FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE SPLIT

WPA2 Enterprise

Računalna forenzika - seminarski rad

Ivan Lukšić
Bruno Grbavac

Diplomski studij računarstva (250)
Akademska godina 2021./22.

Sadržaj

1 Uvod u 802.1X

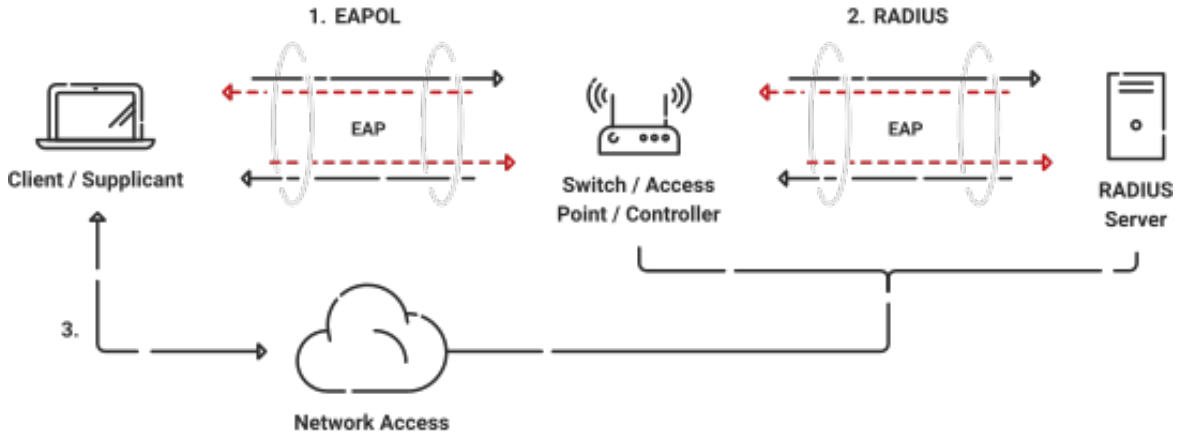
Mrežne okoline s **velikim brojem korisnika** donose posebne prepreke u sigurnom korištenju mreže. Naime, za razliku od osobnih (kućnih), WPA2 Personal bežičnih mreža, mreže s velikim brojem korisnika (npr. korporacije, fakulteti, javne ustanove itd.) ne mogu koristiti dijeljenu tajnu za pristup mreži (*eng.* PSK - Pre-Shared Key).
Naime, takav pristup ne koristi se iz više praktičnih razloga: u tom slučaju ukidanje pristupa pojedincu zahtjevalo bi promjenu zaporke za sve korisnike, nadalje, takav pristup ne dopušta praćenje pristupa mreži od strane pojedinaca itd. **WPA2 Enterprise** mreže stoga autenticiraju korisnike koji pristupaju mreži putem **RADIUS** (*eng.* Remote Authentication Dial-In User Service) servera koji provjerava priložene korisničke podatke zahtjeva za konekciju s podacima u centraliziranoj bazi (komunicira najčešće LDAP ili SAML protokolom) važećih korisnika ustanove, te ovisno o korisniku i sigurnosnoj politici ustanove odobrava određeni nivo pristupa mreži. [10]

Slika 1: 802.1X mreža [10]

2 EAP - Extensible Authentication Protocol

EAP je skup standardnih protokola koji omogućavaju sigurno slanje informacija za mrežnu autentikaciju. Različiti EAP protokoli, često se nazivaju i EAP metode, a dijele se na metode koje autentikaciju temelje na **korisničkim podacima za autentikaciju** (*eng.* credentials) (EAP-TTLS/PAP i PEAP-MSCHAPv2) te one koje se temelje na **digitalnim certifikatima** (EAP-TLS). [10]

3 Elementi 802.1X mreže



Slika 2: Elementi 802.1X mreže [10]

- **Suplikant** - kako bi se klijent uspješno autenticirao, uređaj mora imati instaliran softver kojeg nazivamo suplikantom (podnositeljem zahtjeva). Suplikant sadrži podatke o mrežnoj konfiguraciji i konekciji (certifikati ili korisnički kredencijali), pa mu je stoga glavna zadaća je sudjelovanje u inicijalnoj EAP transakciji u kojoj šalje korisničke podatke **autentikatoru** (pristupnoj točki ili switchu) u svrhu uspostave veze. U slučaju izostanka suplikanta na uređaju, EAP okviri poslani od strane pristupne točke bili bi ignorirani. Ovaj softver automatski je podržan na većini uređaja. [10]

- **Autentikator** - pristupna točka ili switch imaju ulogu posrednika u uspostavi 802.1X konekcije. Autentikator inicira komuikaciju slanjem EAPOL-Start paketa prema klijentu koji se pokušava spojiti na mrežu. Ovisno o konfiguraciji WSS-a (*eng.* Wireless Security Settings) klijentov odgovor sa kredencijalima ili certifikatom se proslijeđuje određenom RADIUS serveru.
  U slučaju da mu je pristup dozvoljen autentikator prima od RADIUS-a **Access_Accept** paket koji sadrži informacije o načinu na koji je potrebno na mrežu povezati klijenta: na koji virtualni LAN spojiti klijenta (*npr.* VLAN za zaposlenike i VLAN za goste), skup Access Control listi koje je potrebno predati klijentu itd..
  Ovaj način personalizacije mrežnih postavki ovisno o korisniku od strane RADIUS servera naziva se *"User Based Policy Assignment"* i jedan je od ključnih svojstava Enterprise mreža. [10]

- **RADIUS server** - RADIUS server element je ove infrastrukture koji donosi odluku o pristupu klijenta mreži. Kredencijale ili digitalni certfikat kojeg mu je proslijedio autentikator RADIUS uspoređuje s podacima odobrenih korisnika te sprječava pristup klijentima koji se ne nalaze među navedenima.
  Bitna sigurnosna značajka pri postavljanju 802.1X mreže je korištenje postupka **validacije certifikata servera**. Ovaj postupak osigurava da se klijent povezuje na željeni server potvrđivanjem certifikata koji server šalje pri početku komunikacije. U slučaju da ovaj postupak nije implementiran na uređaju klijenta, komunikacija je podložna **Evil Twin** napadu.
  Postojanje RADIUS servera kao zasebnog elementa opravdano je jedinom drugom opcijom u kojoj same pristupne točke izvršavaju RADIUS server, što bi bilo podosta zahtjevno za njih. [10]

- **Pohrana identiteta** - 802.1X zahtjeva pohranu korisničkih podataka - korisničkih imena i lozinki u direktoriju s kojim će komunicirati RADIUS serveer (LDAP ili Active Directory server). [10]

4 Koraci autentikacije

Autentikacija u WPA2 Enterprise mrežama odvija se kroz četiri koraka.[10]

1. **Inicijalizacija** - autentikator detektira klijentski uređaj koji pokušava uspostaviti vezu, taj port autentikatora postavlja se u "neautorizirano" stanje, te se stoga propušta samo 802.1X promet.

2. **Inicijacija** - autentikator EAPOL-Start paketom započinje slanje EAP zahtjeva ka klijentu te kao odgovor prima EAP odgovor. Podaci iz odgovora se zatim prosljeđuju RADIUS serveru u obliku RADIUS access request paketa.

3. **Pregovori** - primivši request paket server odgovara ***RADIUS access challenge*** paketom, koji sadrži odobrenu EAP metodu za uređaj koji je poslao zahtjev. Taj se paket preko autentikatora prosljeđuje uređaju čiji se cilj autenticirati.

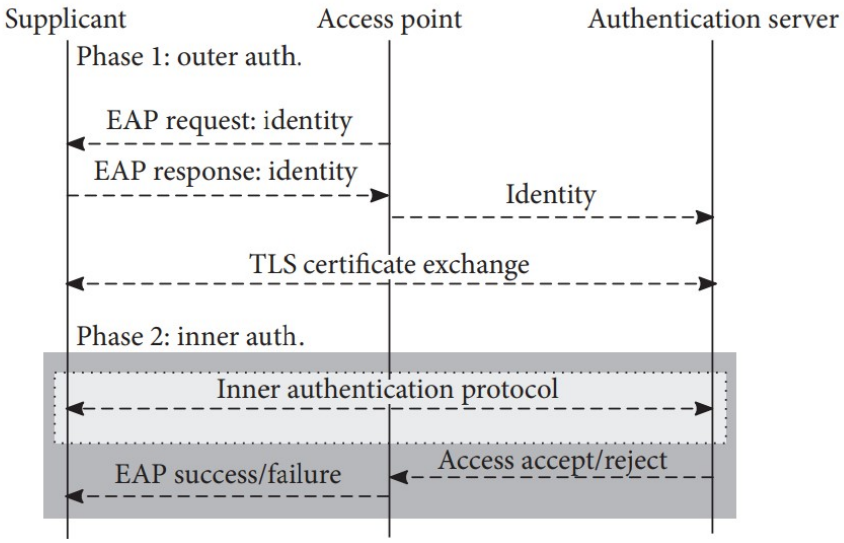
4. **Autentikacija** - primivši EAP challenge, uređaj se konfigurira za određenu EAP metodu, autentikacijski server mu šalje konfiguracijske profile kako bi bio autenticiran. Autenticiravši se, uređaj postiže da je port na koji je spojen prelazi u stanje "authorized" i dobiva pristup mreži.

WPA2 - EAP	EAP-TLS	PEAP-MSCHAPV2	EAP-TTLS/PAP
Enkripcija	Asimetrična kriptografija	Enkriptirani podaci	Ne-enkriptirani podaci
Brzina autentikacije	Brzo - 12 koraka	Sporo - 22 koraka	Najsporije - 25 koraka
Direktoriji aktivnih korisnika	SAML/LDAP/MFA serveri	Active Directory	Non-AD LDAP serveri
Korisničko isksutvo	Najbolje	Prihvatljivo	Loše

Tablica 1: Pregled često korištenih EAP metoda. [10]

5 Autentikacijske metode

U ovom poglavlju opisani su protokoli odnosno metode autentikacije pri 801.1X mrežama. Autentikacija kod 802.1X odvija se kroz "dvije faze", prva "vanjska" faza ima za cilj uspostavu TLS tunela. Naime na podražaj pristupne točke, suplikant predstavlja svoj identitet koji se prosljeđuje RADIUS serveru, koji, u slučaju uspješne provjere identiteta suplikantu preko autentikatora prosljeđuje certifikat servera. Autentikacijom certifikata, uspostavlja se tunel između RADIUS servera i suplikanta. Druga faza autentikacije sastoji se od suplikanta koji svoje kredencijale šalje sigurnim tunelom RADIUS serveru. Ovisno o uspješnosti autentikacije podataka, suplikantu se odija odnosno dopušta pristup mreži. [Quote perković] [3][5][8][9][11]



Slika 3: Autentikacija u 802.1X [11]

- **PAP** - protokol "unutarnje" autentikacije u kojem klijent ponavlja slanje autentikacijskog paketa koji sadrži lozinku i korisničko ime u **plaintextu** dok ne dobije potvrdu od strane servera.
- **MSCHAPv2** - protokol "unutarnje" autentikacije, glavna autentikacijska opcija kod PEAP-a. Problem ovog protokola je korištenje **DES** enkripcije što ga čini jako podložnim na ***brute force*** napad (zbog malog ključa od 56 bita).
- **EAP-MD-5 Challenge** - ne preporuča se za korištenje na WLAN mrežama, zbog nedovoljne zaštite lozinke. Naime, u ovom protokolu server šalje klijentu random string koji ser koristi kao sol pri MD5 hashiranju, te se takva lozinka zajedno s plaintext korisničkim imenom šalje serveru na autentikaciju. Ne implementira uzajamnu

autentikaciju servera i klijenta kao ni mogućnost uspostave dinamičkih (za svaku sesiju) ključeva, koji pružaju sigurnost ekvivalentnu žičanoj konekciji (WEP*).

- **EAP-TLS** - pruža uzajamnu autentikaciju servera i klijenta temeljenu na digitalnim certifikatima. Također omogućava dinamičko generiranje WEP ključeva za sigurnu uzastopnu komunikaciju klijenta i pristupne točke. Negativna strana ove metode jest potreba za ispravnim upravljanjem certifikatima na strani servera kao i strani klijenta, što zna biti izazovno.

- **EAP-FAST** - metoda razvijena od strane CISCO-a, uz tuneliranje koristi tajni ključ PAC (*eng.* Protecteed Access Credential). Ovaj ključ se klijentu dostavlja ručno (npr. na disku) ili automatski (mrežnom konekcijom). Implementirana je i autentikacija servera od strane klijenta koristeći digitalni certifikat.

- **LEAP** - metoda korištena u CISCO Aironet WLAN mrežama. Koristi dinamički generirane WEP ključeve za enkripciju prometa i podržava uzajamnu autentikaciju servera ii klijenta.

- **PEAP** - metoda razvijena od strane Microsofta, Cisco-a i RSA Security. Koristi se za siguran transport autentikacijskih podataka čak i zastarjelih protokola temeljenih na lozinkama preko 802.11 mreže. Kao i TTLS PEAP sigurnost postiže tuneliranjem prometa između klijenta i servera uz to koristeći samo serverove certifikate.

EAP metoda	**MD5**	**TLS**	**TTLS**	**PEAP**	**FAST**	**LEAP**
Zahtjeva certifikat sa klijentske strane	ne	da	ne	ne	ne	ne
Zahtjeva certifikat sa serverske strane	ne	da	da	da	ne	ne
Generiranje i upravljanje WEP ključevima	ne	da	da	da	da	da
Otpornost na Evil Twin AP napad	ne	ne	ne	ne	da	da
Smjer autentikacije	jednostrano	obostrano	obostrano	obostrano	obostrano	obostrano
Zahtjevnost postavljanja mreže	lagano	teško [1]	umjereno	umjereno	umjereno	umjereno
Sigurnost	loša	vrlo visoka	visoka	visoka	visok	visoka [2]

Tablica 2: Pregled EAP metoda. [8]

6 Verifikacija identiteta RADIUS servera

Sami pristupni podaci korisnika RADIUS serveru se dostavljaju kroz već spomenuti siguran tunel. Postojanjem protokola poput PAP-a koji te podatke šalje u čisto, lako je zaključiti da cijela autentikacijska shema 802.1X mreža počiva na sigurnosti enkriptiranog tunela i verifikaciji certifikata servera koja je potrebna da se sam kanal uspostavi.[3]

U slučaju TLS tunela koriste se X.509 certifikati koji uz javni ključ certificiranog subjekta sadrži dodatne informacije o istom. Ovakva situacija na prvu može se činiti slična sigurnom tuneliranju u web preglednicima. U tom slučaju, preglednik koristi IP adresu odnosno ime hosta stranice kojoj pristupamo za verificiranje certifikata. Problem kod bežičnih mreža je što se komunikacija s RADIUS serverom odvija na aplikacijskoj razini, na kojoj nema IP adresa. Jedini identifikator same mreže odnosno servera je SSID (*eng.* Service Set Identifier). SSID se može mijenjati i ne postoji centralizirano tijelo koje jamči jedinstvenost imena mreže, stoga je pristup ekvivalentan onome kod web stranica za ovu primjenu beskoristan. [3]

7 Evil twin napad

Sam napad na WPA 2 Enterprise mrežu može se sažeti u par koraka.Prvi korak bi bio postavljanje pristupne točke istog SSID-a ciljanoj mreži, koja žrtvama nudi jači signal. Naime, klijent će se umjesto na originalnu (sigurnu) pristupnu točku, automatski spojiti na onu s istim SSID-om, ali jačim signalom. U drugom koraku potrebno je osigurati da napadački RADIUS server podržava EAP metode koje koristi klijent. Treći korak je pokretanje programa odnosno skripte koja će vršiti autentikaciju žrtava na lažnu napadačku mrežu.
Ovakav napad otvara prostor za nekoliko napadačkih aktivnosti [3]:

- Napadač može bilježiti korisničke podatke žrtava te ih iskoristiti za prijavu na ciljanu mrežu ili ostale usluge s istim podacima. Ovo je trivijalno u slučaju kada klijent koristi PAP, koji te podatke šalje neenkriptirane. Dohvaćanje tih podataka moguće je i u slučaju korištenja MSCHAPv2 ili MD5-Challenge metoda, jer su obje podložne dictionary napadima.

- Ponudi li napadač stvarni internet pristup žrtvi moguće je pokretanje raznih Man In The Middle napada i prikupljanje još više podataka iz žrtvinog prometa itd.

Kroz dosad rečeno, da se naslutiti kako sigurna konfiguracija ovakve mreže uvelike ovisi o verifikaciji RADIUS servera. Iako je to ključan detalj, taj korak sam od sebe ne pokriva sve "rupe" pri postavljanju mreže, već je potrebno obratiti pozornost i na korake poput:

- sami korisnički podaci, odnosno zaporke i korisnička imena kojima se prijavljuju na WPA Enterprise mrežu trebali bi biti, što je to više moguće, odvojeni od korisničkih podataka kojima se korisnik prijavljuje na neke **druge usluge**. Ovakvim pristupom napadaču se smanjuje vrijednost kompromitiranih podataka, te je rizik kompromitiranja istih stoga manji.[3]

  npr. korisnički podaci za povezivanje na Eduroam mrežu koriste se za prijavu na sve sustave koji **AAI@EduHr** platformi - e-Građani, fakulteti itd.

- korisniku je potrebno omogućiti što jednostavnije **sigurno** konfiguriranje mrežne konekcije. To postižemo obraćajući pozornost na dizajn klijentske aplikacije koja se koristi za uspostavu veze. Sa što manje koraka koje ostavljamo u ovisnosti o korisniku, smanjujemo vjerojatnost da veza bude nesigurno konfigurirana.[3]

8 Priprema i provedba napada

8.1 Hardver

Za izvesti napad smo koristili Raspberry Pi 3 Model B. To je malo jednoploč no računalo sa 64 bitnim procesorom i 1GB RAM-a. Uz Raspberry Pi smo koristili i TP-LINK TL-WN722N Wireless USB adapter za dijeljenje WiFi-a. Uz to smo koristili prijenosni punjač kapaciteta 20.000mAh. Izgled spojenih uređaja je vidljiv iz slika 8.1 i 8.1

Slika 4: Slika sklopovlja od gore

Slika 5: Slika sklopovlja sa strane

8.2 Operacijski sustav

Za operacijski sustav smo koristili Kali Linux koji ima distribuciju za Raspberry Pi. Distribuciju smo skinuli s linka te pomoću balenaEtcher alata smo flashali sliku operacijskog sustava na SD karticu koju smo stavili u Raspberry Pi. Kali je operacijski sustav temeljen na Debianu koji ima primjene u testiranju sigurnosti i računalnoj forenzici i dolazi s mnogim predinstaliranim alatima.

8.3 Alati korišteni za provedbu napada

Za izvesti napad smo koristili Eaphammer koji koristi hostapd za stvaranje pristupne točke. Pomoću Eaphammera je omogućeno jednostavno, a kada stavimo u kontekst ozbiljnost podataka koje pribavljamo, rudimentarno postavljanje napada i prikupljanje podataka. Instalacija jednog paketa uz nekoliko naredbi omogućava prikupljanje podataka, o čemu više u potpoglavlju 8.4.

Eaphammer je alat za izvođenje ciljanih evil twin napada na WPA2-Enterprise mreže u svrhu procjene sigurnosti bežične mreže. Kao takav, fokus stavlja na kreiranje sučelja jednostavnog za korištenje bez veće ručne konfiguracije. [12]

U svrhu provedbe napada na eduroam, mi smo koristili značajku krađe Radius pristupnih podataka dostupno s Eaphammerom. Eaphammer podržava sljedeće EAP metode:

- EAP-PEAP/MSCHAPv2
- EAP-PEAP/GTC
- EAP-PEAP/MD5
- EAP-TTLS/PAP
- EAP-TTLS/MSCHAP
- EAP-TTLS/MSCHAPv2
- EAP-TTLS/MSCHAPv2 (no EAP)
- EAP-TTLS/CHAP
- EAP-TTLS/MD5
- EAP-TTLS/GTC
- EAP-MD5

Za pokretanje pristupne točke u terminal se unese sljedeća naredba:

```
./eaphammer -i wlan1 --channel 4 --auth wpa-eap --essid eduroam --creds
```

8.4 Provedba napada

Koristeći Eaphammerov wiki na githubu smo kreirali pristupnu točku, iako kreirati i konfigurirati pristupnu točku nije baš kopirati tri naredbe, ali osim nekih problema s certifikatima i postavljanja za korištenje USB adaptera, postavljanje nije pretjerano komplicirano. Pokrenuvši naredbu danu u 8.3 pristupna točka je kreirana te se lozinke počinju prikupljati.

Raspberry Pi zajedno s antenom i prijenosnom baterijom spremamo u malu torbu te s njom hodamo predominantno u krugu kampusa te kafića u koje studenti zalaze. U krugu kampusa smo uspjeli uhvatiti neku količinu lozinki, no kada bi izašli iz dometa pravog eduroama znatno veću količinu podataka bi skupili nego kada bi istu količinu vremena proveli u krugu gdje postoji prava eduroam mreža.

Test smo provodili povremeno kroz nekoliko tjedana te bi nosili Raspberry sa sobom kada bi to imali smisla. Kroz tih par tjedana procijenili bi da smo prikupljali podatke između 15 i 20 sati te skupili 508 parova korisničko ime - lozinka.

Važno je napomenuti da osim ovih prikupljenih lozniki je postojalo četiri korisnika koji su se pokušali spojiti na pristupnu točku međutim su odspojeni zbog neispravnog certifikata. Tako da iako je ovaj seminar napravljen da ukaže kako postoje ozbiljni nedostatci u eduroam sustavu te postavkama korisnika istog, moramo staviti u kontekst kako je ipak većina ispravno konfigurirala svoje uređaje da ne šalju svoje podatke svim pristupnim točkama.

Iako većina ispravno konfigurira pravilno svoj uređaj, zabrinjavajuće je da u našem izračunu 21.64% korisnika eduroama kojih smo susreli neispravno konfigurira svoje uređaje te su ranjivi na ovakve, jednostavne, napade. Smatramo kako bi trebalo više raditi na osvješćivanju prijetnji koje postoje, jer ako uspijemo prikupiti ovoliko velik broj lozinki na našem fakultetu, čiji studenti bi trebali biti osvješteni budući im je to struka, možemo samo pretpostavljati kakvi bi rezultati bili da je istraživanje bilo eksenzivnije.

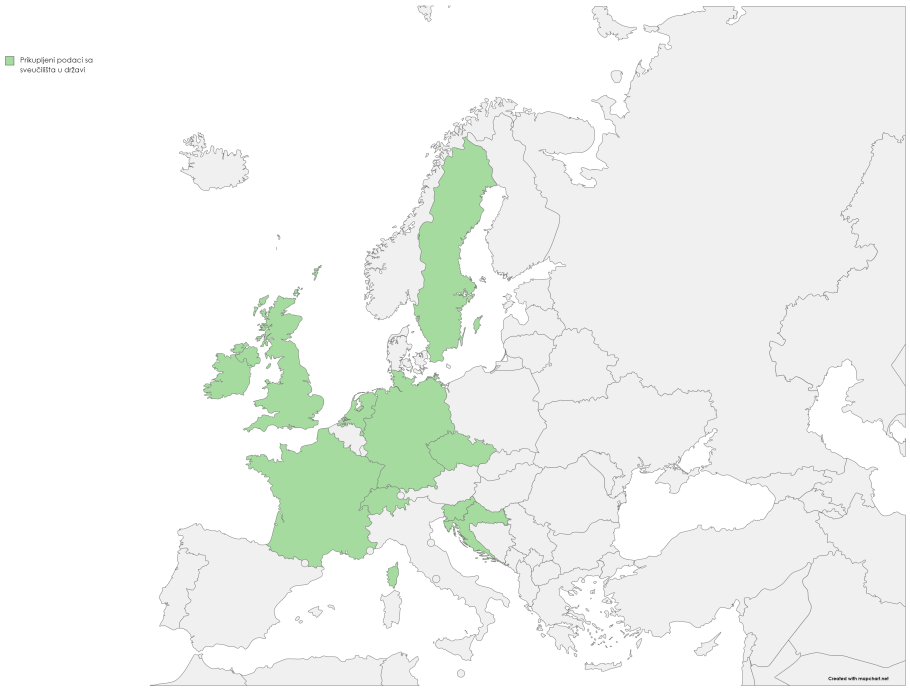
9 Analiza prikupljenih podataka

9.1 Općenite informacije

Prilikom izrade seminara smo skupili 508 korisničkih vjerodajnica dok zbog izostanka certifikata nismo uspjeli skupiti neznatno više od 2300 vjerodajnica. Iako je većina korisnika ispravno konfigurirala povezivanje, od čak **21.64%** korisnika se mogu dobiti vjerodajnice pomoću ovog napada.

Vjerodajnice smo ponajviše dobivali TTLS/PAP metodom pomoću koje smo prikupili 67.26% vjerodajnica, pomoću GTC metode smo prikupili 28.3% vjerodajnica, a pomoću mschapv2 4.44% vjerodajnica. Prve dvije metode prikupljaju vjerodajnice u *plaintextu* dok posljednja metoda šalje enkriptiranu pomoću DES šifre koju je moguće, zbog šifre duge 56 bita, *brute force* napdom dekriptirati.

Vjerodajnice koje smo prikupljali potječu poglavito iz Hrvatske, no 20 vjerodajnica potječe iz inozemstva, na karti na slici 9.3 se vidi iz kojih sve država potječu vjerodajnice. Postoji još jedna vjerodajnica koja nije prikazana na mapi zbog preglednosti, a ona potječe iz Sjedinjenih Američkih Država.



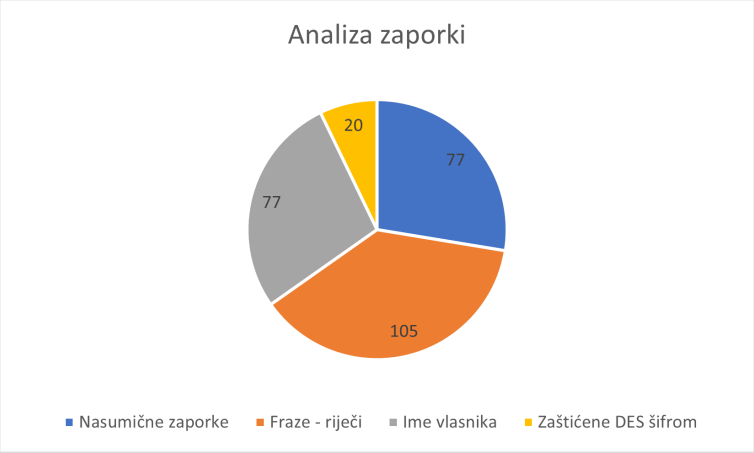
Slika 6: Države iz kojih vjerodajnice potječu

9.2 Analiza prikupljenih zaporki

Prilikom analize zaporki posebno smo izdvojili skole.hr račune jer se isti ne koriste koliko na fakultetima i većinom imaju prvotne nasumične zaporke pa bi promijenila statistiku koju pokušavamo održati što istinitijom.

Slika 7: Analiza skole.hr zaporki

Iz prve slike se vidi kako kod skole.hr računa prevladavaju nasumične zaporke s malom količinom fraza riječi i imena korisnika.



Slika 8: Analiza zaporki

Dok je kod druge slike stvar različita. Najrasprostranjenije zaporke su one s nekom riječi, više ili manje vezano uz interese korisnika. Podjednako rasprostranjena su imena vlasnika,

najčešće u kombinaciji s datumom rođenja, i nasumične zaporke.

Kako je dio prikupljenih zaporki zaštićen DES šifrom, iako moguće dobiti brute force napadom, nismo to činili već ostavili kao zasebnu stavku.

9.3 Sigurnost prikupljenih zaporki

Na sljedećoj slici prikazana je analiza samih lozinki, iz čije se prosječne entropije da zaključiti o prosječnoj sigurnosti lozinke eduroama. Ta prosječna entropija iznosi oko 80 bita, što znači da je napadaču napad na lozinku ekvivalentan napadu na binarnu lozinku od 80 bita.

- !#%()*-.0123456789:<=@ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijkl mnopqrstuvwxyz - 75 simbola, korištena abeceda
- 6518 suma simbola kod prikupljenih zaporki
- 9.20488282145946E+23 - entropija $E = \log_2(R^L)$
- 79.6067455385336 - bitova entropije

Slika 9: Entropija korištenih lozinki.

10 Zaključak

Kroz ovaj seminar smo dali teorijsku pozadinu rada WPA2-Enterprise mreža, kako funkcionira autentikacija, što je to evil twin napad, što je EAP i koji su njegovi modovi. Također smo u sklopu seminara proveli i napad na eduroam koji je također WPA2 Enterprise mreža s mnoštvom korisnika koji nisu nužno educirani kako se ispravno povezati na mrežu te koje su možebitne posljedice tako da je idealan za provođenje napada.

Napad smo proveli kroz 3 tjedna krajem svibnja i početkom lipnja te skupili 508 korisničkih vjerodajnica i nad njima napravili analizu kako bi procijenili sigurnost lozinki te korelaciju interesa korisnika i njihove lozinke pri tome ukazujući na propuste.

Kroz ovaj seminar želimo dvojako ukazati na ranjivosti u digitalnom svjetu, prva je ranjivost na prikupljanje podataka lažnom pristupnom točkom na što su mnoge kolege, kao što vidimo, ranjivi, druga je ranjivost na social engineering napade korelacijom lozinki s interesima korisnika gdje se vidi ranjivost korisnika, doduše u dosta manjem broju nego na prikupljanje podataka. Ovaj seminar je eklatantan primjer zašto treba još mnogo raditi na edukaciji korisnika kako bi spriječili ovakve napade.

Eduroam ima mnoge pogodnosti za učenike i studente, međutim, kao što je pokazano u seminaru, ima velike propuste. Iako su ti propusti posljedica pogrešne konfiguracije od strane korisnika, ne smijemo, kao osobe stručne u tome, ostaviti i pustiti problem da postoji kao korisnička greška, već edukacijom pokušati mitigirati problem, jer iako smo mi podatke prikupljali za ovaj seminar samo u svrhu analize, netko drugi može isto napraviti s malicioznim namjerama.

Literatura

[1] How to Install Kali Linux on Raspberry Pi? (Complete Guide), RaspberryTips, s interneta: https://raspberrytips.com/use-kali-linux-raspberry-pi/, zadnji pristup: 1.6.2022.

[2] Pi-PwnBox-RogueAP, Brun-Nouvion J., Dipsylala, s interneta: https://github.com/koutto/pi-pwnbox-rogueap/wiki/13.-WPA-WPA2-Enterprise-(MGT)-Rogue-AP-Evil-Twin, zadnji pristup: 1.6.2022.

[3] The Evil Twin problem with WPA2-Enterprise, Nussel L., s interneta: https://users.suse.com/~lnussel/The_Evil_Twin_problem_with_WPA2-Enterprise_v1.1.pdf, zadnji pristup: 1.6.2022.

[4] Attacking WPA2 enterprise, Reggiani M., s interneta: https://resources.infosecinstitute.com/topic/attacking-wpa2-enterprise/, zadnji pristup: 1.6.2022.

[5] Attacking WPA-Enterprise Wireless Networks, Neely M., s interneta: https://www.slideshare.net/NEOISF/attacking-and-securing-wpa-enterpris, zadnji pristup: 1.6.2022.

[6] WPA/WPA2-ENTERPRISE Best Practice Guide, Teck_k2, s interneta: https://teckk2.github.io/wifi%20pentesting/2018/08/09/WPA-WPA2-Eneteprice-best-practice.html, zadnji pristup: 1.6.2022.

[7] Attacking and Defending WPA Enterprise Networks, Kumar D., s interneta: https://www.contextis.com/en/blog/attacking-and-defending-wpa-enterprise-networks, zadnji pristup: 1.6.2022.

[8] 802.1X Overview and EAP Types, Intel, s interneta: https://www.intel.com/content/www/us/en/support/articles/000006999/wireless/legacy-intel-wireless-products.html, zadnji pristup: 1.6.2022.

[9] Extensible Authentication Protocol (EAP), Webster E., s interneta: https://www.techtarget.com/searchsecurity/definition/Extensible-Authentication-Protocol-EAP, zadnji pristup: 1.6.2022.

[10] What is 802.1X? How Does it Work?, Secure W2, s interneta: https://www.securew2.com/solutions/802-1x, zadnji pristup: 1.6.2022.

[11] On WPA2-Enterprise Privacy in High Education and Science, Perković, T. and Dagelić, A. Bugarić, M. and Čagalj, M., s interneta: https://doi.org/10.1155/2020/3731529, zadnji pristup: 1.6.2022.

[12] EAPHammer Wiki, s0lst1c3, s interneta: `https://github.com/s0lst1c3/eaphammer/wiki`, zadnji pristup 30.5.2022.