CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Pregled sigurnosti bežičnih mreža

NCERT-PUBDOC-2010-12-001

Nacionalni CERT

Nacionalni CERT

Sadržaj

1 Uvod

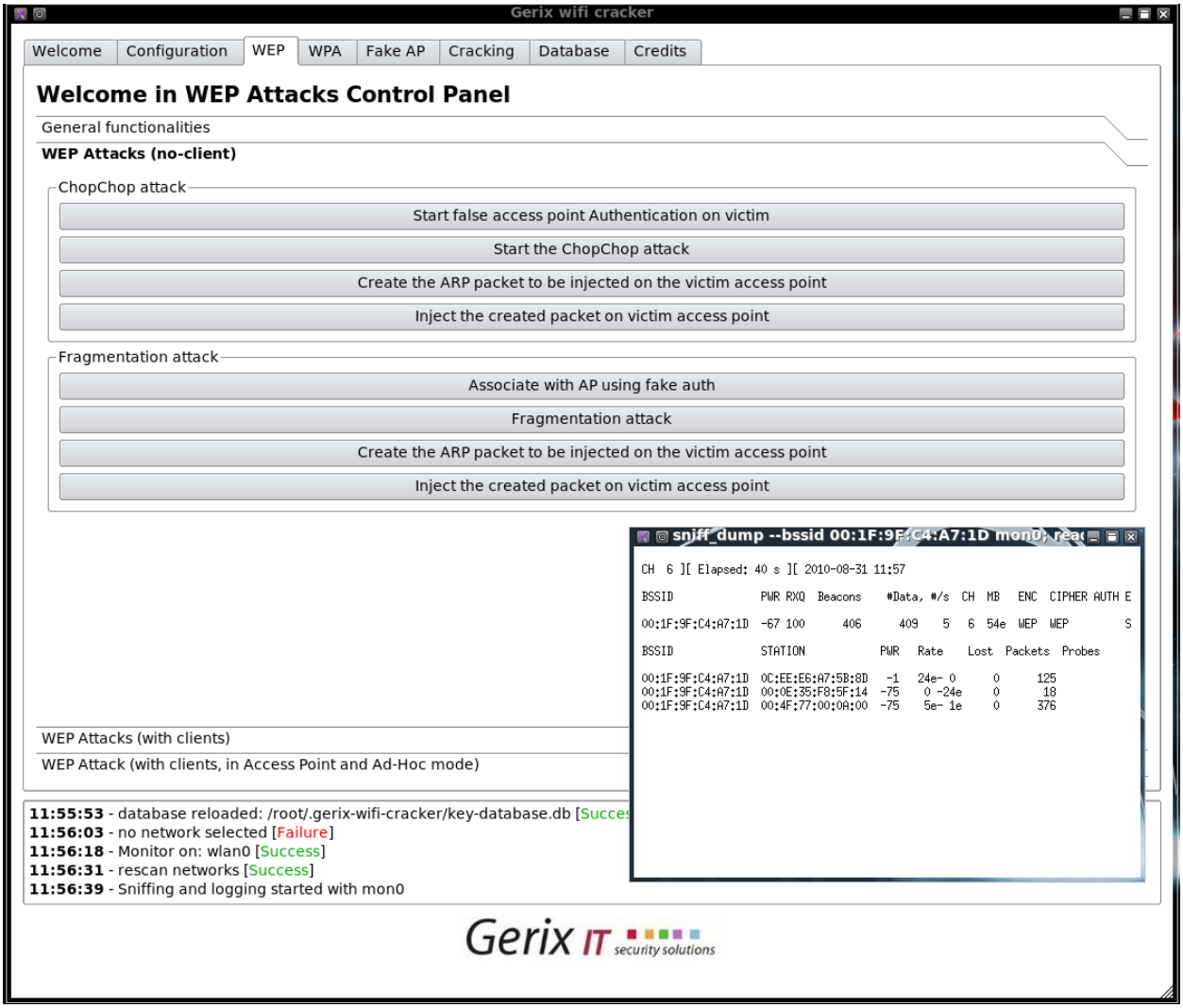
Sigurnost bežičnih računalnih mreža je područje u kojemu se dosta toga brzo mijenja. Početni standard za zaštitu mreže, WEP, se vrlo brzo pokazao potpuno neučinkovitim. Sa današnjim prosječnim prijenosnim računalom i odgovarajućim softverom moguće ju probiti tu zaštitu u par minuta. Kako bi se ispravili nedostatci WEP standarda stvoren je novi standard, WPA, odnosno WPA2 kao konačni oblik specifikacije. Sa naprednijim kriptografskim metodama poput EAP-a i Radius protokola pokušalo se stvoriti protokol koji je u potpunosti otporan na napade koji su se pokazali uspješni nad WEP standardnom.

Povodom objave sigurnosnog propusta u WPA2 standardu zaštite bežičnih mreža, poznatim pod nazivom rupa 196 (*eng. Hole 196*), odlučili smo napraviti pregled sigurnosti bežičnih računalnih mreža sa naglaskom na trenutno aktualne WPA/WPA2 standarde te zatim proučiti stupanj sigurnosti koji pružaju i mogućnosti napada na navedene standarde.

Sigurnost bežičnih mreža unazad zadnjih par godina postala je iznimno važna i za prosječnog korisnika te nije više ograničena samo na tvrtke ili institucije. Telekomunikacijski operateri u svojim ponudama brzog pristupa Internetu gotovo već standardno isporučuju uređaje sa bežičnim pristupom čime je znatno povećana rizična skupina korisnika. Neovlašten pristup korisnikovoj mreži uzrokovati povredu privatnosti i krađu podataka, onemogućiti rad korisničke mreže, izvesti napad na neki treći sustav ili jednostavno može uzrokovati direktnu financijsku štetu korisniku u vidu visokog računa na kraju mjeseca zbog velike količine potrošenog prometa prema Internetu[1].

2 Wired Equivalent Privacy (WEP)

WEP je jedan od prvih raširenih standarda za zaštitu podataka u bežičnoj mreži. Predstavljen je zajedno sa 802.11 protokolom daleke 1997. godine. Danas WEP pruža jako slabi stupanj zaštite, napadač sa nevelikim tehničkim znanjem može probiti zaštitu u nekoliko minuta. Za takav napad su danas dostupni gotovi alati koji omogućavaju izvršavanje napada uz nekoliko pritisaka na tipku miša. Primjer takvog alata je Gerix Wifi Cracker. Njegovo grafičko sučelje je prikazano na slici 1.



Slika 1. Gerix Wifi Cracker

3 Wi-Fi Protected Access (WPA/WPA2)

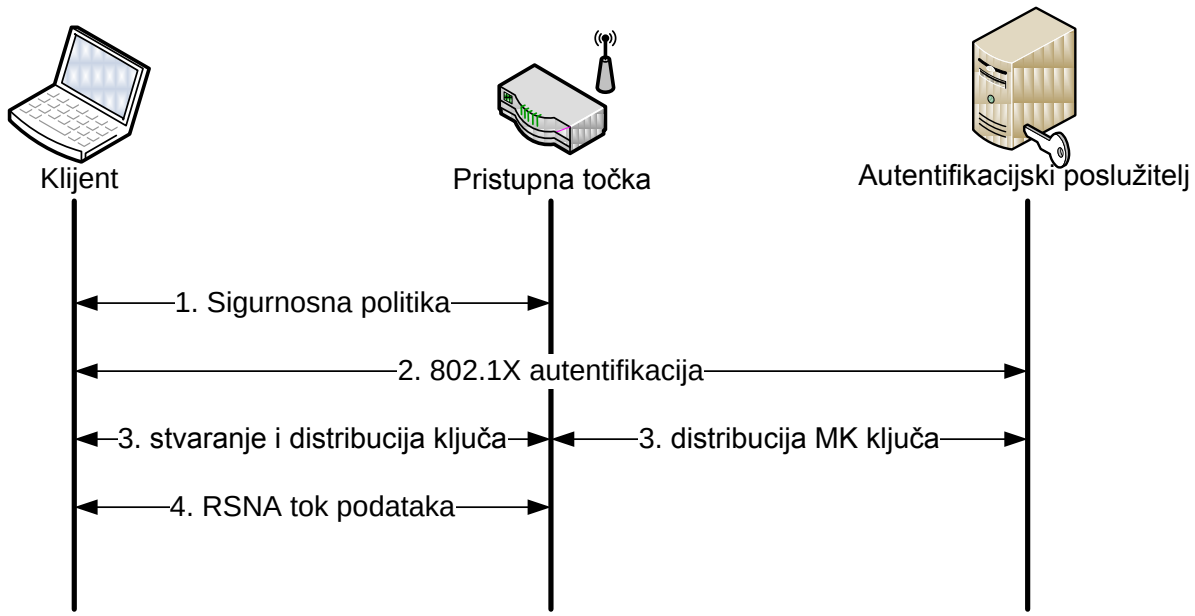
Kao zamjena za slabu zaštitu koju pruža WEP stvoren je WPA protokol. Razlikujemo WPA i WPA2 zaštitu. WPA zaštita je većinom usklađena sa 802.11i standardom, dok WPA2 u potpunosti implementira taj standard.

U daljnjem tekstu će biti detaljnije opisane metode funkcioniranja WPA/WPA2 zaštite kao i moguće metode napada.

Ključna razlika naspram prijašnje metode (WEP) je odvajanje korisničke autentikacije od osiguravanja tajnovitosti i cjelovitosti samih podataka. Navedenim načinom je osigurana sigurnosna arhitektura koja je skalabilna i robusna te se može prilagoditi kako zahtjevima kućnog korisnika tako i velikih korporacija. Ovaj princip se naziva Robust Security Network (RSN) i koristi 802.1X autentikaciju, robusnu raspodjelu ključeva te nove mehanizme osiguravanja tajnovitosti i cjelovitosti podataka. Kako bi se osigurala kompatibilnost sa starijom mrežnom opremom koja ne podržava novi standard definiran je Transitional Security Network (TSN) u kojem mogu sudjelovati novi standard RSN i stari, WEP. Ukoliko autentikacija između entiteta u bežičnoj mreži koristi rukovanje u četiri koraka ono se naziva Robust Security Network Association (RSNA). Uspostavljanje sigurne komunikacije se sastoji od četiri dijela (Slika 2.):

- Dogovor oko sigurnosnih metoda
- 802.1X autentikacija
- stvaranje ključeva i njihova distribucija
- RSNA podatkovna sigurnost

U sljedećim odlomcima biti će detaljno objašnjen način uspostavljanja veze u WPA standardu, kako bismo bolje razumjeli opise napada na ovaj standard [2].

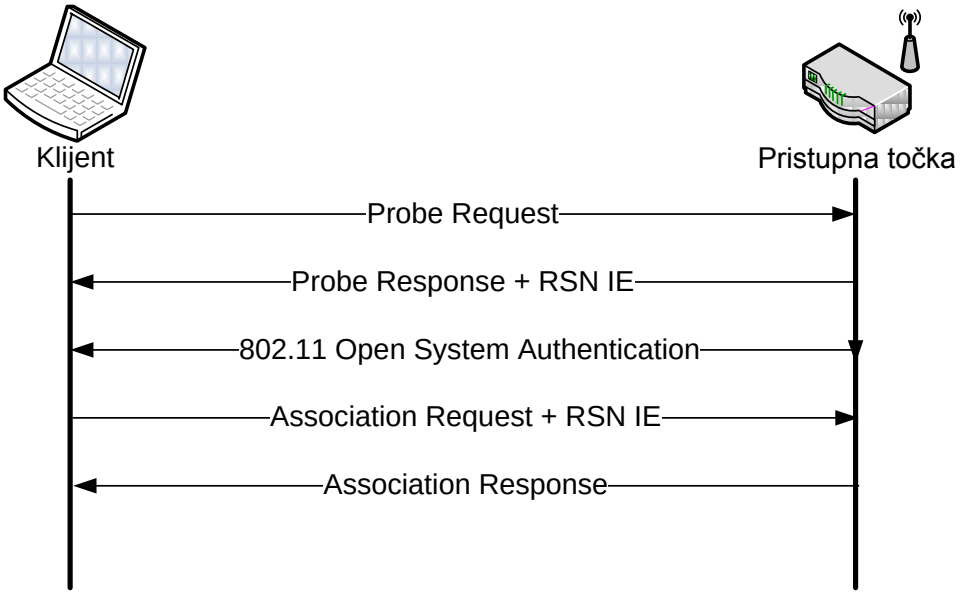


Slika 2. Autentikacija u četiri koraka

3.1 Prva faza, dogovor oko sigurnosnih metoda

Kako bi spajanje na pristupnu točku moglo početi, zainteresirane strane se moraju dogovoriti oko korištenja sigurnosnih metoda. Pristupna točka u svojoj Beacon ili Probe Respond poruci oglašava svoje raspoložive metode. Nakon toga slijedi „open authentication“ poruka koja je slična kao i kod TSN arhitekture. Odgovor klijenta je dan u poruci Association Request na koju zatim pristupna točka odgovara sa Association Response, odabir sigurnosne metode se nalazi u RSN IE polju Association Request poruke (Slika 3.) RSN IE polje sadrži sljedeće podatke:

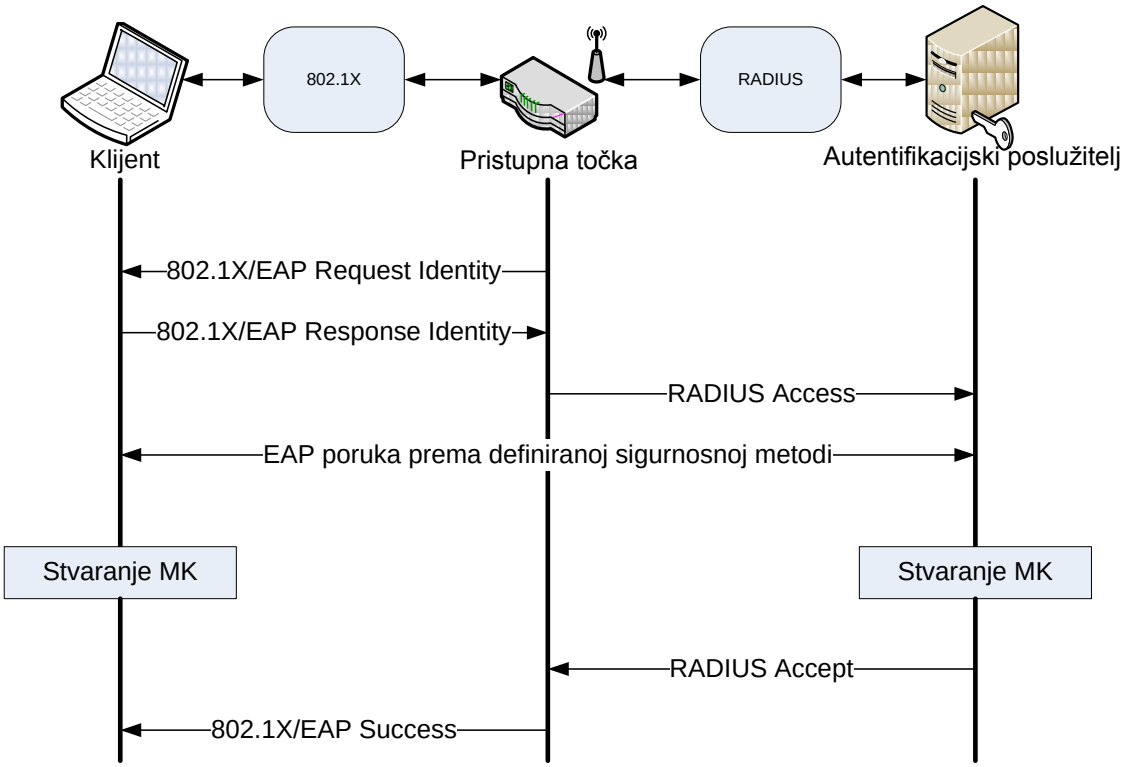
- podržane autentikacijske metode (802.1X, Pre-Shared Key (PSK)),
- sigurnosni protokoli za jednoodredišni promet (CCMP, TKIP itd.) ,
- sigurnosni protokoli za višeodredišni promet (CCMP, TKIP itd.) ,
- podrška za pred autentikaciju koja dopušta korisnicima jednostavniji i transparentni prijelaz na drugu pristupnu točku unutar iste mreže.



Slika 3. Prva faza prvi 802.11i autentikaciji

3.2 Druga faza, 802.1X Autentikacija

Druga faza se sastoji od 802.1X autentikacije zasnovane na Extensible Authentication Protocol (EAP) i sigurnosnoj metodi koja je dogovorena u koraku prije kao što su EAP/TLS, EAP/TTLS ili PEAP. 802.1X autentikacija počinje kada pristupna točka pošalje zahtjev za podatcima koji identificiraju klijenta. Nakon toga slijedi razmjena poruka unutar koje se stvara zajednički Master Key (MK). Procedura završava Radius Accept porukom od autentikacjiskog poslužitelja prema pristupnoj točki koja sadržava MK i krajnju EAP Success poruku za klijenta. Slijed poruka je prikazan na slici 4.

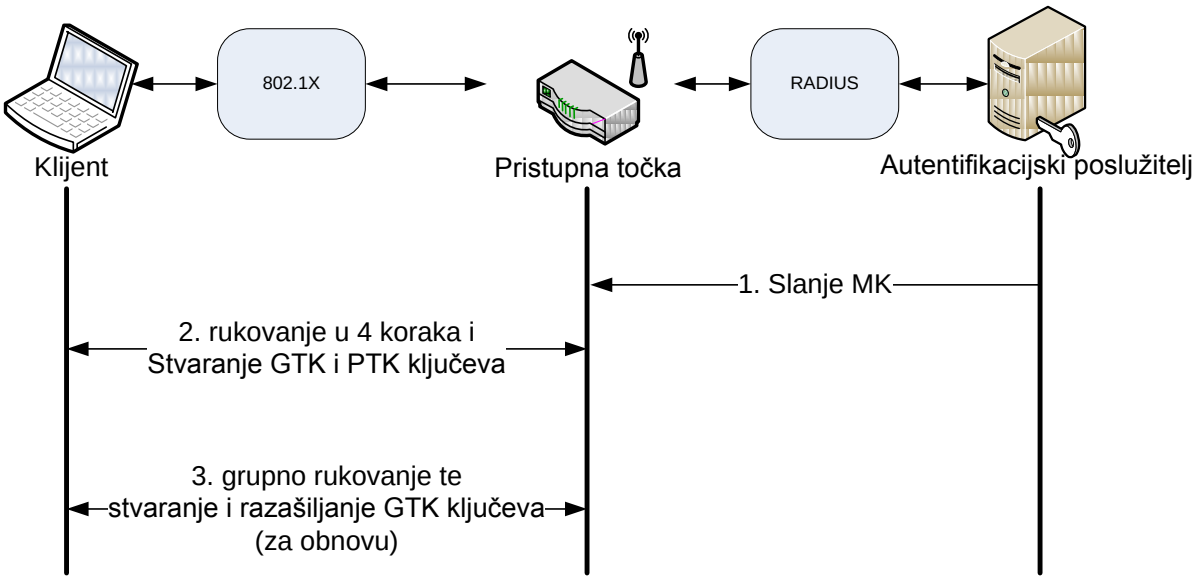


Slika 4. Druga faza, 802.1X autentikacija

3.3 Treća faza, hijerarhija ključa i njegova distribucija

Sigurnost komunikacije se oslanja na tajnost ključeva. U RSN svaki od ključeva ima ograničeno vremensko trajanje. Sigurnost cijelog sustava je osigurana skupom ključeva organiziranih u hijerarhiju. Nakon što se uspostavi sigurna sjednica koriste se privremeni ključevi sa ograničenim vremenskim trajanjem dok god se sjednica ne završi. Stvaranje tih ključeva i njihova razmjena se vrši u trećoj fazi (slika 5.). Prilikom stvaranja ključeva i njihove razmjene potrebno je obaviti dvije uspostave veze:

- uspostava veze u četiri koraka za Pairwise Transient Key (PTK) i izvedeni Group Transient Key (GTK)
- grupna razmjena ključeva za obnovu GTK



Slika 5. Stvaranje ključeva i njihovo razašiljanje

Način stvaranja Pairwise Master Key (PMK) ovisi o odabranoj metodi autentikacije:

- Ukoliko se koristi Pre-Shared Key (PSK), PMK je jednak PSK. PSK se stvara iz riječi koja sadrži između 8 i 63 znaka. Ovakav način pruža jednostavnu implementaciju sigurnosti kod kućnih korisnika ili malih tvrtki budući da ne zahtjeva autentikacijski poslužitelj.
- Ako se koristi autentikacijski poslužitelj onda se PMK stvara iz 802.1X autentikacijskog MK.

PMK se nikada ne koristi za kripitiranje nego se iz njega stvaraju privremeni ključevi ograničenog vremenskog trajanja. Za jednoodredišni (*eng. unicast*) promet taj ključ se naziva Pairwise Transient Key (PTK). Duljina PTK ključa ovisi o korištenom kriptografskom protokolu. TKIP ima ključ duljine 512 bita, dok CCMP ima ključ duljine 384 bita. PTK ključ se sastoji od više polja:

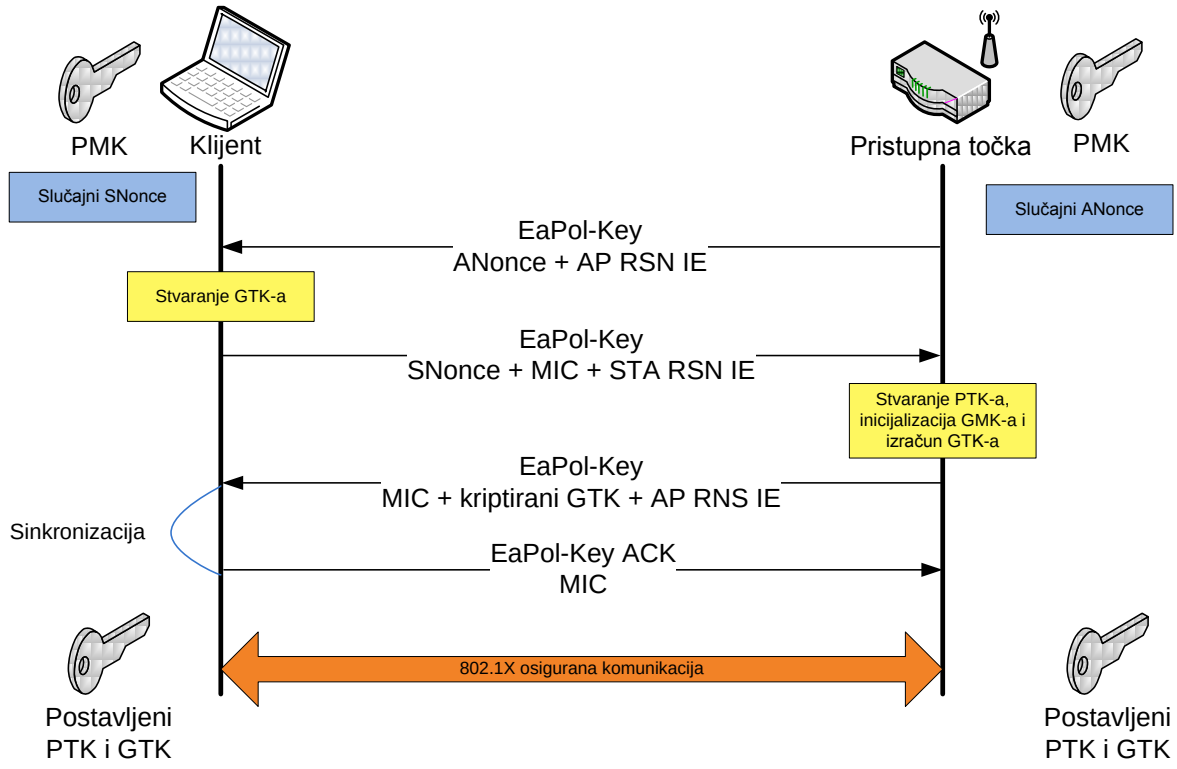
- Key Confirmation Key (KCK) – ključ dužine 128 bita namijenjen korištenju u autentikacijskim porukama (MIC) tijekom uspostavljanja veze.

- Key Encryption Key (KEK) – ključ dužine 128 bita namijenjen osiguravanju povjerljivosti podataka tijekom uspostavljanja veze.
- Temporary Key – ključ dužine 128 bita kojim se kriptiraju podatci kod TKIP-a ili CMMP-a.
- Temporal MIC Key – ključ dužine od dva puta po 64 bita služi autentikaciji podataka pri korištenju Michael algoritma sa TKIP protokolom. Svaka krajnja točka u komunikaciji ima svoj ključ.

Korištenjem uspostave veze u četiri koraka koju inicira pristupna točka moguće je:

- potvrditi znanje klijenta o PMK,
- stvoriti novi PTK,
- postaviti ključeve koji osiguravaju tajnost i cjelovitost,
- zaštiti prijenos GTK ključa od čitanja i
- potvrditi odabir načina zaštite podataka.

Tijekom uspostave sigurne komunikacije u četiri koraka, koristi se protokol Extensible Authentication Protocol over LAN (EAPOL). Komunikacija potrebna za uspostavu sigurne veze sadrži četiri EAPOL-Key poruke se razmjene između klijenta i pristupne točke. Taj proces je prikazan na slici 6.



Slika 6. Uspostavljanje komunikacije u četiri koraka

PTK ključ se stvara iz PMK-a, znakovnog niza, MAC adrese pristupne točke, MAC adrese klijenta i dva slučajna broja (ANonce i SNonce). Pristupna točka stvara prvu poruku koja sadrži

slučajno stvoreni broj ANonce kojeg šalje klijentu bez zaštite. Klijent na temelju stvorenog SNonce i primljenih podataka može stvoriti PTK, a zatim i stvoriti pripadne MIC ključeve. MIC ključ zajedno sa SNonce se šalje pristupnoj točci u poruci kodiranoj sa KCK ključem. Pristupna točka zatim iz te poruke pročita SNonce broj pomoću kojeg može stvoriti PTK i njegove privremene ključeve. Nakon što su ključevi stvoreni moguće je provjeriti MIC u drugoj poruci kako bi pristupna točka znala da li se klijent zna PMK i da li je dobro izračunao PTK i privremene ključeve. U trećoj poruci koju šalje pristupna točka sadržan je GTK ključ kriptiran sa KEK ključem. Zadnja poruka šalje potvrdu o provedenom postupku te signalizira pristupnoj točki da je klijent postavio potrebne ključeve za komunikaciju. Nakon primitka te poruke pristupna točka postavlja svoje ključeve za komunikaciju.

Višeodredišni promet je zaštićen svojim ključem nazvanim Group Transient Key (GTK) koji se stvara iz Group Master Key (GMK). GMK se stvara iz znakovnog niza stalne duljine, MAC adrese pristupne točke i slučajnog broja GNonce. Dužina ključa varira između 128 i 256 bita ovisno o kriptografskom protokolu koji se koristi. Postupak razmjene ključeva je vrlo sličan kao i kod jednoodredišnog prometa pa neće biti dodatno razjašnjen.

4 Ranjivosti u WPA/WPA2 zaštiti

4.1 Ranjivosti u Pre-Shared Key (PSK) načinu rada

Premda je do sada objavljen veći broj potencijalnih ranjivosti u WPA/WPA2 zaštiti njihovo iskorištavanje nije praktično iskoristivo. Najpraktičniji napadi su oni na PSK ključ. PSK pruža mogućnosti jednostavnijeg postavljanja sustava bez autentikacijskog poslužitelja. PSK je niz znakova od 256 bita ili riječ od 8 do 63 slova preko kojega se izračunava ključ.

PSK ključ jednak je PMK ključu i izračunava se uz pomoć PBKDF2 metode PKCS#5 standarda koja za parametre uzima slijedeće vrijednosti: lozinka, SSID, SSID dužina, 4096, 256. Pri čemu je 4096 broj sažetaka, a 256 je dužina izlaza. Formula za izračun je definirana na sljedeći način:

$$PSK = PMK = PBKDF2(lozinka, SSID, dužina\ SSID - a, 4096{,}256)$$

PTK se stvara iz PMK korištenjem sigurnosnog rukovanja u 4 koraka. Sve informacije potrebne za njegovo izračunavanje se šalju nezaštićeno. Iz toga slijedi da snaga zaštite koju pruža WPA/WPA2 u PSK načinu rada leži na snazi samog ključa. Budući da se ključ izračunava na temelju nekoliko parametara koji ovise o pojedinoj pristupnoj točci i klijentu nije moguće stvoriti napad sa sažetcima već izračunatih lozinki.

Napad na ključ je moguć isprobavanjem svih kombinacija, problem takvog procesa je trajanje i vrlo često praktična neizvedivost u zadovoljavajućim vremenskim okvirima. Kako bi se znatno ubrzao proces pogađanja lozinke potrebno je snimati promet između pristupne točke i klijenta koji uključuje uspostavljanje sigurne veze u četiri koraka. Točnije potrebno je imati prve dvije poruke toga postupka kako bi se moglo početi pogađati PSK vrijednost. U te dvije poruke kao što je već opisano se nalaze vrijednosti ANonce i SNonce na temelju kojega se može smanjiti područje rješenja za PSK. Ukoliko je PSK pogođen, iz MIC polja moguće je izračunati KCK [3].

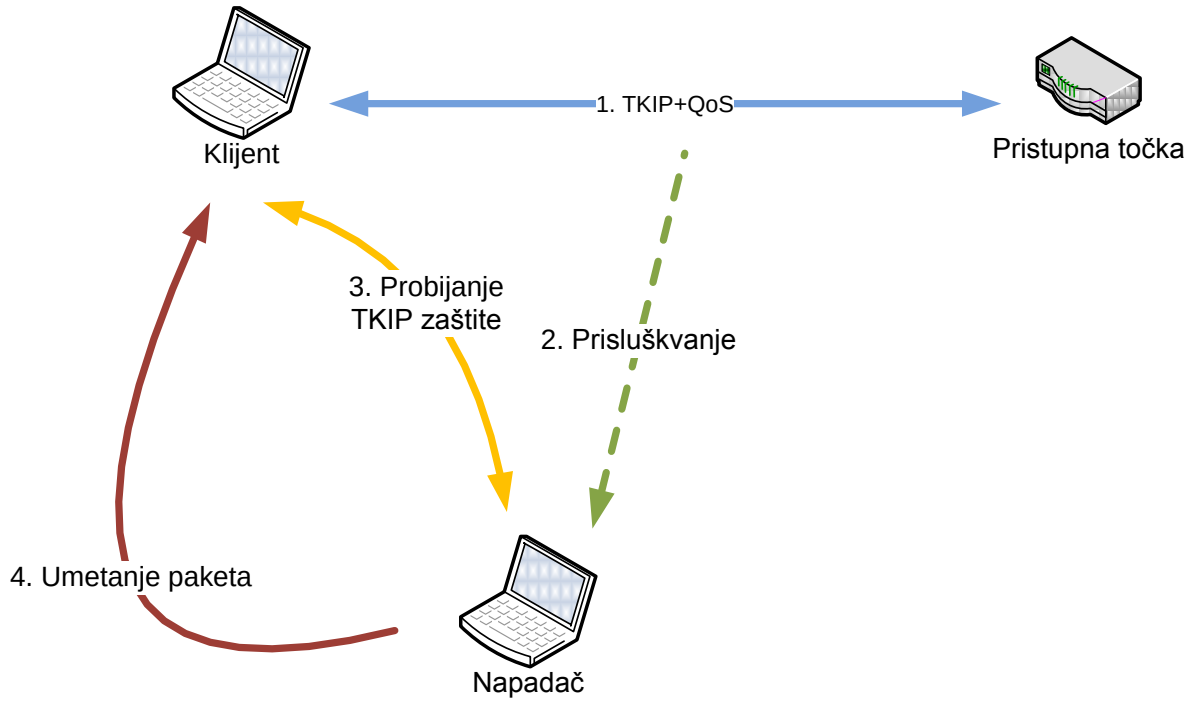
4.2 WPA TKIP ranjivost

Ranjivost TKIP komponente unutar WPA zaštite je otkrivena 2008. godine. TKIP je stvoren kako bi WPA bio kompatibilan sa starijim uređajima koji su podržavali samo WEP zaštitu. Kako bi ranjivost mogla biti iskorištena pristupna točka mora ispunjavati nekoliko uvjeta:

- Najvažniji uvjet koji pristupna točka mora ispuniti je podržavanje višestruke struje (eng. multiple streams) podataka o kvaliteti usluge (QoS). Takav način praćenja QoS je uključen u IEEE 802.11e standardu kojeg implementira većina današnjih uređaja.
- IP adrese u napadanoj mreži moraju biti dobrim dijelom poznate napadaču
- Veliki interval između obnove privremenog ključa (npr. 3600 sekundi)

Današnje korisničke mreže u velikom broju ispunjavaju zadane uvjete. Napad počinje snimanjem prometa u mreži dok se ne zapazi paket protokola ARP. Njih je lagano zapaziti zato što izvorišna adresa nije kriptirana i karakteristične su duljine. Sadržaj paketa u ARP zahtjevu većinom nije kriptiran. Dijelovi koji jesu kriptirani su: zadnji bajt izvorišne i odredišne adrese, 8 bajtova MICHAEL MIC-a i 4 bajta ICV zaštitne sume. Kako bi dekriptirao ostatak paketa napadač pokreće takozvani *chopchop* napad. Da bi napad uspio potrebno je koristiti različiti QoS

kanal u odnosu na onaj sa kojega je primio paket. Obično postoji kanal sa vrlo malo ili bez prometa kod kojeg je TSC brojač još uvijek manji. Ukoliko je pokušaj pogađanja posljednjeg bajta *chopchop* napada bio neuspješan paket će se odbaciti. Ukoliko je pokušaj pogađanja bio uspješan, klijentu se šalje MIC okvir s izvješćem o pogrešci, ali se TSC brojač ne uvećava. Napadač mora čekati barem 60sekundi nakon kako bi mogao pokušati ponovo pogoditi (slika 7.) [4].



Slika 7. Napad na WPA-TKIP

U trenutnom obliku šteta koja se može napraviti sa ranjivosti TKIP-a u WPA je ograničena. Ukoliko napad uspije napadač može nesmetano umetnuti određeni broj paketa u komunikaciju, veću štetu je teško napraviti iz nekoliko razloga:

1. Osnovni ključ za pristup mreži se ne razotkriva
2. Funkcionira samo ukoliko je uključen QoS na višestrukim kanalima
3. Napad je spor, barem 12 minuta prije nego što je moguće umetnuti pakete. Nakon što je moguće umetnuti pakete, tempo umetanja je7-15 paketa svakih 4 minute.
4. Umetnuti paketi moraju biti vrlo mali, manji od 100 bajtova
5. Umetanje paketa u pristupnu točku nije moguće. Moguće je umetnuti samo u klijenta.

Budući da je otkrivanje sigurnosnih propusta i njihovo iskorištavanje uglavnom evolucijski proces, što se pokazalo sa WEP zaštitom, ovaj propust mogao bi poslužiti kao početna točka za opasnije napade.

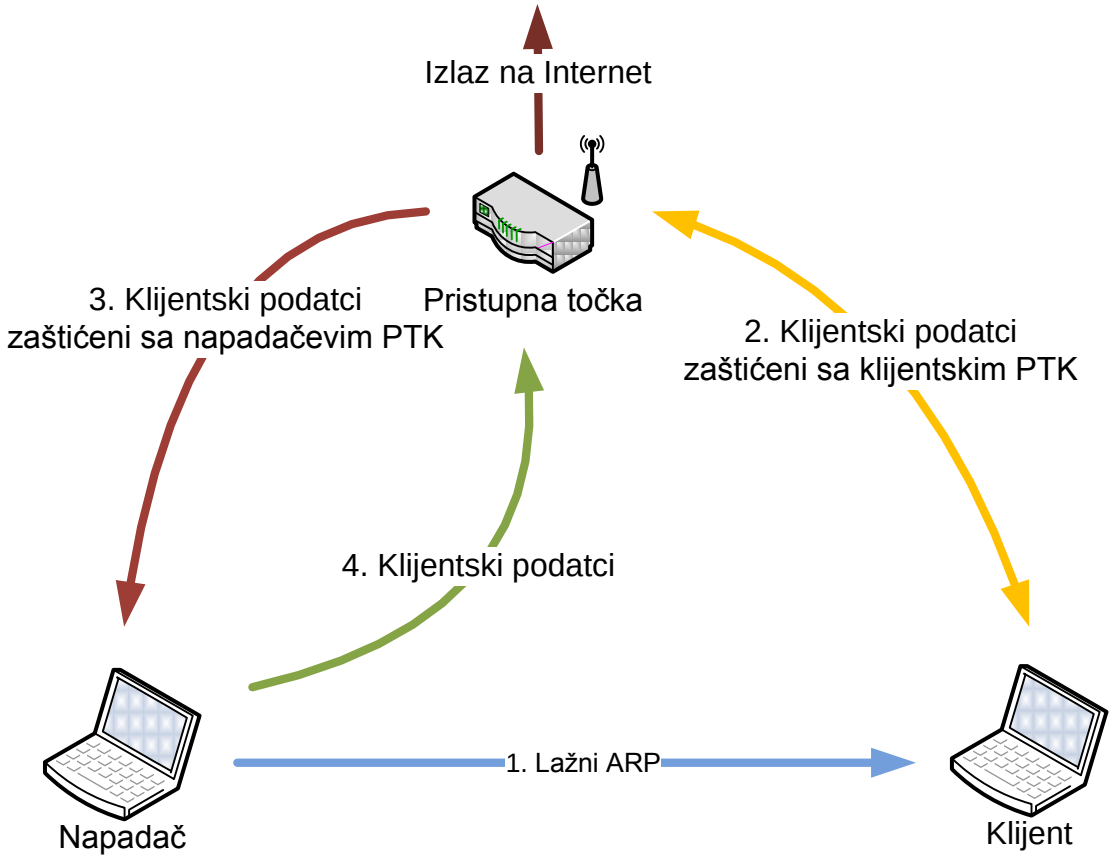
4.3 Rupa 196

Do pojave propusta poznatog pod nazivom „Hole 196“ ili rupa 196 u WPA2 zaštiti nije bilo poznatih mogućnosti napada osim pogađanjem lozinke. Na Defcon konferenciji 2010. godine je predstavljena ranjivost i softver koji iskorištava tu ranjivost. Pronađena ranjivost omogućuje dekriptiranje komunikacije drugih korisnika napadaču koji se već nalazi u mreži. Kao što je već objašnjeno u prethodnim poglavljima u WPA2 zaštiti svaki korisnik ima svoj ključ za komunikaciju koji je stvoren na temelju zajedničkog ključa. Na taj način se štiti povjerljivost komunikacije svakog korisnika. No uz pojedinačne ključeve, svi klijenti dijele jedan zajednički grupni ključ, Group Temporal Key (GTK). GTK ključ je potreban kako bi klijentska računala mogla primiti višeodredišne i sveodredišne (*eng. broadcast*) poruke od pristupne točke. GTK je jednak za sve korisnike na jednom basic service set ID (BSSID). Svaka pristupna točka ima jedinstveni BSSID. Prema specifikaciji 802.11-2007 samo pristupna točka može slati pakete koji su zaštićeni GTK ključem.

Napadačko računalo koje je već spojeno na pristupnu točku posjeduje GTK ključ sa kojim može stvoriti sveodredišni pakete i poslati ih drugim korisnicima mreže. Budući da pristupna točka samo šalje podatke ona će ignorirati paket, no ukoliko se kao izvorišna adresa postavi ona pristupne točke korisnička računala neće znati razliku i neće moći provjeriti da li se radi o lažiranom paketu ili ne.

Ovakav propust omogućava napadaču da izvede napad lažiranim Address Resolution Protocol (ARP) paketom. Sam napad se provodi u nekoliko koraka.

1. Napadač šalje lažirani ARP paket. U lažiranom paketu se kao izlaz iz mreže postavi napadačko računalo, tako da sav odlazni promet prolazi preko napadačkog računala.
2. Nakon što klijentska računala imaju krive zapise o relaciji MAC adresa i IP adresa, šalju svoje podatke napadačkom računalu preko pristupne točke. Promet od klijenta prema pristupnoj točci je zaštićen klijentskim PTK-om.
3. Zatim pristupna točka preusmjeruje promet (zbog krivo zapisa o MAC adresama) napadaču. Pristupna točka dekriptira promet pomoću klijentskog PTK-a i ponovo zaštićuje sa napadačkim PTK-om.
4. Sada napadač može pročitati sav promet klijenta. Kako klijent ne bi zamijetio napad, napadač prosljeđuje klijentski promet na pravu lokaciju (Slika 7.).



Slika 7. Tijek „hole 196“ napada

Budući da napadač nakon uspješno provedenog napada ima pristup prometu svih klijenata može snimati njihov promet kako bi došao do povjerljivih informacija poput korisničkih imena i lozinki, brojeva kreditnih kartica i slično. Također napadač može izvršiti napad uskraćivanjem usluge (*eng. DoS*) ili umetnuti maliciozni softver [5].

5 Zaključak

Sigurnost računalne mreže postaje sve važniji faktor u jednakoj mjeri kod kućnih korisnika kao i kod poslovnih korisnika. Kako bi zaštitili svoju mrežu korisnicima se preporuča postavljanje zaštite na WPA standard sa AES kriptografskim standardom kako bi ostvarili maksimalnu zaštitu. WEP zaštita je izrazito slaba i bilo tko s malo većim znanjem o računalnim mrežama ju može probiti, iz toga razloga se preporuča što prije prijeći na neki oblik WPA zaštite. Za sada je jedini dostupni napad na WPA zaštitu koji omogućava potpun pristup mreži onaj sa pogađanjem lozinke. Postoje načini koji smanjuju područje rješenja ali opet njihovo izvršavanje traje. Kod kućnih korisnika jačina zaštite ovisi izravno o dužini lozinke. Kod korištenja cjelovitog WPA sustava sa autentikacijskim poslužiteljem sigurnost je još veća. Sigurnosni propust pri TKIP-u je prisutan no ima vrlo ograničenu primjenu. Hole 196 ranjivost je puno ozbiljnija no zahtjeva popriličnu količinu tehničkog znanja kako bi se iskoristila i pruža opasnost samo od unutarnjih napada. Velike tvrtke su podložne takvom tipu napada gdje veliki broj korisnika ima pristup mreži. Do početnog pristupa samoj mreži u velikoj tvrtci moguće je doći i socijalnim inženjeringom kao uvod u daljnji napad. Zaštita od Hole 196 napada je za sada samo korištenje dodatnih sigurnosnih protokola poput SSL/TLS-a.

6 Literatura

1. John Edney, William A. Arbaugh ; Real 802.11 Security Wi-Fi Protected Access and 802.11i, Addison Wesley – ISBN: 0-321-13620-9, 2004
2. Guillaume Lehembre, Wi-Fi security – WEP, WPA and WPA2, 2005
3. Martin Beck, Erik Tews; Practical attacks against WEP and WPA, 2008
4. AirTight Networks; WPA/WPA2 TKIP Exploit: Tip od the Iceberg?, 2009
5. AirTight Networks; Hole196 Vulnerability in WPA2 2009