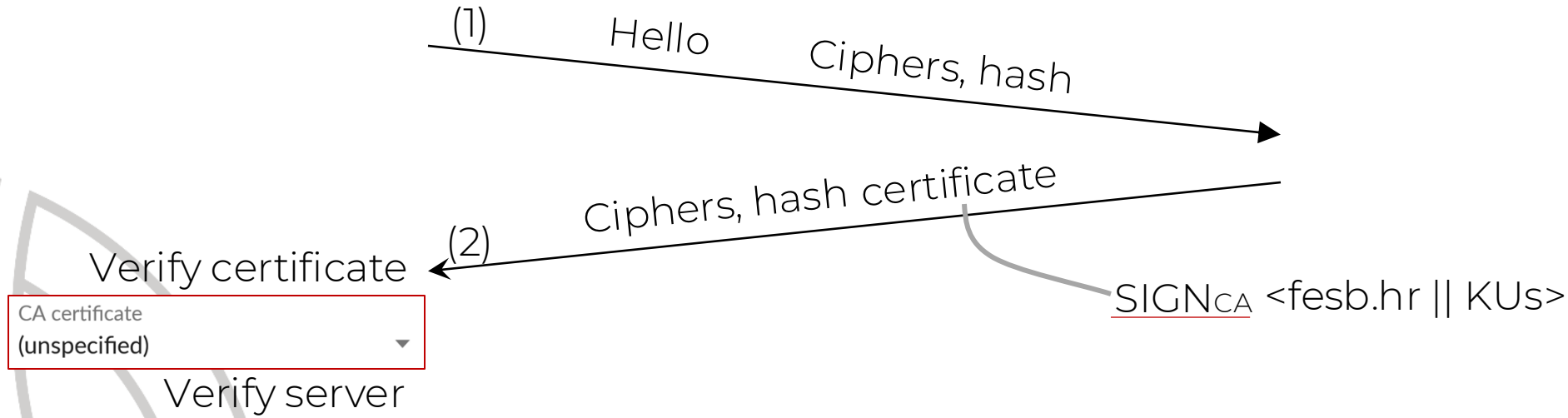
- vs Eduroam installer

Security problem with eduroam's WiFi

- EAP-TTLS (+ PAP: Password Authentication Protocol)

  U 802.1X/EAP mreži postoje mnogi oblici autentifikacije, a jedan od sigurnijih oblika je EAP-TTLS. EAP-TTLS poznat je kao tunelirana metoda autentifikacije. Njegova sigurnost leži u činjenici da se prije slanja korisničkih vjerodajnica autentifikacijskom poslužitelju, između korisničkog klijenta i autentifikacijskog poslužitelja na koji se vjerodajnice prenose, postavlja TLS tunel.

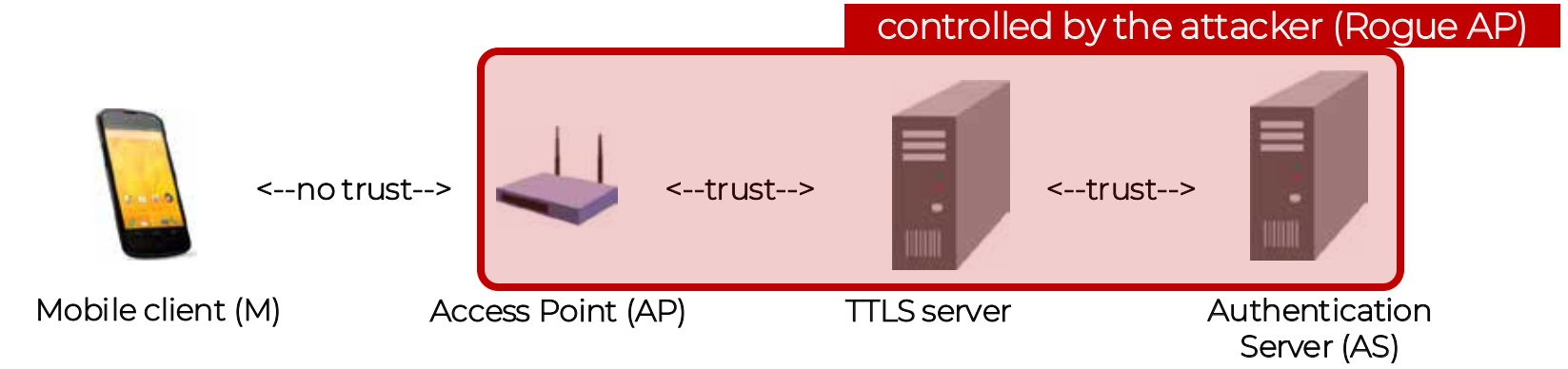
  Prednosti korištenja takvog tunela su da se ne samo štite vjerodajnice korisnika, već se omogućuje i provjera autentifikacijskog poslužitelja na temelju njegovog TLS certifikata.



- Klijent NE provjerava autentifikacijski poslužitelj (AS)
- Onemogućavanjem provjere certifikata poslužitelja možemo uspješno pokrenuti napad lažnim predstavljanjem - Honeypot

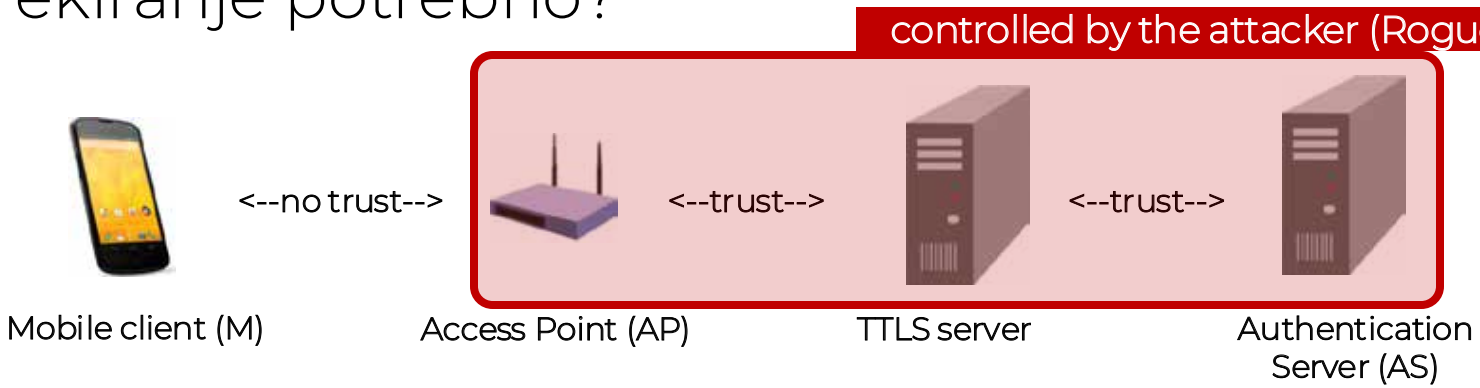
Security problem with eduroam's WiFi

- Eduroam nije siguran od aktivnih napada kada korisnici izostave validaciju certifikata

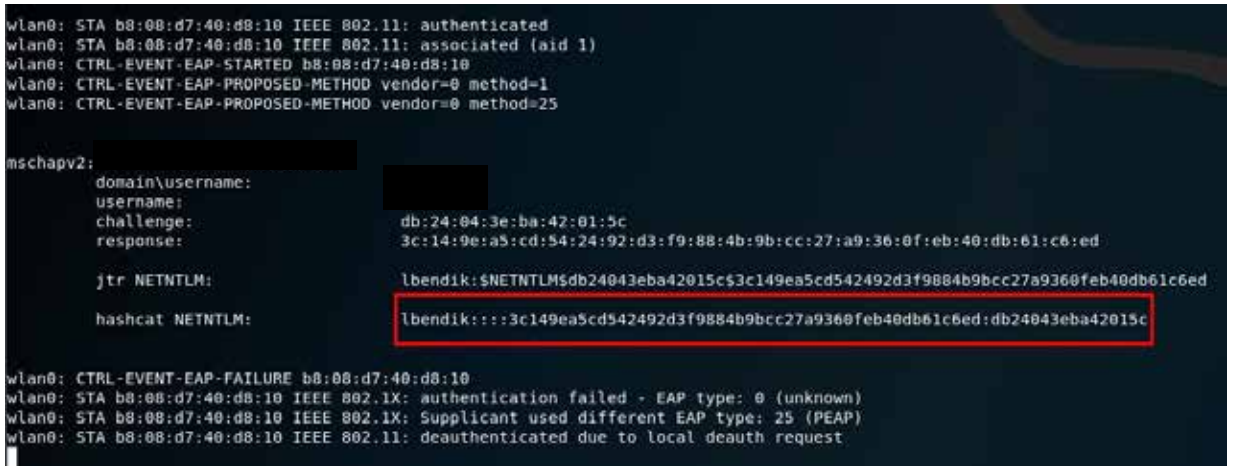


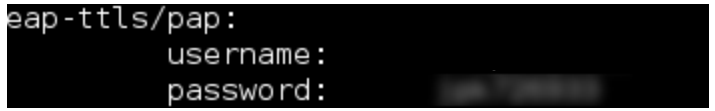
Security problem with eduroam's WiFi

- Zašto je krekiranje potrebno?



WPA2 & WPA3 Enterprise Common Protocols	Level of Encryption	Credentials
EAP-TLS	Public-Private Key Cryptography	Passwordless
PEAP-MSCHAPv2	Bad Encryption (MD4, Compromised since 1995)	Passwords
EAP-TTLS/PAP	No Credential Encryption	Passwords





Uobičajene Tehnike Krekiranja

Dictionary + Rules

Mask / Hybrid

Rainbow Table

Pure brute force

Kriterij uspjeha:
Kompleksnost algoritma
Duljina lozinke
Poznata kompleksnost
predvidivi elementi
Hardver

Kako Mogu Razbiti Hasheve?

Ukratko, pogađamo *plaintetxt*, pretvaramo ga u hash i uspoređujemo hashove, vrlo brzo.

Budući da je cracking hash-a često dinamično, GPU-ovi su jedni od najbolje opreme za ovaj zadatak i često se upotrebljavaju.

Neki se algoritmi bolje izvode na CPU-u, poput Argon2 i PBKDF2.

Hashcat
https://github.com/hashcat/hashcat

JohnTheRipper
https://github.com/openwall/john

Mdxfind
https://www.techsolvency.com/pub/bin/mdxfind/

Hash Crackiranje na Supeku

srce

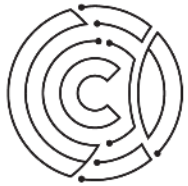
Primjer apptainera

```
# Preuzmi hashcat i izgradi sliku kontejnera
apptainer build hashcat.sif docker://dizcza/docker-hashcat

# premještanje slike sa scratch diska u korisnički direktorij

mv hashcat.sif $HOME/radionica_hashcat/basic

# premještanje u korisnički direktorij

cd $HOME/radionica_hashcat/basic
```

Primjer gpu.sh

```
#PBS -q gpu-test
#PBS -l select=1:ncpus=4:ngpus=1:mem=8gb
#PBS -l walltime=00:30:00
#PBS -N hashcat-benchmark
#PBS -o hashcat_output.log
#PBS -e hashcat_error.log

cd $PBS_O_WORKDIR

module load libs/cuda

HASH_FILE="hash_from_docx.txt"
WORDLIST="top100.txt"
RULE="best64.rule"

apptainer exec hashcat.sif hashcat \
-m9600 \
-a0 $HASH_FILE $WORDLIST \
-r $RULE
--status
```

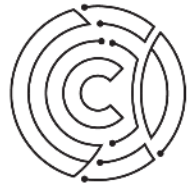
Supek benchmark



```
---------------
* Hash-Mode 0 (MD5)
---------------
Speed.#1.....: 67544.1 MH/s (53.32ms) @ Accel:64 Loops:1024 Thr:512 Vec:1
-------------------
* Hash-Mode 100 (SHA1)
-------------------
Speed.#1.....: 21947.1 MH/s (82.25ms) @ Accel:64 Loops:1024 Thr:256 Vec:1
-----------------------
* Hash-Mode 1400 (SHA2-256)
-----------------------
Speed.#1.....:  9493.5 MH/s (95.14ms) @ Accel:8 Loops:1024 Thr:1024 Vec:1
-----------------------
* Hash-Mode 1700 (SHA2-512)
-----------------------
Speed.#1.....:  3192.9 MH/s (70.67ms) @ Accel:32 Loops:256 Thr:256 Vec:1
-------------------------------------------------------------
* Hash-Mode 22000 (WPA-PBKDF2-PMKID+EAPOL) [Iterations: 4095]
-------------------------------------------------------------
Speed.#1.....:  1116.9 kH/s (48.98ms) @ Accel:8 Loops:512 Thr:512 Vec:1
--------------------
* Hash-Mode 1000 (NTLM)
--------------------
Speed.#1.....:   114.8 GH/s (31.22ms) @ Accel:32 Loops:1024 Thr:1024 Vec:1
-------------------
* Hash-Mode 3000 (LM)
-------------------
Speed.#1.....: 64973.0 MH/s (13.66ms) @ Accel:64 Loops:1024 Thr:128 Vec:1
```

srce

SUPEK: Napad uz hashcat apptainer



BRUTE FORCE:

```
> apptainer exec --nv --bind hashcat.sif hashcat -m 5500 /lab/mschap.hash \
  -a 3 ?d?d?d?d?d?d?d?d --username -w 3 -O \
  --session=mschap_pin --potfile-path /lab/mschap_pin.pot
```

RULE-BASED ATTACK:

```
> apptainer exec --nv --bind hashcat.sif hashcat -m 5500 /lab/mschap.hash \
  /lab/pap_roots.txt -a 0 -r /lab/custom.rule --username -w 3 -O \
  --session=mschap_rules --potfile-path /lab/mschap_rules.pot
```

HYBRID - CUSTOM RULES BASED ON ANALYSIS

- Sakupi uzorak lozinki (npr. 200) u plain-text observed.txt
- Analiziraj uzorak: dužine, učestalosti znak-klasa po poziciji, zajednički prefix/suffix, ponavljanja.
- Izvedi najvjerojatnije mask(e) i pravila (npr. `PREFIX + 4digits + !` → mask `?u?l?l?l?d?d?d?d?s`).

```
> apptainer exec --nv --bind hashcat.sif hashcat -m 5500 /lab/mschap.hash \
  /lab/pap_roots.txt -a 6 ?d?d?d?d --username \
  --session=lab_hybrid_4d --potfile-path /lab/pot_hybrid_4d.pot -w 3 -O
```

srce

HRVATSKI CENTAR KOMPETENCIJA ZA HPC

Hvala na pažnji

toperkov@fesb.hr

Projekt EuroCC 2 financiran je sredstvima Zajedničkog poduzeća za europsko računarstvo visokih performansi (EuroHPC JU) i sredstvima Njemačke, Bugarske, Austrije, Hrvatske, Cipra, Češke, Danske, Estonije, Finske, Grčke, Mađarske, Irske, Italije, Litve, Latvije, Poljske, Portugala, Rumunjske, Slovenije, Španjolske, Švedske, Francuske, Nizozemske, Belgije, Luksemburga, Slovačke, Norveške, Turske, Sjeverne Makedonije, Islanda, Crne Gore i Srbije pod brojem Ugovora 101101903.