Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Marko Lavrinec

Analiza protokolov za priključevanje v brezžična omrežja

diplomsko delo

univerzitetni študijski program
prve stopnje
računalništvo in informatika

Mentor: prof. dr. Nikolaj Zimic

Ljubljana, 2017

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Brezžična računalniška omrežja so se zelo razmahnila. S tem so postali še bolj pomembni postopki priključevanja v omrežja. Najbolj pogosta so privatna omrežja, kjer upravljavec omrežij strogo določa dostop do omrežja.

Zelo hitro se uveljavljajo tudi omrežja, ki omogočajo uporabo določeni skupini uporabnikov, ki se dinamično spreminja in se poljubno določa. Primera takšnih omrežij sta hotelsko omrežje ter mestno omrežje (npr. WiFreeLjubljana). Standard priključevanja za takšne tipe omrežij ne predvideva.

V diplomski nalogi preglejte možne načine prijave v brezžična omrežja ter posebej opredelite nevarnosti, ki so jim omrežja izpostavljena. Poudarek naj bo na zgoraj omenjenih omrežjih z dinamično skupino uporabnikov.

Zahvaljujem se svojemu mentorju Nikolaju Zimicu in asistentu Mattiji Petroniju za pomoč in svetovanje pri izbiri in izvedbi teme. Prav tako se zahvaljujem Anji Rupar in Romani Debeljak za lektoriranje diplomskega dela.

Kazalo

Seznam uporabljenih kratic

kratica	angleško	slovensko
IEEE	Institute of Electrical and Electronics Engineers	Združenje inženirjev s področja elektrotehnike in elektronike
WEP	Wired Equivalent Privacy	Standard za šifriranje
WPA	Wi-Fi Protected Access	Standard za šifriranje
WPA2	Wi-Fi Protected Access 2	Standard za šifriranje
GHz	Gigahertz	Gigaherc
MB/s	Megabit per Second	Megabitov na sekundo
MAC	Media Access Control	Nadzor dostopa do medija
SSID	Service Set Identifier	Identifikator nabora storitev
IP	Internet Protocol	Internetni protokol
DHCP	Dynamic Host Configuration Protocol	Omrežni protokol za dinamično nastavitev gostitelja
ARP	Address Resolution Protocol	Protokol za prepoznavanje naslovov
HTTP	Hypertext Transfer Protocol	Protokol za prenos hiperteksta
HTTPS	HyperText Transfer Protocol Secure	Protokol za varni prenos hiperteksta
SSL	Secure Sockets Layer	Protokol za šifriranje
RC4	Rivest Cipher 4	Protokol za šifriranje
AES	Advanced Encryption Standard	Protokol za šifriranje
CRC	Cycle Redundancy Code	Ciklična redundančna koda

kratica	angleško	slovensko
IV	Initialization Vector	Začetni vektor
XOR	Exclusive OR	Vsota po modulu 2
LAN	Local Area Network	Lokalno omrežje
ASCII	American Standard Code for Information Interchange	Ameriški standardni nabor za izmenjavo informacij
MIC	Message Integrity Code	Niz, s katerim se potrjuje verodostojnost sporočila
HMAC	Hash Message Authentication Code	Algoritem za potrjevanje identitete
MD5	Message Digest 5	Razpršilni algoritem
SHA1	Secure Hash Algorithm 1	Razpršilni algoritem
RFC	Request for Comments	Definicija standardov in protokolov
TKIP	Temporal Key Integrity Protocol	Protokol za integriteto začasnega ključa
DNS	Domain Name Server	Domenski strežnik
SIP	Session Initiation Protocol	Protokol namenjen spletni telefoniji
JSON	JavaScript Object Notation	Standard za izmenjavo podatkov

Seznam tujih pojmov

pojem	pomen
Avtentikacija	Preverjanje prisotnosti
Linux	Odprtokodni operacijski sistem
Wireshark	Orodje za poslušaje in analizo omrežne komunikacije
Broadcast	Sporočilo, ki je namenjeno vsem v omrežju
Multicast	Sporočilo, ki ima v omrežju več prejemnikov
Monitor mode	Način poslušanja celotnega omrežja

Povzetek

Naslov: Analiza protokolov za priključevanje v brezžična omrežja

Avtor: Marko Lavrinec

V tem diplomskem delu smo podrobno analizirali protokole za priključevanja na brezžična omrežja.

V začetku smo spoznali postopek prijave na odprta omrežja, kasneje pa še na omrežja, zaščitena z različnimi algoritmi. Pri vseh smo se seznanili s sporočili, ki se ob prijavi na omrežje izmenjajo, prav tako pa smo preverili tudi, kakšna so varnostna tveganja pri njihovi uporabi.

Glavni poudarek testiranj je bil na odprtih omrežjih s kasnejšim zahtevanjem prijave. Tu smo najprej spoznali, kakšna so ta omrežja, kaj ponujajo in kje jih najdemo. Sledilo je preverjanje varnosti. Poizkušali smo prestreči geslo in na več načinov zaobiti prijavo. V nekaterih primerih nam je to tudi uspelo. S tem smo dokazali, da taka omrežja ne ponujajo visoke stopnje varnosti in da moramo biti pri njihovi uporabi previdni.

Ključne besede: brezžična omrežja, analiza priključevanja, varnost brezžičnih omrežij, šifrirni algoritmi, prisluškovanje brezžičnemu omrežju.

Abstract

Title: Analysis of Protocols used for Connecting to Wireless Networks

Author: Marko Lavrinec

In this thesis we have conducted a detailed analysis of protocols used for connecting to wireless networks.

First we studies the procedure of registering to open networks and then to networks protected with various algorithms. With all procedures we examined the messages that are exchanged when registering to a certain network and we checked the security risks involved.

The main emphasis was given to open networks with subsequent requests for registering. First we got to know these networks; we examined what they are like, what they have to offer and where we could find them. Next we checked the security. We tried to intercept a password and avoid registering. In some cases we succeeded, which proves that such networks do not provide a high level of security and that one should be careful when using them.

Keywords: wireless networks, analysis of connecting, security of wireless networks, encryption algorithms, spying on wireless networks.

Poglavje 1

Uvod

Živimo v svetu, kjer vedno več komunikacije prehaja na brezžična omrežja. Pri tem je pomembno, da se komunikacija odvija hitro ter da je varna in učinkovita. Da bi nam to uspelo zagotoviti, potrebujemo dobre protokole, ki skrbijo za priključevanje v omrežje.

V tem diplomskem delu si bomo ogledali nekaj takih protokolov. Na prvo mesto bomo postavili varnost, saj je to eden ključnih dejavnikov pri popularnosti in uveljavljenosti le-teh.

V 2. poglavju si bomo najprej ogledali, kaj so brezžična lokalna omrežja, kako delujejo, kako so specificirana ter na kakšen način se jim lahko prisluškuje. V 3. poglavju bomo pod drobnogled vzeli odprta omrežja, kjer bomo preučili, kako poteka priključevanje na omrežja; nato pa bomo preverili še njihovo varnost. V 4. poglavju bomo podobno storili še z zaščitenimi omrežji, kjer si bomo podrobneje ogledali protokole WEP, WPA in WPA2 ter jih medsebojno primerjali. V 5. poglavju bomo pregledali še posebno vrsto odprtih omrežij, ki od nas lahko zahtevajo naknadno prijavo v omrežje. Primerjali bomo, v kolikšni meri so boljša od običajnih odprtih omrežij, ter ugotavljali, zakaj v teh določenih primerih niso raje zaščitena omrežja.

Poglavje 2

Brezžična lokalna omrežja

Brezžična komunikacija je povezava dveh ali več naprav, pri čemer se za komunikacijo ne uporablja kablov, ampak visokofrekvenčna elektromagnetna valovanja. Uporabnik zato med uporabo omrežja ni omejen z dolžino kabla, ampak se lahko prosto premika znotraj območja, ki ga pokriva dostopna točka [22].

Tehnologija postaja vedno bolj popularna, še posebej s hitrim razvojem pametnih telefonov in prenosnih računalnikov. Za uporabnike je zanimiv predvsem zaradi enostavne namestitve in prostega premikanja znotraj dosega vstopne točke. Veliko lokalov in veleblagovnic svojim strankam nudi brezžični dostop do interneta, večina jih to ponuja brezplačno. Prav tako po mestih potekajo projekti večjih brezžičnih mrež, ki želijo uporabnikom omogočiti dostop do spleta po celem mestu [2]. Primer takega omrežja je WiFreeLjubljana, ki dostop do spleta ponuja v središču Ljubljane.

2.1 Standard IEE802.11

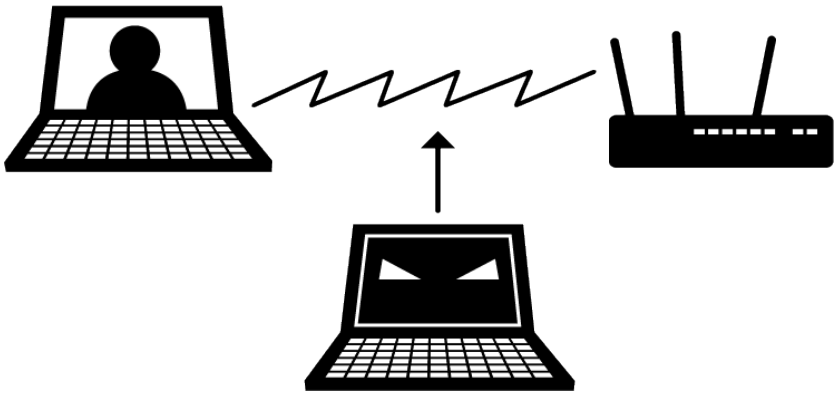
IEEE je leta 1997 postavil prvotni standard 802.11, namenjen brezžičnim lokalnim omrežjem. Najprej je bil definiran na frekvenčnem področju 2,4 GHz in je bil namenjen industriji, znanosti in medicini. Podpiral je hitrosti 1 MB/s in 2 MB/s. [17]

Prvotnemu standardu je sledilo več izboljšav. V večini primerov se je izboljševala hitrost, povečevala varnost in zmanjševala možnost napak. Popravki so bili objavljeni v novejših verzijah in so bili imenovani po zaporednih črkah angleške abecede. Tako je naprej sledil standard 802.11a, nato 802.11b in tako naprej, do standarda 802.11ac, ki se uveljavlja danes, v pripravi pa so tudi že novejši.

Standard 802.11ac, ki se trenutno uvaja, je naredil tudi preskok na 5 GHz frekvenčno področje, kar je ponudilo še dodatno povečanje hitrosti, a je obenem zmanjšalo doseg omrežja.

2.2 Prestrezanje brezžične komunikacije

Ker komunikacija tako rekoč poteka po zraku, jo lahko prestreza vsak, ki je v dosegu in ima za to ustrezna orodja. Tak primer prikazuje slika 2.1. Uporabniku, ki brezžično komunicira z vstopno točko, neopazno z zajemanjem podatkov prisluškuje tudi neznana naprava, ki lahko v primeru slabo zaščitenega omrežja razbere celotno komunikacijo.



Slika 2.1: Skica brezžične komunikacije

V nadaljevanju bomo izvajali poizkuse prestrezanja komunikacije, pri čemer bomo uporabljali Kali Linux [6], ki je odprtokoden projekt, med drugim namenjen tudi testiranju varnosti v brezžični komunikaciji.

V tem operacijskem sistemu lahko našo mrežno kartico nastavimo na način opazovanja (Monitor Mode), s katerim lahko zajemamo vso komunikacijo, ki se odvija na določeni frekvenci. To lahko storimo z naslednjim ukazom:

Ukaz 2.1 *airmon−ng start wlan0*

S tem ukazom smo našo mrežno kartico *wlan0* nastavili v način opazovanja, ob enem pa se je preimenovala v *wlan0mon*.

Sedaj lahko začnemo poslušati promet z naslednjim ukazom:

Ukaz 2.2 *airodump−ng -w izvoz wlan0mon*

S parametrom *-w* smo nastavili, da se bo ves zajet promet shranil v datoteko *izvoz.cap*, ki jo nato lahko odpremo s programom Wireshark [11], s katerim nato vidimo celotni zajeti promet.

V primeru, da bi želeli prestrezati promet na določenem kanalu, bi to lahko storili tako, da bi zgornjemu ukazu dodali parameter *-c*, sledila pa bi mu številka kanala. Podobno bi lahko naredili tudi za prisluškovanje napravi z določenim naslovom MAC. V tem primeru bi dodali parameter *–bssid*, sledil pa bi mu še želeni MAC naslov naprave.

Poglavje 3

Odprta omrežja

Odprta ali nezaščitena omrežja so tista, za katera ne potrebujemo gesla, da se lahko nanje priključimo. Do njih lahko dostopa vsak uporabnik, ki ima ustrezno napravo in je v dosegu točke oddajanja.

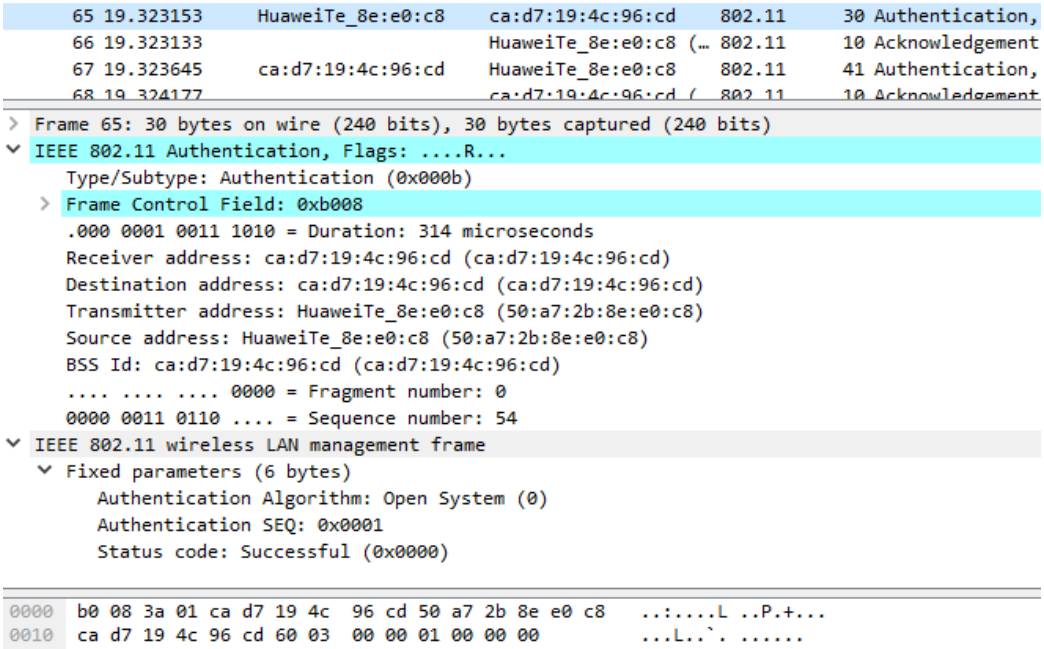
V tem poglavju si bomo ogledali delovanje odprtih omrežij: kako poteka priključevanje nanje in kako varni smo pri njihovi uporabi. Prav tako bomo raziskali, kaj lahko storimo, da se še dodatno zaščitimo pred krajo naših podatkov.

3.1 Analiza priključevanja

Preden se neka naprava, na primer mobilni telefon ali računalnik, poveže na brezžično omrežje, steče med to napravo in vstopno točko vrsta zahtev in ukazov, ki omogočijo da slednja napravo zazna in prepozna.

Za potrebe raziskave smo po postopku, opisanem v poglavju 2.2, prestregli komunikacijo med domačim usmerjevalnikom in pametnim telefonom v času, ko se je ta priključeval v omrežje. Lahko vidimo, da je priključujoča se naprava najprej poslala 30 bajtov velik paket, namenjen preverjanju prisotnosti. To sporočilo prikazuje slika 3.1. V njem sta bila naslova MAC naše naprave in naprave, na katero smo se želeli priključiti. Poleg tega pa sta bila podana še parametra, da gre za prijavo na odprt sistem in da je zaporedna

številka paketa za preverjanje prisotnosti v prvem sporočilu enaka 1.



Slika 3.1: Zahteva za prijavo v odprto omrežje

Na naše sporočilo je vstopna točka odgovorila s sporočilom podobne strukture. S tem je potrdila, da je prejela zahtevo za priključitev. Zaporedna številka v tem sporočilu je 2. Poleg tega pa ima to sporočilo še dodatnih 11 bajtov, ki sporočajo parametre odprte prijave.

Po prejemu potrdila je naša naprava poslala zahtevo za priključitev, ki je velika 106 bajtov. Sporočilo najprej vsebuje glavo s podanima naslovoma MAC, nato pa še jedro zahteve. V jedru imamo na začetku nekaj podatkov o naših nastavitvah, spodaj pa je podan parameter SSID in njegova dolžina. Sledijo podatki, ki oddajni točki sporočajo, s kakšno hitrostjo lahko naša naprava sprejema podatke. Razberemo tudi podatek, katero verzijo protokola naj uporabljata napravi za komunikacijo. V našem primeru je to 802.11n.

Usmerjevalnik je nato napravi odgovoril s sporočilom *association response*, dolžine 174 bajtov. V njem je sporočil, s katerimi hitrostmi lahko oddaja in sprejema, ter potrdil protokol oddajanja.

Sledila je zahteva DHCP. Ta služi za dodelitev lastnega lokalnega naslova

IP, ki ga dobimo v odgovoru na zahtevo. Poleg te pa se nato pošlje še zahteva ARP. Z njo se naprava predstavi ostalim v lokalnemu omrežju in jim pošlje zahtevo za pridobitev njihovih naslovov MAC. S tem se je postopek prijave zaključil in prijavljeni smo bili v brezžično omrežje.

3.2 Varnost

Odprta omrežja nudijo zelo nizko stopnjo varnosti in predstavljajo tveganje za uporabnike in ponudnike. Uporabniku se ob povezavi na odprto omrežje komunikacija ne šifrira. To pomeni, da lahko v primeru, ko nekdo prisluškuje omrežju, skoraj brez težav vidi in razume celotno komunikacijo.

To smo storili tudi mi. Ponovili smo postopek iz poglavja 2.2 in začeli prisluškovati celotni komunikaciji. Brez težav smo pri tem dobili vse pakete in tako videli, kaj vse dela uporabnik ter katere spletne strani obiskuje. Na težave smo naleteli le pri spletnih straneh, ki uporabljajo šifriranje SSL, torej tiste, ki se nahajajo na spletnem naslovu, ki se začne s HTTPS. Omenjene strani namreč vsebino šifrirajo, zato je brez poznavanja ključa komunikacijo skoraj nemogoče dešifrirati.

Odprta omrežja pa predstavljajo tveganja tudi za lastnike vstopnih točk. Do njihovega omrežja lahko namreč dostopajo vsi, ki se nahajajo v bližini. S tem jim upočasnjujejo omrežje, lahko pa pride tudi do hujših težav. Če se v takšno omrežje priklopi neznanec, namreč le-ta dobi tudi IP-naslov tega omrežja. V primeru nezakonitih obiskov spletnih strani ali ob kakšnih drugih sumljivih dejanjih bi se torej zabeležila številka IP lastnika omrežja, kar bi zelo otežilo identifikacijo pravega storilca, obenem pa bi lastniku verjetno prineslo kar nekaj težav.

3.3 Ugotovitve

V tem poglavju smo spoznali odprta omrežja in ugotovili, da se, navkljub enostavni prijavi za uporabnika, v ozadju izmenja kar nekaj pomembnih in-

formacij in podatkov o omrežju.

Ugotovili smo tudi, da nam odprto omrežje ne more ponuditi velike stopnje varnosti, zato smo na vsakem koraku izpostavljeni tveganjem, kar velja tako za uporabnike kot ponudnike.

Domača omrežja je najbolje še dodatno zaščititi. Več o tem pa si lahko preberemo v 4. poglavju.

Poglavje 4

Zaščitena omrežja

Zaradi velikega tveganja uporabe odprtih omrežij in zaradi potrebe po zaščiti omrežja pred priključevanjem tretjih oseb so se razvili algoritmi za šifriranje brezžičnega prometa in za prijavo v omrežje. Začelo se je s protokolom WEP, ki ga definira že sam standard 802.11. Kasneje pa sta mu sledila izpopolnjena in bolj varna WPA in WPA2. Poleg teh treh algoritmov obstajajo še drugi, ki pa niso tako pogosto uporabljeni [23].

V sledečem poglavju si bomo torej pogledali vse tri glavne protokole zaščitenih brezžičnih omrežij, podrobneje pa se bomo posvetili njihovemu delovanju, analizi priključevanja in varnosti.

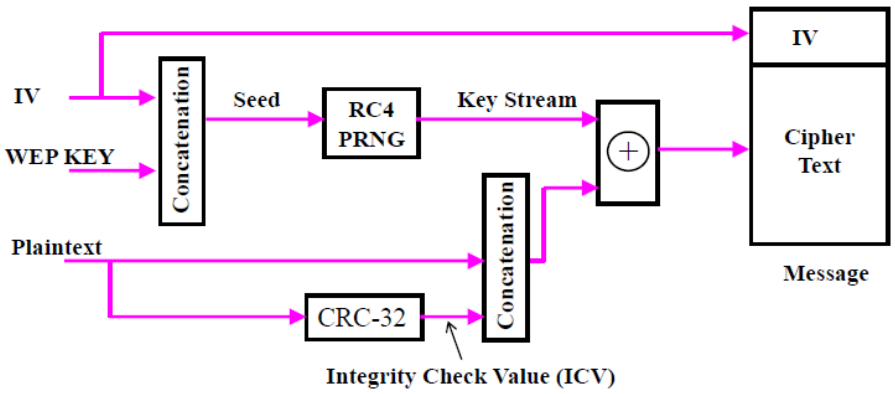
4.1 WEP

Šifrirno shemo za brezžično izmenjavo podatkov med sprejemno in oddajno točko definira standard 802.11. Imenuje se WEP (Wired Equivalent Privacy) in je bil ustvarjen z namenom preprečitve nepooblaščenega dostopa do omrežja. Za šifriranje uporablja šifrirni algoritem RC4, za varnostno potrditev integritete pa se doda še CRC-32 koda [23].

4.1.1 Šifriranje

Kot lahko vidimo na sliki 4.1, je šifriranje sestavljeno iz dveh delov. V zgornjem delu se iz IV in gesla zgenerira seme, katerega dolžina je lahko 64 ali pa 128 bitov. V prvem primeru je geslo dolgo 40 bitov, v drugem pa 104 bite. IV je vedno dolžine 24 bitov, kar pomeni, da ima vrednosti od 0 do 16.777.216 [18]. Seme se nato šifrira z algoritmom RC4. V spodnjem delu se iz našega sporočila, ki ga želimo poslati (Plain text), izračuna varnostna CRC-32 koda, ki se priključi na konec izvirnika.

Nad zgornjim in spodnjim delom se izvede operacija vsote po modulu 2 (XOR), katere izhod predstavlja šifrirano sporočilo. Končno poslano sporočilo, je tako poleg glave, sestavljeno iz javnega, torej nešifriranega IV in šifriranega sporočila.



Slika 4.1: Šifriranje pri protokolu WEP [24]

Ko sprejemnik prejme šifrirano sporočilo, iz njega najprej vzame IV in s svojim geslom zgenerira seme, ki ga pošlje skozi RC4. Nad dobljeno kombinacijo in šifriranim sporočilom nato izvede še operacijo vsote po modulu 2 in kot rezultat dobi želeni izvirnik.

4.1.2 Analiza priključevanja

Priključevanje na omrežje, zaščiteno s kodiranjem WEP, je sestavljeno iz štirih ključnih delov. Najprej naprava, ki se želi priključiti v omrežje, pošlje

zahtevo za avtentikacijo *Authentication Request*, s katero vstopni točki sporoči, da bi se rada priključila na napravo. Ta ji na sporočilo odgovori z izzivom. Priključujoča se naprava po zgoraj predstavljenem postopku šifrira izziv in rešitev vrne vstopni točki. Ta preveri rešitev in napravi sporoči, ali je bila njena avtentikacija uspešna ali ne [23].

Ker želimo preveriti kaj se dejansko dogaja pri priključevanje na omrežje s protokolom WEP in ker nas zanimajo razlike s prijavo na odprt sistem, smo se povezali na nadzorno ploščo našega usmerjevalnika. Za naše omrežje smo nastavili šifriranje WEP – *shared key* in shranili nastavitve.

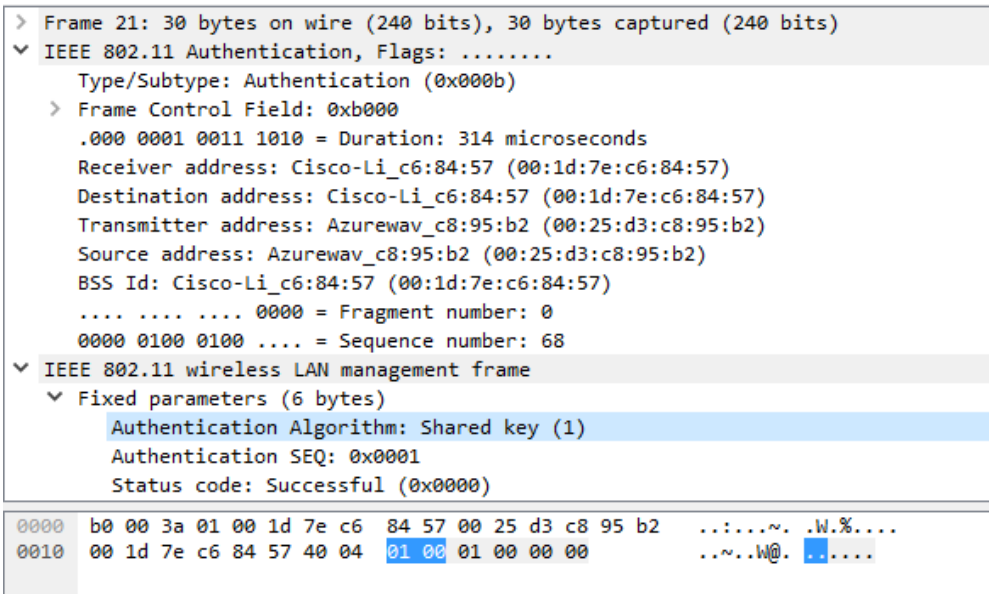
Za šifriranje WEP smo lahko izbirali med *open system* in *shared key* načinom prijave. Glede na vir [15] je razlika med njima v tem, da mora biti pri *shared key* izziv nujno pravilno rešen, sicer prijava ni mogoča. V primeru *open system* pa lahko narobe rešimo izziv, a se še vedno povežemo na vstopno točko, ne moremo pa dostopati do omrežja in ostalih naprav.

Napravo za prisluškovanje smo ponovno postavili med vstopno točko in terminalom, ki se je povezoval na omrežje. Za začetek priključevanja je terminal vstopni točki poslal paket za preverjanje prisotnosti, velik 30 bajtov. Paket je, poleg glave z MAC naslovi naprav, vseboval še nadzorni okvir *IEEE 802.11 wireless LAN*, velik 6 bajtov. V njem sta bila 2 bajta, ki sta sporočala, da gre za prijavo tipa *open system*; poleg tega pa še 2 bajta velika številka avtentikacijske zaporedne številke, ki je v prvem sporočilu enaka 1. Zadnja 2 bajta sta vsebovala statusno kodo, ki je naznanjala, da ni prišlo do napak.

Vstopna točka je odgovorila s sporočilom, ki je imelo zaporedno številko 2 in statusno kodo 0x000d, kar pomeni, da ne podpira našega načina prijave v omrežje.

Ker je torej vstopna točka odgovorila z napako v prijavi, je naša naprava ponovno poslala zahtevo za preverjanje prisotnosti, ki je imela zaporedno številko 1; prva dva bajta okvirja pa sta naznanjala avtentikacijo s *shared key*, kot to prikazuje slika 4.2.

Na ta paket je vstopna točka odgovorila s pritrdilnim odgovorom, torej s statusno kodo uspešno, zraven pa je poslala še 141 bajtov, med katerimi



Slika 4.2: Zajet paket pri avtentikaciji s protokolom WEP

je 128 bajtov velik izziv, kot to prikazuje slika 4.3. Izziv je predstavljen kot naključno generirana kombinacija znakov, ki jih mora naprava pravilno šifrirati, s čimer dokaže, da pozna ključ omrežja.

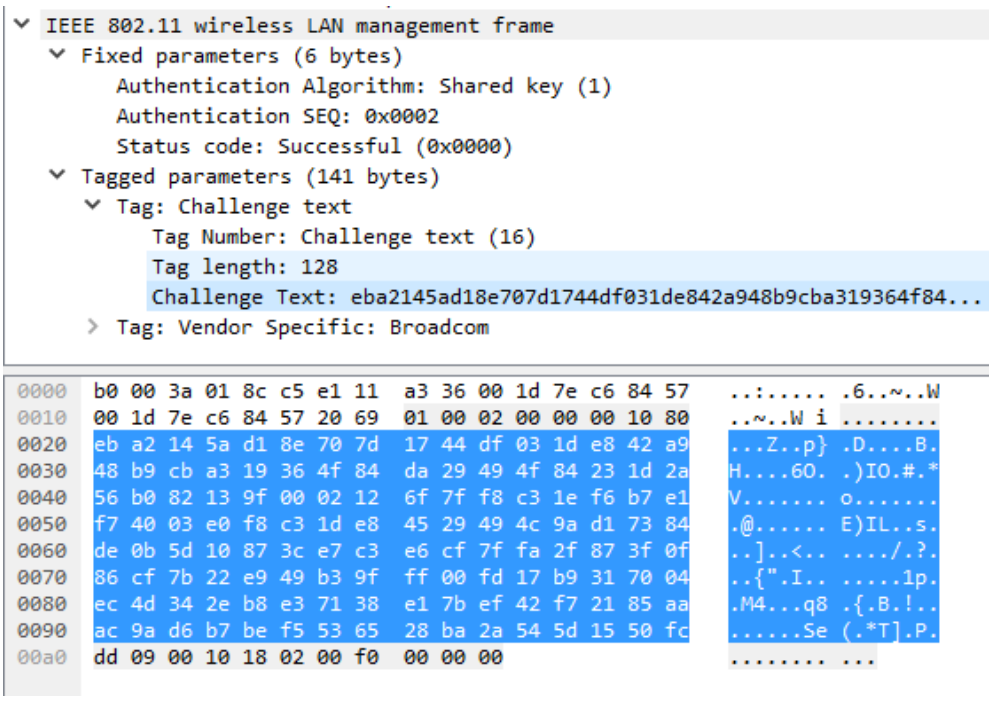
Na prejeti paket je naša naprava odgovorila s 168 bajtov velikim paketom, ki vsebuje glavo, IV, dolžine 3 bajte, in 136 bajtov ostalih podatkov. V teh podatkih se skriva tudi odgovor na izziv.

Ker je bilo zaradi raziskave v prvem primeru vpisano napačno geslo, je prejšnji paket napačno rešil izziv, zato je posledično vstopna točka odgovorila s statusno kodo 0x00f, kar pomeni, da je zavrnila avtentikacijo zaradi napake v rešitvi izziva.

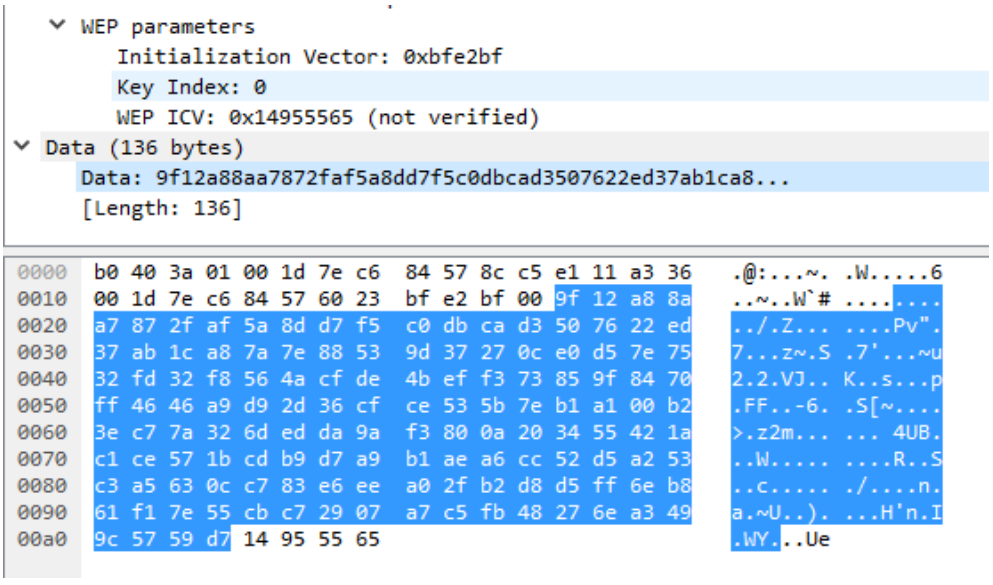
V poizkusu, pri katerem smo vnesli pravilno geslo, pa je bil odgovor na izziv prav tako velik 168 bajtov. Ta odgovor prikazuje slika 4.4.

Odgovor na ta paket je bil zadnji paket s statusno kodo 0x0000, ki je pomenila, da smo vnesli pravilno geslo in da se lahko prijava nadaljuje.

Prijava je nato potekala tako kot pri odprtem omrežju. Najprej je naša naprava poslala paket *Association Request*, v katerem je navedla svoje podatke, torej katere hitrosti in standarde podpira. Vstopna točka pa ji je



Slika 4.3: Poslan izziv



Slika 4.4: Poslan odgovor na izziv

odgovorila z *Association Response*, ki je vsebovala svoje podatke o hitrosti in protokolih.

Vsi nadaljnji paketi so bili šifrirani, iz njih lahko brez dekodiranja razberemo samo osnovne zastavice, pošiljatelja in prejemnika ter IV.

4.1.3 Prisluškovanje omrežju

Eden večjih problemov tega protokola je, da za šifriranje vseh sporočil uporablja glavni ključ (geslo). To pomeni, da lahko vsak, ki prestreza naša sporočila in pozna ključ omrežja, dešifrira našo komunikacijo. Za dešifriranje sporočil je namreč potrebno poznati le IV, ki je javni, in ključ. Torej lahko vsak, ki pozna geslo, brez težav prisluškuje in razume našo komunikacijo, podobno kot je bilo to mogoče pri odprtih omrežjih.

4.1.4 Varnost

Protokol WEP že od leta 2003 ne velja več za varnega [10]. Prisluškovanje namreč ni edina težava. Obstaja kar nekaj napadov, ki lahko s pomočjo statistike izpeljejo gesla ali pa na podlagi neavtorizirane naprave ustvarjajo promet, prav tako pa je možen napad s pomočjo slovarja. Če namreč iz naše analize slik 4.3 in 4.4 razberemo izziv in njegovo rešitev, nam lahko uspe s pomočjo slovarja izpeljati geslo, s katerim je bil izziv rešen.

Ena izmed glavnih ranljivosti protokola WEP je IV. Njegove težave so:

- IV je dolg samo 24 bitov, kar pomeni, da se bo hitro ponovil (v približno 7 urah v zasedenem omrežju);
- IV je javen, torej nam do razbitja manjka samo še geslo;
- standard 802.11 ne definira obveznega spreminjanja IV-ja, ampak je to poljubno, kar pomeni, da je lahko pri usmerjevalnikih inicializacijski vektor konstanten [21];
- IV je del RC4 šifriranja, kar pomeni, da se bo celoten *Key stream* ponovil, kar lahko zaradi javnosti IV-ja takoj zaznamo.

Napadalci na omrežja WEP pogosto uporabijo šibkost zadnje točke zgornjega seznama. V zahtevah algoritma RC4 namreč piše, da se skrivni ključ ne sme nikoli ponoviti, pri omrežjih WEP pa se ponovi. Če tako zajamemo dve različni sporočili z isto vrednostjo IV in nad njima opravimo operacijo vsote po modulu 2, pa bomo dobili rezultat algoritma RC4, iz katerega lahko izpeljemo naše geslo [8].

Napad smo tudi sami testirali. Prisluškovali smo omrežju, obenem pa smo z drugo napravo, ki sicer ni bila prijavljena v omrežje, generirali zahteve ARP, s katerimi smo spodbujali hitro spreminjanje števca IV. Ko se nam je nabralo dovolj podatkov, smo z ukazom *aircrack-ng capWEP.cap* pognali preverjanje ujemanja. Kot rezultat smo dobili niz 6765736C6F, ki predstavlja kodo ASCII našega gesla. Če niz pretvorimo v znake angleške abecede, pa dobimo za rezultat *geslo*.

4.2 WPA

Zaradi hudih varnostnih pomanjkljivosti pri protokolu WEP se je pojavila zahteva po novem, varnejšem protokolu, ki bi bil zmožen delovati na stari strojni opremi starejših usmerjevalnikov.

Nov protokol se je imenoval WPA (Wi-Fi Protected Access). Protokol deluje na isti strojni opremi kot WEP, torej prav tako uporablja šifriranje RC4. Narejenih pa je bilo kar nekaj drugih sprememb: številka IV je postala tajna, začne se uporabljati začasne ključe, glavni ključ pa se ne uporablja več za šifriranje sporočil, ampak samo še za generiranje ključev. Protokol je uvedel še MIC, ki je še dodatno zavaroval sporočila [24].

Za izmenjavo začasnih ključev je protokol uvedel 4-kratno rokovanje. Namen le-tega je, da napravi iz poznanega glavnega ključa (gesla omrežja) izračunata začasne ključe, ki jih po končanem 4-kratnem rokovanju začneta uporabljati za šifriranje povezave. Glavni ključ se nikoli ne prenaša po omrežju, služi pa temu, da se iz njega lahko izpelje začasne ključe, ki služijo potrjevanju identitete in nadaljnjemu šifriranju sporočil. Napravi si v pri-

meru, da ne pride do napake, pri rokovanju izmenjata štiri sporočila.

4.2.1 Štirikratno rokovanje

Štirikratno rokovanje je sestavljeno iz štirih sporočil. Vsa imajo enako zgradbo, ki je prikazana na sliki 4.5. Taka zgradba sporočila je uporabljena tudi pri paketu za izmenjavo ključev za skupinsko komunikacijo, ki pa ni več del tega rokovanja. To sporočilo se razlikuje od definicije sporočila v standardu 802.1X, saj ima nekaj dodatnih polj.

Key Information je velik 2 bajta in nosi nekaj osnovnih podatkov in zastavic. Tako je v njem označeno: kateri šifrirni algoritem se bo uporabljal; index ključ in zastavice za potrjevanje paketov; zastavica MIC, ki pove, če je nastavljen podatek MIC; zastavice za šifriranje, napako, zahtevo in tip ključev. Zastavica za šifriranje pove, če so podatki v sporočilu šifrirani, zastavica za napako pa, če je prišlo v prejšnjem sporočilu do napake [4].

Descriptor Type 1 byte	
Key Information 2 bytes	Key Length 2 bytes
Replay Counter 8 bytes	
Key Nonce 32 bytes	
EAPOL-Key IV 16 bytes	
Key Receive Sequence Counter (RSC) 8 bytes	
Key Identifier 8 bytes	
Key MIC 16 bytes	
Key Data Legth 2 bytes	Key Data 0 ... n bytes

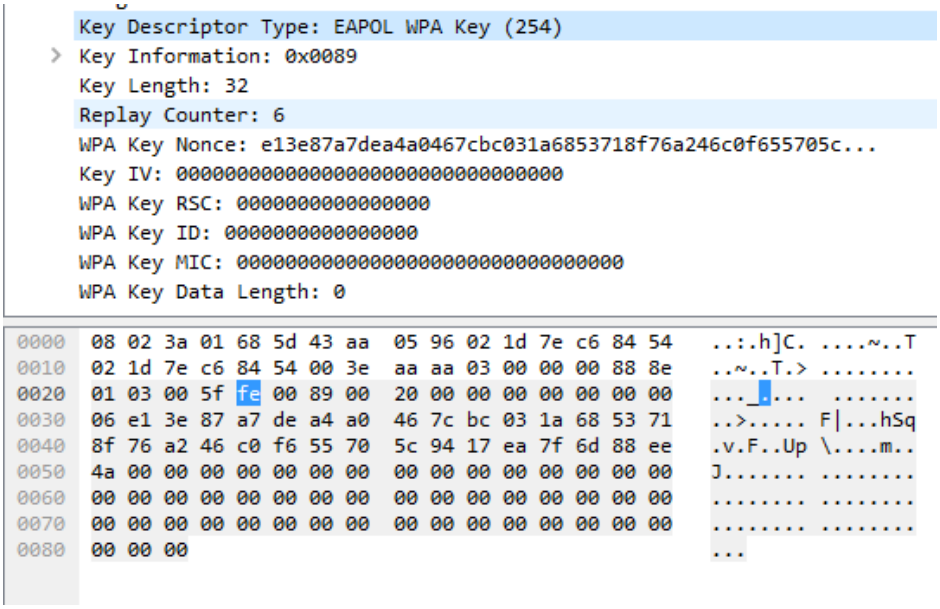
Slika 4.5: Izgled paketa pri 4-kratnem rokovanju [4]

Prvo sporočilo

Zajem prvega sporočila 4-kratnega rokovanja s programom Wireshark prikazuje slika 4.6. Njegove informacije ključa (0x0089) pomenijo, da gre za šifriranje RC4 in metodo HMAC-MD5. Zabeleženo je še, da gre za parne ključe in da zahteva potrditev prejema.

Sporočilo je poslano brez šifriranja in ne vsebuje številke MIC. To je edino sporočilo, ki ima MIC nastavljen na vrednost 0 [4].

Število *WPA Key Nonce* predstavlja naključno število, imenovano *ANonce*, ki bo v prihodnjih korakih služilo za izračun začasnih ključev.



Slika 4.6: Prvo sporočilo pri 4-kratnem rokovanju

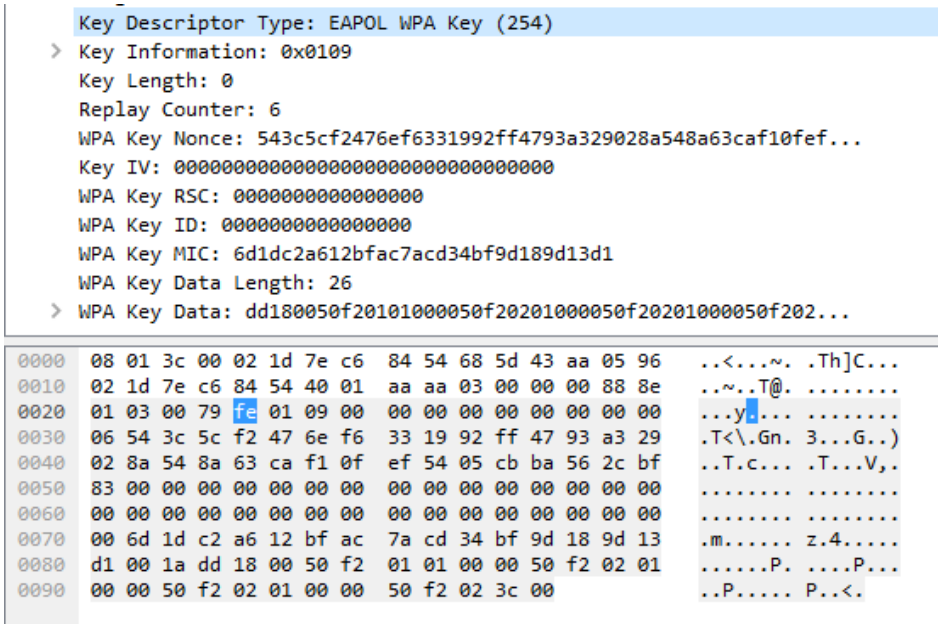
Drugo sporočilo

Glavni podatek v drugem sporočilu, vidnem na sliki 4.7, je *WPA Key Nonce*, ki predstavlja naključno število, imenovano *SNonce*. To število je manjkajoči del za izpeljavo začasnih ključev.

Po prejemu tega podatka lahko na podlagi *ANonce* in *SNonce* obe napravi izračunata začasne ključe.

Okvir vsebuje tudi nešifrirane podatke, ki so namenjeni večji varnosti, saj preprečujejo menjavo šifriranja. Kljub temu da niso šifrirani, jih je izredno težko ponarediti, saj jih ščitijo podatki MIC.

V številki 0x0109 pri *Key Information* je zastavica MIC nastavljena na 1, kar pomeni, da je *WPA Key MIC* mogoče izračunati z algoritmom HMAC-MD5, ki kot rezultat vrne 16 bajtov in je podrobneje opisan v naslednjem podpoglavju.



Slika 4.7: Drugo sporočilo pri 4-kratnem rokovanju

HMAC-MD5

Algoritem MD5 je specificiran v RFC1321. Kot vhod vzame poljubno dolg niz in iz njega generira 128 bitov dolg izhod. Za različne vhode je možen isti izhod, pri istih vhodih pa vedno dobimo isti izhod [12]. Namen algoritma je, da deluje na način, po katerem iz izhoda ni mogoče v obratni smeri algoritma dobiti originalnega vhoda. Zaradi določenih napak v zasnovi algoritma se ta sedaj odsvetuje, saj naj bi veljal za zlomljivega in neprimernega za nadaljnjo uporabo [1].

Algoritem HMAC je specificiran v RFC2104. Uporablja se med dvema napravama, ki hranita skupni skriti ključ z namenom preverjanja informacij, poslanih med njima [13].

Algoritem HMAC-MD5 se v drugem sporočilu 4-kratnega rokovanja uporabi tako, da iz poslanih podatkov izračuna MD5, nato pa ta služi kot vhod v HMAC. Kot ključ se uporabi iz prvega in drugega sporočila izračunan začasni ključ. Tu gre tudi za prvo uporabo ključev v komunikaciji. Izhod tega sporočila predstavlja MIC. V primeru, da ne poznamo glavnega ključa, ne moremo generirati pravega MIC-a. MIC torej tu služi dvema namenoma: prepreči spremembe sporočila ter avtentikacijo osebe, ki ne pozna gesla [4].

Tretje sporočilo

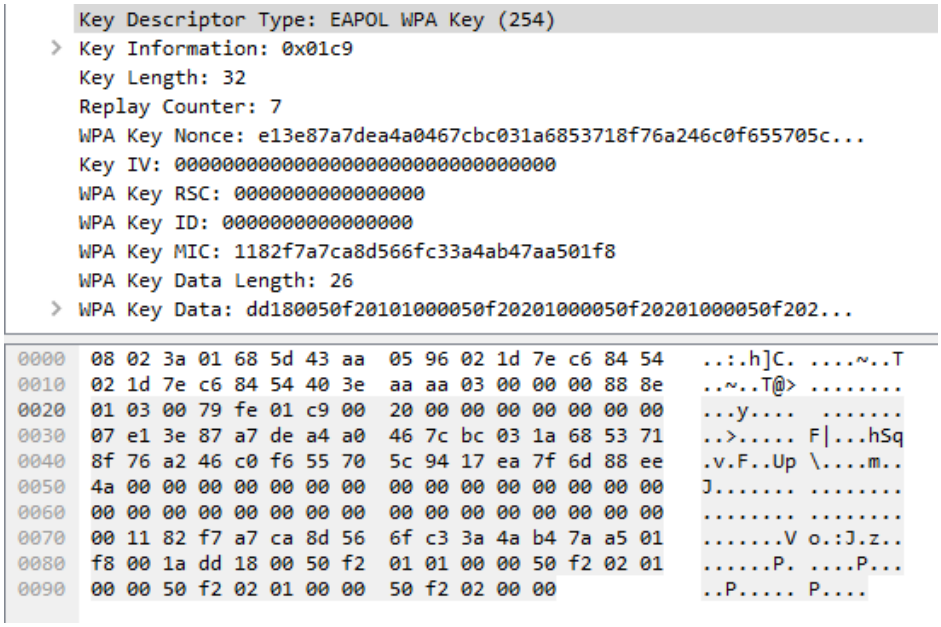
Po prejemu drugega sporočila lahko vstopna točka iz njenega *Key Nonce* izračuna manjkajoči del začasnih ključev. Po tem koraku imata obe točki končano rokovanje s ključi. Tretje in četrto sporočilo pa sta nato namenjena vključitvi ključev v komunikacijo.

Tretje sporočilo služi dvema ciljema. Vstopna točka z njim potrdi, da zaupa priključujoči se napravi in da lahko začneta uporabljati šifrirano komunikacijo. Ključi pa se ne začnejo uporabljati, dokler ni sprejeto četrto sporočilo. Tretje sporočilo je prikazano na sliki 4.8 in je tudi zadnje nešifrirano sporočilo, ki ga vstopna točka pošlje priključujoči se napravi, v primeru, ko je prijava uspešna.

V sporočilu je ponovno *Key Nonce* kot referenca, ki trenutno sicer nima večjega pomena, vendar pa lahko služi potrditvi, da gre za isto rokovanje kot doslej [4].

Četrto sporočilo

Četrto sporočilo, prikazano na sliki 4.9, je namenjeno potrditvi, da bodo od sedaj naprej uporabljeni začasni ključi. V tem sporočilu ne najdemo nobenih posebnosti. Ko je ta korak končan, je med vstopno točko in napravo vzpostavljena šifrirana povezava. V nadaljnjih paketih vstopna točka pošlje še ključe



Slika 4.8: Tretje sporočilo pri 4-kratnem rokovanju

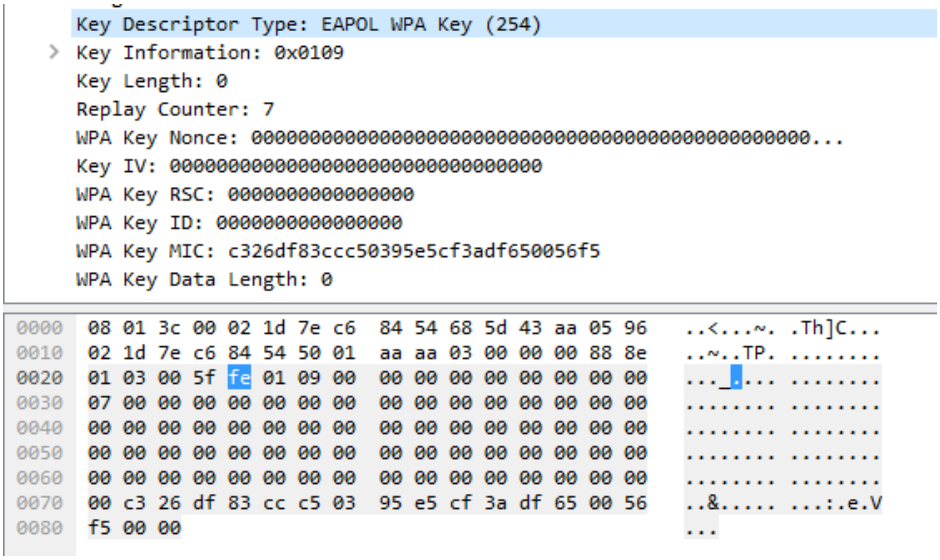
za skupinsko oddajanje (*Broadcast* in *Multicast*), a ti so že v šifriranih paketih. S tem dobita obe napravi vse ključe, zato njuna nadaljnja komunikacija lahko poteka varno.

Vsa nadaljnja komunikacija je šifrirana z začasnimi ključi, ki pa se zaradi varnosti po določenem času spremenijo. Tako napadalci ob dešifriranju začasnih ključev ne morejo dešifrirati celotne komunikacije ampak samo del, v katerem so se ti ključi uporabljali.

4.2.2 Analiza priključevanja

Tako kot v poglavjih 3.1 in 4.1.2 smo se tudi zdaj lotili pregleda komunikacije, ki jo lahko zajamemo pri priključevanju. Tudi tu je naprava, ki se priključuje v omrežje, poslala 30 bajtov veliko zahtevo za priključitev. V njej se nahaja standardna glava, zraven pa še 6 bajtov, ki povedo, da gre za avtentikacijski algoritem odprtega sistema, zaporedno številko 1 in statusno kodo uspešno.

Na ta paket se je vstopna točka odzvala s sporočilom, velikim 41 bajtov, v katerem je posredovala statusno kodo uspešno.



Slika 4.9: Četrto sporočilo pri 4-kratnem rokovanju

Priključujoča naprava ji je odgovorila s prošnjo za priključitev (*Association Request*), veliko 83 bajtov. V njej lahko poleg naslovnih podatkov najdemo tudi možne hitrosti, s katerimi lahko naprava oddaja in sprejema. Zraven je bilo še nekaj zastavic, naveden pa je bil tudi algoritem, s katerim bo naprava šifrirala promet.

Vstopna točka je poslala odgovor na priključitev (*Association Response*), ki je vseboval statusno kodo uspešno, zraven pa je priložila še svoje zastavice in hitrosti, s katerimi lahko sprejema in oddaja.

Tudi naslednje sporočilo je poslal usmerjevalnik. Sporočilo, veliko 131 bajtov, je bilo prvo v nizu 4-kratnega rokovanja. Nanj je prijavljajoča se naprava odgovorila s 157 bajtov dolgim sporočilom *Key (Message 2 of 4)*. Obe sporočili sta podrobneje opisani zgoraj pod točko 4.2.1, skupaj z ostalima dvema sporočiloma štirikratnega rokovanja.

Ker je bilo v prvem primeru vneseno napačno geslo, sta se prejšnji dve sporočili ponavljali, spreminjala pa se je številka *Replay counter*, ki je šla do 4. Priključujoča naprava je nato ugotovila, da nima pravilnega gesla, zato je poslala paket za odjavo iz naprave.

V primeru, ko je bilo geslo vnešeno pravilno, se je prejšnja komunikacija

ponovila (sicer z drugimi vrednostmi naključnih števil), velikosti paketov pa so ostale iste. Ker je bila v tem primeru podana pravilna MIC številka v sporočilu *Key (Message 2 of 4)*, je vstopna točka izvedla avtentikacijo in nanj odgovorila s sporočilom *Key (Message 3 of 4)*, velikim 157 bajtov.

Štirikratno rokovanje se je zaključilo s sporočilom *Key (Message 4 of 4)*, velikim 131 bajtov. Od tu naprej so se pošiljala šifrirana sporočila.

4.2.3 Varnost

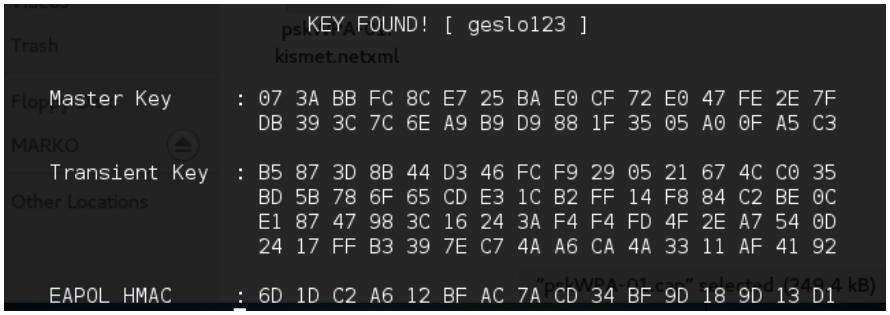
Algoritem WPA je močno dvignil stopnjo varnosti, glede na ostale do sedaj analizirane šifrirne algoritme, in se izognil večini težav, ki smo jih našli pri njih. Tako nam ni pomagalo, če smo si spremenili naslov MAC, saj se na napravo brez gesla vseeno nismo mogli povezati. S prisluškovanjem nam ni uspelo zajeti niti gesla niti začasnih ključev. V primeru, da bi nam pri napadu s silo uspelo dobiti kakšen začasni ključ, bi sicer lahko dešifrirali komunikacijo, vendar pa ne vso, saj se začasni ključi tu po določenem času spremenijo.

Navkljub vsemu pa še vedno lahko prestrežemo 4-kratno rokovanje, ki ni šifrirano. V njem lahko najdemo potrebne podatke, s katerimi nam lahko uspe pridobiti geslo omrežja. Tako je mogoče iz drugega sporočila 4-kratnega rokovanja prebrati vsebino, ki se s pomočjo protokola HMAC-MD5 šifrira z geslom, rezultat pa se zapiše v MIC.

Zdaj lahko s poizkušanjem dobimo geslo. Za pridobivanje gesla obstaja kar nekaj programov, ki nam olajšajo delo; med njimi je tudi *aircrack-ng*. Če za njegov vhod nastavimo zajeto datoteko, ki vsebuje 4-kratno rokovanje, in slovar z gesli, gre program skozi vse vnose v slovarju in išče ujemanje. Če ujemanje najde, bo skoraj zagotovo našel geslo omrežja, s katerim se lahko priključimo nanj.

Tak poizkus smo naredili tudi mi. Našo mrežno kartico smo nastavili na Monitor Mode in nato izvedli ukaz *aireplay−ng −0 5 −a MAC wlan0mon*, s katerim smo poslali 5 zahtev za odjavo vseh naprav iz omrežja na naslovu MAC. Takoj za tem smo klicali ukaz *airodump−ng −c 9 −−bssid MAC −w*

pskWPA wlan0mon, s katerim smo začeli prisluškovati omrežju, izhod pa se je shranil v datoteko *pskWPA.cap*. Program smo po zajetem 4-kratnem rokovanju končali. Za tem smo izvedli ukaz *aircrack-ng -w slovar pskWPA.cap*, ki je skozi slovar, ki smo ga našli na spletu [3], poslal zajeto rokovanje. Kot prikazuje slika 4.10, nam je program našel geslo omrežja, ki je bilo v tem primeru *geslo123*.



Slika 4.10: Najdeno geslo

Ker je bilo geslo minimalne dolžine in ker ni bilo edinstveno, se je našlo v slovarju, zato je bil ta napad mogoč. Če bi si torej želeli izogniti takemu napadu, bi morali nastaviti daljše in unikatnejše geslo, ki ga ni moč najti v slovarju.

Vendar pa je bil marca 2009 objavljen članek *Practical Attacks Against WEP and WPA*, dostopen na viru [20], v katerem je opisan potencialni napad na WPA, ki uporablja protokol TKIP, ki je do tedaj veljal za nezlomljivega [19]. Zanimivo je, da opisani napad ni izveden s slovarjem in grobo silo, tako kot smo to storili mi v prejšnjem poizkusu, saj slednja za napad nista potrebna.

4.2.4 Prisluškovanje

Ker naša komunikacija poteka brezžično, jo je zelo težko omejevati in preprečevati prisluškovanje. Tako pred prisluškovanjem nismo varni, gre pa tu za večjo stopnjo varnosti, kot kjerkoli v do sedaj testiranih omrežjih. Naši ključi namreč tu niso enaki kot za druge naprave, tako kot je bilo to pri

WEP-u, kar pomeni, da oseba, ki samo pozna naš ključ omrežja, še ne more dešifrirati komunikacije.

Poznavanje gesla pa osebi lahko zelo koristi. Tako v primeru zajetja 4-kratnega rokovanja in poznavanja gesla napadalec lahko izračuna začasne ključe, kar mu omogoči dešifriranje komunikacije. Seveda pa tu ponovno velja omejitev, saj napadalec v primeru razbitja začasnega ključa še vedno ne more razumeti šifrirane komunikacije protokola HTTPS.

Če ima naše omrežje geslo, ki ga ni lahko izračunati in se ne pojavlja v slovarjih, lahko torej rečemo, da je naša komunikacija trenutno varna. Potrebno pa je upoštevati, da se bodo lahko čez čas v sistemu našle tudi nove varnostne luknje. Obenem pa narašča procesorska moč računalnikov, zato bo dešifriranje vedno lažje.

4.3 WPA2

WPA2 je nadgradnja protokola WPA. WPA2 nima več iste infrastrukture kot WEP, zato na starejši strojni opremi, ki morda podpira WEP in WPA, ni več mogoč. Novi protokol je predvsem zamenjal šifrirne algoritme, za večjo varnost pa ima tudi preverjanje prisotnosti glave [24].

Glavna razlika med standardoma je v tem, da WPA2 vpeljuje napredne standarde šifriranja in z algoritmom AES nadomesti TKIP. AES vpeljuje standard 802.11i in je, za razliko od RC4, bločni šifrator, torej šifriranja ne izvaja samo nad enim znakom hkrati, ampak nad celotnim blokom [19].

4.3.1 Analiza priključevanja

Priključevanje v brezžično omrežje smo preverili enako kot v preteklih primerih, le da je bilo tokrat zavarovano s protokolom WPA2.

Prvo sporočilo, dolgo 30 bajtov, je bilo poslano iz priključujoče se naprave in je imelo enako zgradbo kot vsa prva sporočila, opisana v zgornjih primerih.

Na to sporočilo je vstopna točka odgovorila podobno kot pri protokolu WPA, s 40 bajtov dolgim sporočilom, ki je nosilo statusno kodo uspešno.

Priključujoča se naprava je nato poslala 82 bajtov velik paket, imenovan *Association Request*, s katerim je predstavila svoje zmožnosti oddajanja in sprejemanja.

Na sporočilo je vstopna točka odgovorila s 57 bajtov velikim sporočilom *Association response*.

Za tem se je začelo 4-kratno rokovanje, ki je opisano v poglavju 4.2.1 pri protokolu WPA, le da je bil tu uporabljen drug protokol za šifriranje. Med zastavicami *Key Information* je namreč deskriptor nastavljen na 2, kar pomeni, da je za šifriranje izbran AES in HMAC-SHA1.

Prvo sporočilo rokovanja je bilo veliko 153 bajtov in ga je poslala vstopna točka.

Drugo sporočilo je poslala priključujoča se naprava in je bilo veliko 155 bajtov.

Ker je bilo tudi tu v prvem primeru vpisano napačno geslo, sta se ti dve sporočili ponovili še štirikrat, vedno z istim izzivom, spreminjal pa se je le *Replay Counter*. Temu je sledil paket za deavtentikacijo, velik 36 bajtov, poslala pa ga je priključujoča se naprava.

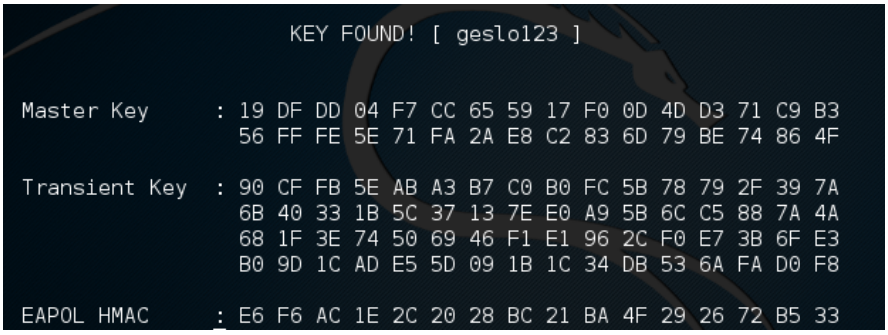
V primeru, ko je bilo vneseno pravilno geslo, pa se je postopek prejšnjih sporočil ponovil z enako velikimi paketi, drugemu sporočilu pa je sledilo tretje, v nizu 4-kratnega rokovanja, ki je bilo veliko 187 bajtov.

Rokovanje se je zaključilo s sporočilom priključujoče naprave, velikim 131 bajtov, za tem pa so se začeli pošiljati šifrirani podatki.

4.3.2 Varnost

WPA2 trenutno še nima znanih uspešnih napadov [5], zato je naše edino upanje poizkušanje. Tako kot pri WPA je tudi tu mogoč napad na 4-kratno rokovanje s pomočjo slovarja, zato smo zajeto komunikacijo iz prejšnje analize poslali skozi program *aircrack-ng*. Tudi v tem primeru smo bili uspešni, tako kot to prikazuje slika 4.11. Geslo je bilo ponovno nastavljeno na *geslo123*, kljub temu pa lahko vidimo iz slike 4.10, protokola WPA, in slike 4.11, protokola WPA2, da se razlikujeta v generiranih ključih, saj so ti ve-

dno generirani na novo. Poleg tega pa je tu med drugim šlo tudi za različne šifrirne algoritme.



Slika 4.11: Najdeno geslo pri protokolu WPA2

Ker nam je uspelo razbiti geslo, imamo tudi tu vidne ključe, s katerimi bi lahko dešifrirali promet. Tako kot pri protokolu WPA bi se takim napadom lahko izognili z daljšimi in unikatnimi gesli. WPA2 potrebuje več procesorske moči kot WPA [5], kljub temu pa nam je *aircrack-ng* skoraj v enakem času našel geslo tako za WPA kot za WPA2 pri uporabi istega slovarja.

4.4 Ugotovitve

V tem poglavju smo spoznali omrežja z različnimi metodami šifriranja. Najprej smo si ogledali protokol WEP, ki se skoraj ne uporablja več in ima marsikatero pomanjkljivost. Prikazali smo, kako poteka šifriranje, nato pa smo naredili še analizo priključevanja.

Za protokolom WEP smo se osredotočili še na WPA. Lotili smo se analize celotnega priključevanja, podrobneje pa smo spoznali 4-kratno rokovanje, ki pri tem igra ključno vlogo. Ogledali smo si tudi varnost protokola WPA in poizkusili dobiti glavno geslo omrežja.

Sledil je pregled protokola WPA2, ki je še dodatno dvignil stopnjo varnosti, strukturno pa je ostal podoben predhodniku. Tudi tu smo poizkusili izmakniti ključ omrežja in mu nato prisluškovati.

Kot lahko vidimo, nam zaščitena omrežja močno dvignejo stopnjo varnosti. Tu pa moramo biti še vedno previdni in skrbeti za to, da uporabljamo novejše in bolj izpopolnjene protokole povsod, kjer je to mogoče. S tem omrežja ne zavarujemo samo pred napadi, ampak tudi pred nepooblaščenim dostopom tretjih oseb, ki ga lahko s svojo prisotnostjo upočasnjujejo.

Poglavje 5

Odprta omrežja s kasnejšim zahtevanjem avtentikacije

Poglavje 5 nadgrajuje in nadaljuje poglavje 3. Predstavili bomo brezžična omrežja, ki so sicer odprta, vendar pa od uporabnika običajno še vedno zahtevajo geslo ali kakšen drug način prijave.

Prav tako si bomo ogledali, kje se ta omrežja najpogosteje pojavljajo, in preučili dejanska tveganja na primeru konkretnega omrežja.

5.1 Značilnosti omrežij s kasnejšim zahtevanjem avtentikacije

Lastniki odprtega omrežja lahko svoje omrežje bolje zaščitijo tako, da od uporabnika zahtevajo dodatno prijavo v sistem, po tem ko se je ta že povezal na vstopno točko in preden mu je omogočen dostop do svetovnega spleta. V ta namen se uporabniku po uspešni prijavi na brezžično točko odpre okno brskalnika, v katerem je prijavna stran, ki običajno zahteva geslo.

Tak način prijave pogosto najdemo na mestnih omrežjih, bencinskih črpalkah, v hotelih, bolnišnicah, restavracijah in ostalih podobnih javnih ustanovah. Uporabnik običajno pridobi geslo z nekim nakupom ali s tem, da strani zaupa del svojih osebnih podatkov.

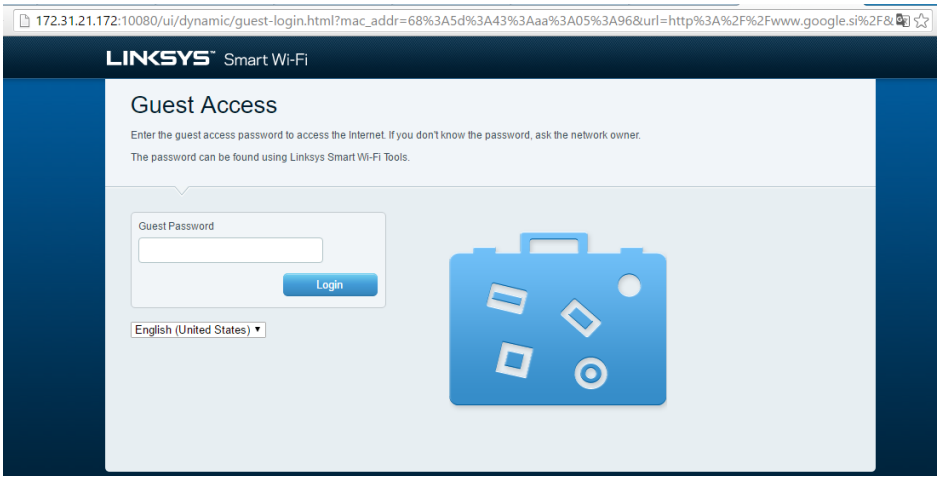
Primer takega odprtega omrežja je WiFreeLjubljana, ki v mestu Ljubljana ponuja brezplačno enourno brskanje po internetu uporabniku, ki posreduje svojo telefonsko številko. Za dodelitev daljšega časovnega intervala lahko uporabnik za določene zneske kupi različne pakete, ki mu omogočajo nadaljnje brskanje po internetu, obenem pa tudi polno hitrost prenosa podatkov [9]. Omrežje naj bi bilo zgrajeno iz 400 oddajnikov od 1360 predvidenih [14], ki naj bi ponujali do 150-metrski doseg v odprtih prostorih pri dobrih pogojih [7].

5.2 Analiza domačega omrežja

Za primer celovitega testiranja odprtega omrežja s kasnejšim zahtevanjem prijave na omrežje smo si zagotovili usmerjevalnik Linksys EA6400, ki omogoča tudi možnost naknadne prijave z njihovim poimenovanjem *način za goste* (guest mode).

Ta način nam ob uspešni povezavi na naše omrežje se nam odpre spletna stran, ki jo prikazuje slika 5.1 in od nas zahteva vnos gesla, ki ga je administrator nastavil ob konfiguraciji usmerjevalnika. Dokler gesla ne vpišemo, povezava do svetovnega spleta ne deluje. Če želimo v brskalniku odpreti kakšno stran preko protokola HTTP, nas vedno preusmeri na prijavno stran; v primeru, da želimo obiskati stran na naslovu s protokolom HTTPS, pa nas brskalnik obvesti, da žal ne moremo dostopati do želene spletne strani. S tem se je vstopna točka izognila težavi s certifikati, saj se preusmeritve ne da narediti, če gostitelj nimamo certifikata strani, do katere želimo dostopamo. Pri spletni strani, ki uporablja protokol HTTP, se namreč podatki ne šifrirajo, prav tako pa se ne preverja pravilnega izvora spletne strani, zato je usmerjevalnik lahko namesto spletne strani poslal preusmeritveno zahtevo. Pri protokolu HTTPS pa to ni bilo mogoče, saj ta uporablja certifikate. Vsaka spletna stran s tem protokolom ima svoj certifikat, ki ga izda pooblaščena agencija. S pomočjo certifikatov se nato šifrirajo prenosi spletne strani, obenem pa se potrdi njihov pravi izvor. Ker usmerjevalnik certifikata

nima, po tem protokolu ni mogel vrniti zahteve za preusmeritev na prijavno spletno stran. V primeru, da bi ta vseeno zahteval preusmeritev, pa bi nam to zahtevo najverjetneje prestregel brskalnik in preprečil izvajanje zaradi neujemanja certifikata.



Slika 5.1: Prijava v način za goste

Ob vnosu gesla se nam odpre povezava do svetovnega spleta; preusmeri nas nazaj, od koder smo prišli. Če nas je torej iz spletne strani google.si preusmerilo na prijavno stran, nas po vnosu pravilnega gesla preusmeri nazaj na spletno mesto google.si.

V konfiguraciji usmerjevalnika lahko nastavimo tudi omejitev na MAC naslov naprave. S tem si zagotovimo, da lahko do našega omrežja dostopajo samo naprave s poznanimi naslovi MAC. V navodilih za uporabnika sicer piše, da filtriranje na naslov MAC ne zagotavlja visoke stopnje varnosti, prav tako pa tudi priporočajo pogosto menjavo gesla za odprto omrežje v načinu za goste [16].

Ker nas zanima, kako varna so ta omrežja, si bomo v nadaljevanju pogledali nekaj primerov testiranja varnosti našega domačega omrežja z vključenim načinom za goste in nato preverili, kako se je omrežje na napad odzvalo. Začeli bomo s preprostimi spremembami, ki jih lahko poznajo tudi laiki in za katere ne potrebujemo posebnih orodij. Takšen primer sta sprememba DNS

strežnika in PING, ki ju brez težav izvaja vsak slehernik in nam lahko hitro pokažeta stopnjo zaščite omrežja. Nadalje bomo prešli na zahtevnejše postopke, kjer bomo najprej preizkusili prisluškovanje, da bi ugotovili, kakšne podatke lahko pridobimo z njim. Med drugim bomo poizkusili prestreči tudi geslo in naslove MAC priključenih naprav, kar bomo v nadaljevanju izrabili tudi za našo prijavo na omrežje. Eksperimentiranje bomo zaključili s spreminjanjem imen vstopnih točk, da bi tako preverili, ali je na tak način mogoče ukrasti uporabnike pravemu omrežju in s tem pridobiti tudi druge uporabniške podatke.

5.2.1 Spreminjanje strežnika DNS

Glede na to, da nam je vstopna točka že dodelila IP-naslov, smo se odločili preveriti, če je blokiran samo strežnik DNS. Ko smo v naših nastavitvah spremenili DNS na javni Googlov DNS, povezava s svetovnim spletom še vedno ni delovala, iz česar lahko sklepamo, da je omrežje odporno na najbolj osnovni način spreminjanja nastavitev na strani odjemalca.

5.2.2 PING

Ker nam ni uspelo zaobiti strežnika DNS, smo preizkusili, kaj bi se zgodilo, če bi poznali IP-naslove spletnih strani. Ko smo jih vnesli v brskalnik, nas je ta še vedno preusmeril na spletno stran za prijavo, PING pa je javljal, da dostopa do določenega IP-naslova ni mogoče izvesti.

Zanimivo pa je, da nam je v primeru, ko smo želeli izvesti PING na katerokoli obstoječo domeno, uspelo dobiti njen IP-naslov. Tako smo z ukazom PING google.si dobili Googlov IP-naslov. Vendar pa PING na ta IP-naslov ni bil mogoč, iz česar lahko sklepamo, da nimamo zaprte povezave na DNS strežnik. Ker se je to zgodilo, smo se odločili PING ponoviti tudi po spremembi DNS strežnika. Naš DNS strežnik smo nastavili na javni Googlov DNS z IP-jem 8.8.8.8. Po tej spremembi nismo prejeli nobenega odgovora, niti IP-naslova spletne strani, ki jo PING-amo.

Ugotovili smo, da je za naš privzeti strežnik DNS nastavljen usmerjevalnik, ki deluje, čeprav še nismo dokončali prijave v omrežje, kar pomeni, da je naš promet znotraj omrežja mogoč in da se ukazi, ki so naslovljeni nanj, tudi uspešno izvedejo. Rezultati odkrivajo potencialno luknjo v varnosti omrežja, ki pa je v času našega diplomskega dela nismo uspeli dokazati.

Test z ukazom PING nam je pokazal tudi, da za nas niso zaprta samo vrata 80 in 443, ki jih uporabljata HTTP in HTTPS. V preteklosti smo namreč že imeli opravka s takimi, ki so blokirali samo ta vrata, promet na ostalih pa je potekal nemoteno tudi brez prijave, kar je bilo moč izrabiti naprimer za klic po protokolu SIP.

5.2.3 Prisluškovanje

Tako kot pri običajnem odprtem omrežju je tudi v načinu za goste enostavno prisluškovanje in razumevanje komunikacije. Ponovno smo med vstopno točko in priključujočo se napravo postavili napravo za prisluškovanje. Zajeli smo ves promet, ki se je pretakal po omrežju. Lahko smo videli naprave, ki so priključene na omrežje, in kaj si pošiljajo. Spet smo lahko spremljali in razumeli celoten promet, ki se je pretakal po protokolu HTTP. Ugotovimo lahko, da tu veljajo enake lastnosti kot pri običajnih odprtih omrežjih, opisanih v poglavju 3.2.

5.2.4 Spreminjanje naslova MAC

Ker smo v prejšnjem poizkusu uspeli videti celotno komunikacijo, smo med drugim videli tudi vse naprave, ki so prijavljene v omrežje. Med njimi smo poiskali napravo, ki je že opravila vnos gesla, in s tem avtentikacijo. Našli smo jo tako, da smo v Wiresharku filtrirali rezultate na protokol HTTP in med rezultati poiskali zahtevo za spletno stran. Ko smo videli, da je vrnjena spletna stran, in ne preusmeritev, smo vedeli, da je naprava, ki jo opazujemo, uspešno prijavljena v omrežje. V prestreženem paketu, ki se je poslal med to napravo in usmerjevalnikom, smo poiskali MAC naslov naprave

in se odločili preveriti, kaj se bo zgodilo, če si ta naslov MAC nastavimo tudi mi. Operacijski sistem Kali Linuxu nam to omogoča. Najprej smo izklopili našo mrežno kartico in ji nato nastavili nov naslov MAC z naslednjim ukazom:

Ukaz 5.1 *ifconfig wlan0 hw ether*

Na koncu ukaza smo zapisali še željeni naslov MAC in nato smo našo mrežno kartico ponovno vklopili. S tem smo si na napravi zagotovili želen naslov MAC. Prijavili smo se na omrežje in preverili, ali moramo vnesti geslo. Odprli smo brskalnik in se napotili na spletni naslov google.si. Spletna stran se je takoj odprla, ne da bi nas preusmerila na prijavno stran in od nas zahtevala geslo. S krajo naslova MAC smo očitno zaobšli varnostni sistem, tako da nam je bilo brskanje omogočeno.

Seveda pa bi morali po določeni časovni omejitvi ta postopek ponavljati, saj se podatek, da smo uspešno prijavljeni na vstopni točki, po določeni časovni omejitvi zbriše. V našem primeru je to 24 ur, zato bi po preteku časa naprava od nas ponovno zahtevala geslo.

Prav tako ta napad ne bi bil mogoč, če v omrežje ne bi bila avtenticirana nobena naprava, saj tako ne bi našli nobenega naslova MAC.

Način prestrezanja naslova MAC bi deloval tudi pri omejitvi usmerjevalnika na določene naslove MAC, saj bi si tudi tu lahko spremenili naš naslov MAC na enega izmed teh, ki so že v omrežju, in si s tem zagotovili dostop do omrežja.

Ob naši spremembi naslova MAC na tuj naslov pa se je zgodilo tudi to, da se naprava, ki smo ji ukradli naslov, ni bila več sposobna povezovati v omrežje in je ob vsakem zahtevku za spletno stran prejela sporočilo, da spletna stran ni dostopna. Ugotovitev nas je spodbudila k dodatnim testiranjem in ugotavljanju, zakaj je do tega prišlo.

Zakaj je na nekaterih napravah onemogočen dostop do spleta po kraji naslova MAC

Ponovno smo napravi, prijavljeni na omrežje, ukradli naslov MAC, vmes pa smo postavili še eno napravo za prestrezanje in analizo brezžične komunikacije.

Tako kot v prejšnjem primeru nam je na napravi s spremenjenim naslovom MAC po spremembi uspelo vzpostaviti povezavo in brskati po spletu. Ko pa smo želeli brskati po spletu na napravi, ki smo ji prevzeli naslov, pa spletna povezava ni delovala. Napravi z ukradenim naslovom smo nato izklopili mrežno kartico in na napravi z originalnim naslovom MAC ponovno poslali zahtevo za spletno stran. V tem primeru je povezava spet delovala normalno in spletna stran se je prikazala.

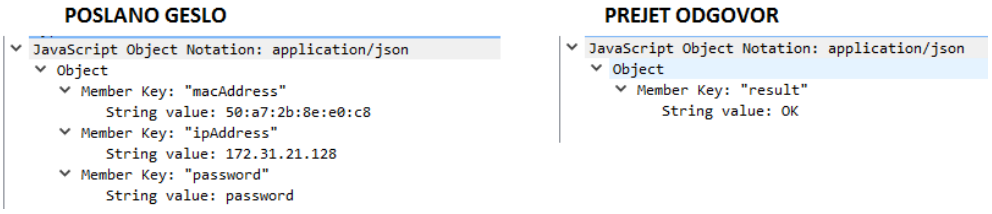
Mrežno kartico smo ponovno vklopili in se povezali na vstopno točko. Sedaj smo na obeh napravah hkrati poslali zahtevo za spletno stran in čakali. Po slabi minuti čakanja sta obe napravi javili, da spletne strani ne moreta prikazati.

Ustavili smo prisluškovanje omrežju in se lotili analize rezultatov. Ugotovili smo, da se je v času, ko se spletne strani niso prikazovale poslalo ogromno paketov *Request to Send* in *Clear to Send*. Paketov, ki bi se morali poslati vmes, pa prisluškujoča naprava ni zaznala.

Iz zgornjih ugotovitev lahko sklepamo, da sta zaradi istega naslova MAC obe napravi ob prejetju paketa *Clear to Send* sklepali, da lahko pošiljata, kar sta tudi storili. Ker sta to počeli obe hkrati, je prišlo do trka, zato ne vstopna točka ne prisluškovalna naprava nista znali razbrati zahteve, ki sta ju pošiljali napravi. V prvem primeru, ko nam je takoj po kraji naslova MAC uspelo vzpostaviti povezavo, pa se je to zgodilo zato, ker je bila v tistem času aktivna samo ena od naprav, druga pa ni ničesar pošiljala, torej ni prihajalo do kolizij. Če bi torej ukradli naslov MAC zelo aktivni napravi v omrežju, bi ji s tem onemogočili uporabo spleta, sami pa prav tako ne bi imeli dostopa do njega.

5.2.5 Prestrezanje gesla

Glede na to, da je viden ves promet pri komunikaciji z vstopno točko, nam lahko uspe prestreči tudi prijavni paket in upamo lahko, da bomo v njem našli geslo. Tako smo pred prvim povezovanjem naprave v omrežje ponovno vključili prisluškovalno napravo. Ko se je naša naprava povezala v omrežje, smo uspešno prestregli tudi spletno stran, ki je od uporabnika zahtevala geslo. Po vnosu gesla se je to zapakiralo v paket JSON in poslalo po omrežju. Geslo ni bilo šifrirano, tako da nam ga je uspelo razbrati. V prvem poizkusu je bilo vnešeno napačno geslo, zato smo od vstopne točke dobili odgovor, v katerem je pisalo »*ErrorInvalidPassword.*« Ko pa je uporabnik vnesel pravilno geslo in se je poslal paket, kot ga prikazuje leva stran slike 5.2, smo dobili pritrdilni odgovor, ki ga prikazuje desna stran slike 5.2. Torej lahko vidimo, da se je pošiljal paket, ki je vseboval MAC naslov naprave, IP-naslov naprave ter geslo. Ko smo prestregli geslo, se na to brezžično točko lahko povezujemo, dokler se geslo ne spremeni.



Slika 5.2: Zajet paket z geslom (levo) in paket z odgovorom (desno)

5.3 Analiza omrežja WiFreeLjubljana

Ker smo v poglavju 5.2 odkrili kar nekaj tveganj pri uporabi odprtih omrežij, smo se odločili preveriti, kako je z varnostjo v poglavju 5.1 omenjenega ljubljanskega omrežja.

Povezali smo se na naključno vstopno točko. Ko smo odprli okno brskalnika, se nam je izpisala stran za prijavo. Za razliko od našega domačega

usmerjevalnika, kjer nas je preusmerilo na spletno stran s protokolom HTTP, nas je tu preusmerilo na šifrirano spletno stran s protokolom HTTPS, kar že takoj dvigne stopnjo varnosti. Spletna stran, ki se je pojavila, je od nas zahtevala telefonsko številko, na katero bi nam poslala geslo za enourno brskanje po spletu.

Tudi tu smo spremenili lastne nastavitve DNS, kar se nam ponovno ni obrestovalo. Naprava se je prav tako kot naše testno okolje povsem enako odzivala tudi na PING.

Za prisluškovanje pa nismo pridobili ustreznih dovoljenj, saj ni skladno z zakonom, zato smo nadaljnje teste opustili. Ker gre za odprto omrežje, pa lahko sklepamo, da naša povezava ni šifrirana, torej je prisluškovanje mogoče. V primeru, da uporabnik obišče določeno spletno stran, lahko prisluškovalec, ki prisluškuje temu oddajniku, prestregel njegovo komunikacijo in jo tudi razbral.

Enako se zgodi tudi s spremembo naslova MAC. Sklepamo lahko, da bi se v primeru, če bi prisluškovali omrežju in pri tem našli MAC naslov naprave, ki je prijavljena v omrežje, ter ji ga nato prevzeli, s tem prijavili v omrežje. Ker ima omrežje več vstopnih točk, bi se tako lahko priklopili na drugo vstopno točko, kot je nanjo povezana naprava, ki smo ji prevzeli naslov MAC. S tem bi se izognili težavi podvojenih naslovov MAC, ki je opisana v poglavju 5.2.4.

Za razliko od prejšnjih dveh dokaj verjetnih napadov pa je tu veliko bolj varno priključevanje in vnos gesla. Spletna stran je namreč zaščitena s šifriranjem, saj uporablja HTTPS, kar nam skoraj onemogoča, da bi lahko dekodirali podatke, ki jih je uporabnik poslal vstopni točki, med drugim tudi geslo in telefonsko številko.

Vendar pa obstaja v zvezi z geslom drugačne vrste pomanjkljivost. V primeru, da uporabnik naroči enourno geslo, mu je to poslano na SMS. Dolgo je štiri znake in vsebuje male črke angleške abecede in števila. To pomeni, da obstaja samo 36^4 možnih kombinacij gesla, kar je enako 1679616 kombinacij. Če bi spisali skripto, ki bi preverjala vse možne kombinacije, obenem pa tudi stalno menjala naš naslov MAC, s čimer bi zakrili svoje sledi, obstaja dokaj

velika verjetnost, da bi nam uspelo. Že samo z dodajanjem enega znaka pa bi število možnih kombinacij naraslo na več kot 60 milijonov, kar bi bilo s poizkušanjem veliko težje razbiti. V primeru, da bi v gesla vpeljali še velike znake angleške abecede, bi pri 5 znakih obstajalo že več kot 916 milijonov kombinacij. Seveda pa bi to pripeljalo tudi do težav pri ločevanju med veliko črko i in malo črko l ter podobnim.

5.3.1 Ponarejanje vstopnih točk

Poleg prisluškovanja obstaja nevarnost, da se povežemo na ponarejeno točko, ki bi bila lahko namenjena kraji naših podatkov.

Na domačem omrežju smo izvedli poizkus. Omrežje smo preimenovali, torej mu spremenili SSID, na ime ljubljanskega omrežja. Tako naš prenosnik, kot mobilna naprava, ki sta že bila povezana na ljubljansko omrežje, sta se tudi na našo ponarejeno točko takoj povezala, kar predstavlja veliko tveganje. Če bi namreč v okolici Ljubljane napadalec vzpostavil lažno brezžično točko, bi se lahko obiskovalcem, ki bi se po naključju povezali nanjo, odprla ponarejena spletna stran ljubljanskega omrežja in od njih zahtevala geslo. To bi bil enostaven način kraje gesla, s katerim bi se napadalec lahko povezal na omrežje. Še huje od tega pa bi bilo, če bi napadalec izkoristil dejstvo, da mestno omrežje ponuja tudi možnost plačila s kreditno kartico. Če bi se žrtev odločila za ta način plačila, bi napadalec z lahkoto prestregel podatke plačilne kartice in žrtvi povzročil kar nekaj škode.

5.4 Ugotovitve

Spoznali smo omrežja s kasnejšim zahtevanjem avtentikacije, pri katerih je prijava na omrežje skoraj identična običajni prijavi na odprto omrežje, le da nas ob zaključku čaka še dodatna stopnja prijave. Tudi tu, tako kot za odprta omrežja, velja, da nas tako omrežje ne zaščiti pred prisluškovanjem in krajo podatkov, med drugim pa tudi gesla, v primeru, da prijavna stran ni zaščitena s protokolom HTTPS.

Prav tako smo ugotovili, da je na takšen način zavarovane vstopne točke možno dokaj enostavno zlorabiti s krajo MAC naslova napravam, ki so že prijavljene v omrežje.

Pri uporabi odprtih javnih omrežij se je torej dobro izogibati spletnih strani, ki nimajo protokola HTTPS, obenem pa tudi strani, preko katerih bi pošiljali občutljive osebne ali druge pomembne podatke, navkljub protokolu HTTPS, saj vedno obstaja tudi tu tveganje, da so nas pretentali.

Poglavje 6

Sklepne ugotovitve

Živimo v svetu, kjer vedno več komunikacije prehaja na brezžična omrežja. Ključno za vso komunikacijo pa je priključevanje na omrežje. Pri priključevanju se namreč napravi druga drugi predstavita in določita osnovne parametre za nadaljevanje komunikacije. Med te parametre sodijo hitrost, verzija standarda, način šifriranja in podobni.

V tem diplomskem delu smo analizirali priključevanje na odprta brezžična omrežja ter na omrežja, zaščitena s protokoli WEP, WPA in WPA2. Ugotovili smo, da smo pri odprtih omrežjih izpostavljeni velikim tveganjem, ki se pri povezovanju na zaščitena omrežja zmanjšajo. Večjo zaščito omogoča tudi izbor pravega šifrirnega algoritma in unikatnost gesla.

Naše omrežje je pametno zaščititi z novejšimi protokoli, ki nimajo znanih ranljivosti. Trenutno se priporoča uporaba protokola WPA2, ki ga podpira velika večina brezžičnih naprav. Prav tako pa je potrebno paziti, komu zaupamo geslo, saj v primeru poznavanja gesla lahko napadalec, ki prisluškuje celotni seji, pridobi glavne in začasne ključe, s katerimi je mogoče nadaljnje razumevanje komunikacije.

Analizirali smo tudi javna omrežja, ki so običajno odprta, zato sodijo med nevarnejša in uporabnike izpostavljajo kraji najrazličnejših podatkov.

Na javnih omrežjih ne moremo nikoli z gotovostjo trditi, da smo se povezali na točko, vredno zaupanja. Obenem pa nam pri takih odprtih omrežjih

lahko tudi prisluškujejo. V teh primerih smo torej vezani na varnost višje nivojskih protokolov, ki jih uporabljamo.

Spoznali smo osnove omrežji WiFi in podrobnosti o varnosti brezžičnega omrežja, za katere bi bilo priporočljivo, da bi jih poznal tudi neuki uporabnik svetovnega spleta. Varnost je torej odvisna od nas samih, naše pozornosti ter izobraženosti na tem področju. Bistvo je, da se zavedamo nevarnosti in da ne nasedamo prevaram, ki se v zadnjem času vse pogosteje dogajajo.

Literatura

[1] Algoritem MD5. Dosegljivo: https://sl.wikipedia.org/wiki/Algoritem_MD5. [Dostopano: 30. 7. 2016].

[2] Brezžično omrežje. Dosegljivo: https://sl.wikipedia.org/wiki/Brez%C5%BEi%C4%8Dno_omre%C5%BEje. [Dostopano 22. 8. 2016].

[3] CrackStation's Password Cracking Dictionary. Dosegljivo: https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm. [Dostopano: 30. 7. 2016].

[4] Details of Key Derivation for WPA. Dosegljivo: http://etutorials.org/Networking/802.11+security.+wi-fi+protected+access+and+802.11i/Part+II+The+Design+of+Wi-Fi+Security/Chapter+10.+WPA+and+RSN+Key+Hierarchy/Details+of+Key+Derivation+for+WPA. [Dostopano: 30. 7. 2016].

[5] Difference Between WPA and WPA2. Dosegljivo: http://www.differencebetween.net/technology/difference-between-wpa-and-wpa2/. [Dostopano: 2. 8. 2016].

[6] Kali Linux. Dosegljivo: https://www.kali.org/. [Dostopano 2. 7. 2016].

[7] Pokritost z omrežjem. Dosegljivo: https://www.wifreeljubljana.si/sl/pokritost-z-omrezjem-wifreeljubljana. [Dostopano 5. 7. 2016].

[8] Understanding WEP Weaknesses. Dosegljivo: http://www.dummies.com/how-to/content/understanding-wep-weaknesses.html. [Dostopano 1. 8. 2016].

[9] WiFreeLjubljana. Dosegljivo: https://www.wifreeljubljana.si/sl/kje-dobim-wifree-kodo. [Dostopano 5. 7. 2016].

[10] Wired Equivalent Privacy. Dosegljivo: https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy. [Dostopano 1. 8. 2016].

[11] Wireshark. Dosegljivo: https://www.wireshark.org/. [Dostopano 2. 7. 2016].

[12] The MD5 Message-Digest Algorithm. Dosegljivo: https://tools.ietf.org/html/rfc1321, 1992. [Dostopano: 30. 7. 2016].

[13] HMAC: Keyed-Hashing for Message Authentication. Dosegljivo: https://tools.ietf.org/html/rfc2104, 1997. [Dostopano: 30. 7. 2016].

[14] Ljubljansko Wi-Fi omrežje WiFreeLjubljana že od lani s pokrivanjem znotraj LJ obroča, a še vedno z nemogočim in neuporabnim vmesnikom. Dosegljivo: http://www.blog.uporabnastran.si/2015/06/16/ljubljansko-wi-fi-omrezje-wifreeljubljana-ze-od-lani-s-pokrivanjem-znotraj-lj-obroca-a-se-vedno-z-nemogocim-in-neuporabnim-vmesnikom/, 2015. [Dostopano 5. 7. 2016].

[15] Igor Bartolic. Wireless Authentication and How to Ensure the Best Wireless Internet Security. Dosegljivo: http://thebestwirelessinternet.com/wireless-authentication.html, 2014. [Dostopano 29. 7. 2016].

[16] Cisco. User Guide - Linksys Router EA6400. Dosegljivo: http://downloads.linksys.com/downloads/userguide/1224698289716/EA6400_combo_PDF_En-FrCA.pdf, 2013. [Dostopano: 8. 7. 2016].

[17] dr. Janez Stergar. STANDARDI BREZŽIČNIH KRAJEVNIH OMREŽIJ - WIFI. Dosegljivo: http://www.s-sers.mb.edus.si/gradiva/rac/moduli/upravljanje_ik/40_brezzicna/03_datoteka.html. [Dostopano 29. 9. 2016].

[18] Arbaug W. A. Edney, J. *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Addison-Wesley Professional, 2003.

[19] Frank H. Katz. WPA vs. WPA2: Is WPA2 Really an Improvement on WPA? Dosegljivo: http://infotech.armstrong.edu/katz/katz/Frank_Katz_CSC2010.pdf. [Dostopano: 30. 7. 2016].

[20] Erik Tews Martin Beck. Practical attacks against WEP and WPA. Dosegljivo: http://dl.aircrack-ng.org/breakingwepandwpa.pdf, 2008. [Dostopano: 30. 7. 2016].

[21] David Wagner Nikita Borisov, Ian Goldberg. Security of the wep algorithm. [Dostopano: 2. 11. 2016].

[22] Inštitut za neionizirna sevanja. BREZŽIČNO LOKALNO OMREŽJE (WLAN). Dosegljivo: http://www.inis.si/index.php?id=103#.V7rfxSiLTIU. [Dostopano 22. 8. 2016].

[23] Zheng J. Ma M. Zhang, Y. *Handbook of Research on Wireless Security*. IGI Global, cop., 2008.

[24] Nikolaj Zimic. Priključevanje v omrežje. Dosegljivo: https://ucilnica.fri.uni-lj.si/pluginfile.php/28661/mod_resource/content/2/5%20-%20PVO%20WS.pdf. [Dostopano: 6. 5. 2016].