WPA3

Denis Fidel

Sušak 3a,6254 Jelšane
Kontakt: denis.fidel12@gmail.com

Abstract. Zaradi velikega naraščanja uporabe pametnih telefonov in pametnih ur ter prenosnih računalnikov v zadnjih letih, je narasla tudi uporaba brezžičnih omrežij. Posledično so brezžična omrežja postala vse bolj zanimiva za napadalce, kar zahteva tudi razvoj varnostnih protokolov z namenom zaščite uporabnikov tovrstnih naprav. Pri svojem projektu sem predstavil najnovejši varnostni protokol za zaščito uporabnikov brezžičnih omrežij - WPA3. Ker je WPA3 nastal na temeljih WPA2 in z namenom odpravljanja njegovih pomanjkljivost sem najprej na kratko predstavil WPA2 in napad, ki ga slednji dopušča. Poročilo sem zaključil s primerjavo obeh protokolov in ugotovitvijo, da WPA3 kljub vsemu ne odpravi vseh pomanjkljivosti svojega predhodnika. Največja težava ostaja *Evil twin* napad, ki je tudi v najnovejši verziji protokola WPA3 še vedno mogoč.

Key words: WPA3, WPA2, Evil twin napad, KRACK napad, CCMP, Four-way handshake, Dragonfly handshake

1 UVOD

Zaradi velikega naraščanja uporabe pametnih telefonov in pametnih ur ter prenosnih računalnikov v zadnjih letih, je narasla tudi uporaba brezžičnih omrežij. Posledično so brezžična omrežja postala vse bolj zanimiva za napadalce, kar zahteva tudi razvoj varnostnih protokolov z namenom zaščite uporabnikov tovrstnih naprav. Glavna naloga varnostnih protokolov pri brezžičnih omrežjih je zagotavljanje zaupnosti, celovitosti in preverjanje pristnosti (angl. confidentiality, integrity and authentication)

Začetki razvoja varnostnih protokolov za brezžična omrežja segajo v leto 1999 z nastankom protokola WEP [13]. Kmalu se je izkazalo, da ta ni dovolj varen, zato je v letu 2003 nastal WPA, ki je bil zamišljen kot prehodna različica WPA2 [12]. Cilj tega poročila je predstavitev in varnostna analiza protokola WPA3, ki je bil objavljen v letu 2018. Ker je WPA3 strukturiran podobno kot WPA2, bo najprej v 2. razdelku za potrebe razumevanja WPA3 opravljen pregled protokola WPA2, skupaj z njegovimi slabostmi. Predstavljen bo tudi sistematičen pregled napada na WPA2, na podlagi katerega bo v 3. razdelku opisan WPA3, skupaj z varnostno analizo. V nadaljevanju, v 4. razdelku, se bom posvetil primerjavi med obema protokoloma. Za konec bo v 5. razdelku sledil še kratek povzetek in zaključne besede.

2 WPA2

Predhodnika protokola WPA2 temeljita na tokovni šifri RC4, ki je sicer hitrejša kot DES in AES, ampak ima veliko pomanjkljivosti - glej članke Ferreira [2], Stubblefield, Ioannidis in Rubin: [4] ali Tews, Weinmann in Pyshkin [5]. Ker sta WEP in WPA temeljila na RC4, je bila tudi strojna oprema dostopnih točk in naprav prilagojena za uporabo le-te.

WPA2 je v tem pogledu prinesel veliko spremembo. Osnova za šifriranje sporočil je namreč postal AES, kar je posledično pomenilo zahtevo po novejši, zmogljivejši strojni opremi. Natančneje WPA2 za šifriranje uporablja protokol CCMP, ki temelji na protokolu AES. Kot prikazuje slika 2, je sporočilo šifrirano po protokolu CCMP rezultat funkcije XOR s parametroma `P` (Plaintext) in `KS` (Keystream). Parameter `P` predstavlja vhodno sporočilo, ki ga želimo šifrirati (vsebina trenutno poslanega paketa). Na drugi strani pa `KS` predstavlja generiran ključ, ki nastane na podlagi protokola AES. Izračun `KS` temelji na različnih parametrih, med drugim tudi `PTK` ali `GTK` (predstavljena spodaj).

Pri šifriranju v protokolu CCMP se torej uporabljata 2 ključa: `PTK` (angl. Pairwise Transient Key) ali `GTK` (angl. Group Temporal Key). Prvi se uporablja, ko je paket namenjen enemu prejemniku (angl. unicast), drugi pa v primeru, ko gre za paket namenjen vsem uporabnikom (angl. broadcast). V obeh primerih morata naprava, ki se povezuje in dostopna točka ob vzpostavitvi povezave generirati oba ključa. Proces povezave uporabnikove naprave in dostopne točke, kjer izpeljeta `PTK` in `GTK` imenujemo *Four-way handshake* in ga prikazuje slika 1.

Če povzamemo, pred zahtevo za povezovanje naprava in dostopna točka izračunata `PMK` (angl. Pairwise Master Key), ki nastane kot rezultat funkcije, katere glavni argument je `PSK` (angl. Pre-Shared Key), znan tudi kot omrežno geslo. Poleg `PMK`, pa dostopna točka generira tudi `GMK` (angl. Group Master Key), ki se uporabi pri

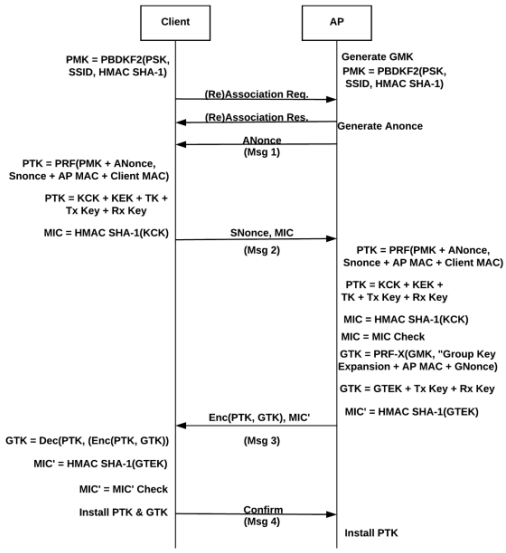

Figure 1. Four-way handshake. [3]

izpeljavi GTK. Ob uporabnikovem zahtevku za povezavo dostopna točka (AP) generira naključno število Anonce in ga pošlje napravi, ki zahteva povezavo. Naprava izbere svoje naključno število (Snonce) in skupaj z ostalimi parametri izračuna PTK in nato še MIC (Message Integrity Ckeck) vrednost, ki zagotavlja, da med prenosom vrednost Snonce ni bila spremenjena. Dostopna točka nato po istem postopku izračuna PTK in MIC, ter preveri ali se izračunan MIC in MIC s strani naprave ujemata. Za tem dostopna točka izračuna še GTK, ga šifrira s PTK ključem (ki ga naprava, ki se povezuje že pozna in posledično lahko odšifrira) in podobno kot prej izračuna še vrednost MIC, vendar tokrat za GTK. Šifriran GTK in MIC se pošlje napravi, ki preveri ali se podatki ujemajo in ob uspešnem preverjanju shrani ključa PTK in GTK, ter slednje sporoči dostopni točki.

Kot vidimo, PTK in GTK nastaneta na podlagi naključno izbranih števil, ki sta različna vsako sejo. S tem WPA2 zagotavlja, da naprava ob vsakem priklopu na dostopno točko za šifriranje podatkov med komunikacijo uporablja nove šifrirne ključe.

Po uspešnem dogovoru o PTK in GTK ključu si torej lahko naprava in dostopna točka izmenjujeta šifrirane pakete. Kot že omenjeno, šifriranje poteka po protokolu CCMP, katerega shemo vidimo na sliki 2.

2.1 Pomanjkljivosti

Prvotna pomanjkljivost WPA2 je bila zahteva po novi strojni opremi, saj AES zahteva večjo računsko moč kot predhodnik RC4. V tem poročilu se bomo bolj osredotočili na pomanjkljivosti, ki so sprožile razvoj WPA3, in sicer napada KRACK in *Evil twin*.

Kot je pokazal Bartoli v članku [6] lahko z metodo KRACK [10] (angl. Key Re-installation Attack)

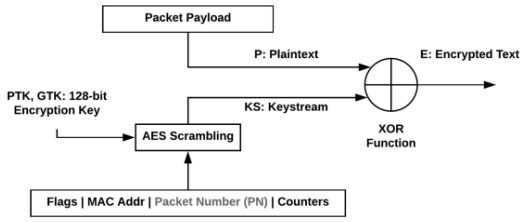

Figure 2. Šifriranje po protokolu CCMP. [3]

izvedemo napad na WPA2 oz. konkretneje na *Four-way handshake*. Izkaže se, da WPA2 dovoli ponovno pošiljanje sporočil iz *Four-way handshake*a, z namenom hitrejše ponovne povezave med napravo in dostopno točko. V praksi namreč naprava v isti seji večkrat prekine in ponovno vzpostavi povezavo z dostopno točko (npr. ko nekaj časa ne uporabljamo mobilnega telefona). Napadalec lahko to izkoristi in s časom odšifrira podatke, ki si jih izmenjujeta uporabnik in dostopna točka. KRACK napad je podrobneje predstavljen v podrazdelku 2.2.1.

Dodatna pomanjkljivost protokola WPA2 je, da omogoča pošiljanje *management* paketov brez šifriranja. Napadalec lahko to izkoristi tako, da s *spoof* tehniko ponaredi izvor sporočila oz. se lažno predstavi kot ena od naprav, povezana na dostopno točko in na ta način dostopni točki v imenu naprave pošilja pakete za deavtentikacijo. S tem lahko napadalec na dostopni točki povzroči *DoS*.

Ostale probleme protokola WPA2 in potek napada na WPA2 bomo predstavili v razdelku 2.2.

2.2 Napad na WPA2

V tem razdelku bomo podrobneje predstavili, kako poteka napad na uporabnika in/ali dostopno točko, ki uporablja WPA2 protokol. Napad bo predstavljen sistematično v več korakih in iz več manjših napadov. Nekateri od njih bodo predstavljeni tudi podrobneje. Pregled tega napada na protokol WPA2 je ključnega pomena pri razumevanju protokola WPA3, saj je ta nastal ravno z namenom odpravljanja tovrstnih pomanjkljivosti, zato bo temu delu namenjenih tudi nekaj več besed, čeprav je primarna tema tega članka protokol WPA3.

Celoten napad je razdeljen v štiri faze. Posamezna faza se začne v določenem stanju, glede na položaj napadalca. Prehod med stanji je lahko neposreden, lahko pa ga napadalec doseže z napadom (npr. Deauthentication attack), s katerim pridobi dodatne informacije in preide v naslednje stanje ali pa doseže končen cilj.

Prva faza se začne v stanju, ko napadalec nima dostopa do omrežja (stanje 3.1.1 na sliki 3), niti do gesla omrežja. Napadalec lahko v tem stanju, glede na želen cilj, izbere enega od 4 napadov:

1) *Deauthentication Attack*, s katerim povzroči *DoS*

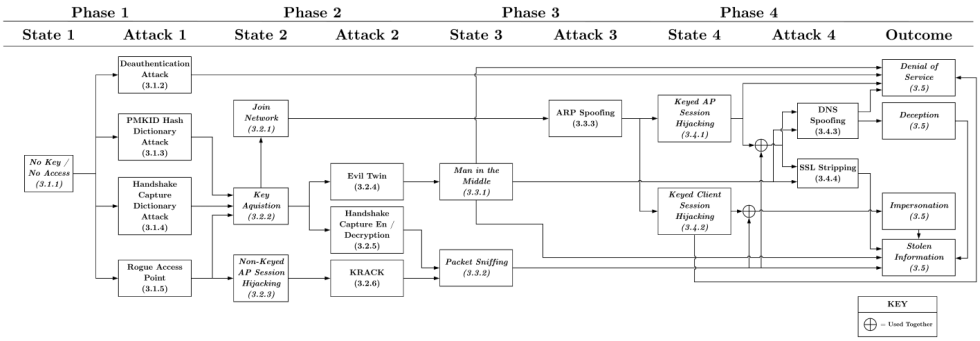

Figure 3. Napad na protokol WPA2. [3]

na dostopni točki. Izvede ga tako, da pošilja veliko količino *deauhentication* paketov v imenu uporabnika in s tem onemogoči delovanje dostopne točke.

2) *Handshake Capture Dictionary Attack*, kjer napadalec poizkuša različna omrežna gesla in z zajetim *Four-way handshake*om prometa med napravo in dostopno točko preverja pravilnost posameznega vnosa. Preverjanje, ali je posamezno geslo pravilno mu omogoča predhodno zajet *Four-way handshake*, saj ima tako vse podatke za izračun `PTK` (iz `PMK` na podlagi uganjenega gesla `PSK`) in tudi `MIC`, s katerim preverja ujemanje.
3) `PMKID` *Hash Dictionary Attack*, kjer napadalec poizkuša različna omrežna gesla (`PSK`) in izračuna PKMID hash, ki ga primerja s poslanim pred *Four-way handshake*om. `PMKID` je rezultat zgoščevalne (angl. hash) funkcije, kjer je edina neznanka napadalcu `PMK`. S poskušanjem različnih `PSK` in izračunom pripadajočega `PMK` (glej prvo vrstico na sliki 1) lahko napadalec dobljen `PMKID` primerja s poslanim med avtentikacijo uporabnika.
4) *Rogue Access Point*, kjer napadalec postavi lažno dostopno točko (podobno kot za *Evil-twin*) in z različnimi tehnikami, kot je denimo *phishing*, od uporabnika ob povezavi zahteva ponoven vnos gesla. Ovira pri tovrstnem napadu je lahko fizičen dostop do omrežja.

V drugi fazi je lahko napadalec glede na izbran napad v prvi fazi v različnih stanjih. Lahko je v stanju, ko ima geslo za povezavo z omrežjem (`PSK`) in se lahko tudi sam poveže v omrežje. Če ima dostop do `PSK`, lahko s poslušanjem prometa tudi odšifrira komunikacijo med uporabnikom in dostopno točko. V primeru, da je bil v prvi fazi izveden *Rogue Access Point* napad, pa se napadalec v stanju, ko uporabnik misli, da komunicira z dostopno točko, v resnici pa vsa komunikacija poteka z t.i. ponarejeno dostopno točko (angl. Rouge access point). V slednjem primeru napadalec nima dostopa do šifrirnega ključa, zato ne more odšifrirat izmenjane podatke med uporabnikom in dostopno točko (kot je to slučaj pri *Evil-twin* napadu), lahko pa izvede KRACK napad.

Omenjena napada KRACK in *Evil twin* sta največji pomanjkljivosti protokola WPA2, zato sta podrobno predstavljena v podrazdelkih 2.2.1 in 2.2.2. Iz njiju lahko napadalec preide v eno od stanj v tretji fazi na sliki 3, iz katerih lahko nato nadaljuje kot prikazuje slika. Na tem mestu bi podrobnosti 3. in 4. faze izpustil, saj je tema tega poročila protokol WPA3. Podrobnejši opis in potek posameznega napada najdemo v 3. poglavju članka Kohliosa in in Hayajneha [3].

Za konec omenimo še, da po uspešno izvedenih napadih in želenih prehodih med fazami, napadalec lahko zaključi v naslednjih 4 stanjih (skladno s sliko 3):

1) Povzroči *DoS* na dostopni točki.
2) V stanju, ko uporabnik misli da komunicira z drugim uporabnikom ali dostopno točko, v resnici pa komunicira z napadalcem (angl. deception).
3) V stanju, ko se napadalec ostalim uporabnikom in dostopni točki predstavi kot eden izmed uporabnikov, čigar identiteto je ukradel (angl. impersonation).
4) V stanju, ko uporabniku ukrade občutljive informacije (npr. gesla, PIN številke).

2.2.1 KRACK napad: S KRACK napadom lahko napadalec uspe odšifrirati sporočila med uporabnikom in dostopno točko, ne da bi poznal šifrirni ključ. Poglejmo najprej, kako poteka šifriranje pri WPA2 oz. kako se v postopku šifriranja uporabljajo ključi.

Postopek šifriranja po protokolu CCMP (glej sliko 2) v zadnjem koraku s funkcijo XOR združi izvorno sporočilo (angl. plaintext) in ključ (`KS`). Ključ `KS` je generiran iz `PTK` (ali `GTK`) in še nekaj ostalih podatkov na podlagi kriptosistema AES. Velja torej:

$$\mathtt{E} = \mathtt{P} \oplus \mathtt{KS},$$

kjer je `E` šifrirano sporočilo. Če napadalec uspe zajeti dva šifrirana paketa, in če privzamemo, da je `KS` v obeh primerih enak, iz zvez:

$$\mathtt{E}_1 = \mathtt{P}_1 \oplus \mathtt{KS} \text{ in } \mathtt{E}_2 = \mathtt{P}_2 \oplus \mathtt{KS}$$

dobimo:

$$\mathtt{E}_1 \oplus \mathtt{E}_2 = (\mathtt{P}_1 \oplus \mathtt{KS}) \oplus (\mathtt{P}_2 \oplus \mathtt{KS}) = \mathtt{P}_1 \oplus \mathtt{P}_2$$

Iz zgornje enačbe sledi, da če napadalec s poslušanjem prometa dobi E_1 in E_2 ter uspe uganiti ali pozna denimo P_1, potem lahko izračuna P_2. Tu lahko napadalec izkoristi morebitno privzeto prvo sporočilo, ki si ga izmenjata uporabnik in dostopna točka.

Preverimo še, zakaj smo lahko privzeli, da sta KS pri dveh zaporednih sporočilih enaka. V resnici WPA2 v splošnem poskrbi, da zaporedna KS nista enaka. Kot prikazuje slika 2 je KS odvisen od več parametrov, med drugim tudi od številke paketa (PN), ki je v splošnem vsak krog šifriranja večja. Če pogledamo ostale parametre podane v AES opazimo, da je v resnici PN edina spremenljivka (seveda znotraj trenutne seje) pri generiranju KS.

Kar napadalcu omogoči uporabo več enakih KS je izboljšava protokola WPA2, ki v resnici povzroči težavo. Pri povezavi uporabnika in dostopne točke je, kot že omenjeno, najprej prisoten *Four-way handshake*. Včasih se zgodi, da mora dostopna točka uporabniku ponovno poslati sporočilo v 3 koraku (Msg 3, slika 1), npr. zaradi ne prejemanja sporočila 4 (Msg 3, slika 1). V tem primeru uporabnikova naprava ponovno nastavi PTK in GTK in med drugim tudi ponastavi PN na 1. Spomnimo se, da je napadalec v stanju, ko uporabnik misli da komunicira z originalno dostopno točko, v resnici pa komunicira s ponarejeno (*Rougue-access point*). Napadalec v tem primeru povzroči ponovno pošiljanje *Msg 3*, potem pa spremlja pakete poslane s strani uporabnika. Podoben postopek lahko ponovi večkrat in tako dobi več paketov s $\mathtt{PN} = 1$, več paketov s $\mathtt{PN} = 2$, itd. Ko zbere dovolj paketov, lahko naredi XOR vseh parov paketov z istim PN. Če uspe uganiti ali če pozna vsebino enega paketa, lahko na ta način odšifrira vse ostale po korakih opisanih zgoraj.

2.2.2 Evil twin napad: Ker napadalec pozna geslo omrežja (PSK), lahko v bližini uporabnika postavi novo zlonamerno dostopno točko. Vse za kar mora poskrbeti je, da ima ta enak SSID, MAC in geslo kot originalna, ter da uporablja isti varnostni protokol. Vse omenjene podatke lahko pridobi s prisluškovanjem prometa med napravama. Ker lahko napadalec pri protokolu WPA2 dostopni točki pošilja ponarejene *deauthentication* pakete, lahko uporabnikovo napravo odjavi iz omrežja. Naprava bo v tem primeru poskusila s ponovno prijavo in pri tem ponavadi izbrala SSID z močnejšim signalom - dostopno točko napadalca. Ko je uporabnik povezan z lažno dostopno točko se ta lahko vede kot *Man in the middle* med uporabnikom in originalno dostopno točko. Na ta način lahko napadalec vidi ves promet, ki ga uporabnik pošilja in prejema.

3 WPA3

Zaradi zgoraj omenjenih pomanjkljivosti, je bil v letu 2018 objavljen protokol WPA3. Tako kot njegov predhodnik, tudi WPA3 za šifriranje sporočil uporablja protokol CCMP, ki zahteva vsaj 128 bitni šifrirni ključ. Šifrirna ključa (PTK ali GTK) sta tudi v tem primeru izpeljana preko *Four-way handshake*a. [12]

Glavna novost protokola WPA3 je način izračuna ključa PMK, ki se uporablja pri *Four-way handshake*u. V starejši verziji (WPA2) je bil PMK izračunan neposredno iz PSK in nekaj ostalih parametrov (glej sliko 1), sedaj pa dogovor o PMK poteka po protokolu *Simultaneous Authentication of Equals* (SAE). Avtentikacija uporabnika je prej temeljila na PSK, pri WPA3 pa temelji na protokolu SAE, ki poleg generiranja PMK opravlja še funkcijo avtentikacije uporabnika. SAE uporablja *Dragonfly handshake*, katerega osnova je problem diskretnega logaritma in kriptografija eliptičnih krivulj.

Za začetek se spomnimo, da je eliptična krivulja v splošnem predstavljena z enačbo:

$$y^2 = x^3 + ax + b \mod p,$$

kjer so:

$$a, b, p \in G \text{ parametri eliptične krivulje,}$$

in velja:

$$G = \langle g \rangle, |G| = q \text{ ter } p, q \in \mathbb{P}.$$

Poglejmo podrobneje, kakšen je postopek generiranja ključa PMK po protokolu SAE oz. *Dragonfly handshake*u, prikazanem na sliki 4. Naj na tem mestu omenim še eno novost v primerjavi z WPA2, in sicer, da geslo omrežja ni neposredno uporabljeno za izpeljavo ključa PMK, ampak se uporablja zgolj za avtentikacijo uporabnika.

Sam postopek generiranja PMK po protokolu SAE se prične z izračunom *password element*a (PE ali samo P), ki geslo omrežja uporablja zgolj kot seme (angl. seed). Parameter P je izračunan po t.i. principu *hunting-and-pecking* ali tudi *try-and-increment*. V osnovi gre za iskanje točke na eliptični krivulji s poizkušanjem različnih x koordinat. Kandidati za x koordinate so izpeljani iz zgoščene (angl. hash) vrednosti, ki nastane na podlagi začetnega semena, identitet obeh naprav (npr. MAC naslov) in števca. Za vsako x koordinato algoritem preveri ali pripadajoča točka (x, y) pripada dani eliptični krivulji. Če da potem algoritem proglasi $\mathtt{P} = (x, y)$, v primeru neuspeha pa poveča števec in postopek ponavlja dokler uspešno ne najde točke na eliptični krivulji, ki jo proglasi za P. Več informacij najdemo v članku Vanhoefa in Ronena [7]. S stališča varnosti je pomembno, da morata pri dogovoru o P pri tovrstnem dogovoru sodelovati tako uporabnikova naprava, kot tudi dostopna točka.

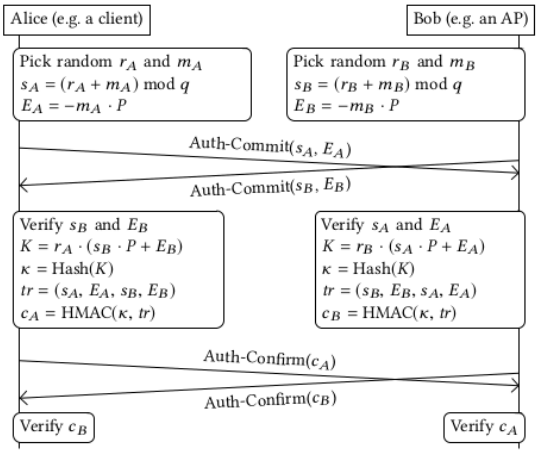

Figure 4. Dragonfly handshake. [7]

Ko je dogovor o točki P sklenjen, lahko obe strani začneta z generiranjem PMK - z *Dragonfly handshake*om (slika 4). Predhodno se obe napravi dogovorita o parametrih eliptične krivulje, ki se bo uporabljala. Sam *Dragonfly handshake* se začne z izbiro naključnih števil $r, m \in [2, q]$ in izračunom:

$$s = (r + m) \mod p \text{ in } \mathtt{E} = -m * \mathtt{P}.^*$$

V prvih dveh korakih *Dragonfly handshake*a si napravi izmenjata pripadajoči vrednosti s in E (natančneje s_A, E_A in s_B, E_B), kar pomeni da sta vrednosti s in E javni, medtem ko sta r, m tajni. Varnost protokola v tem primeru temelji na težavnosti problema DLP (angl. Discrete Logarithm Problem), natančneje da napadalec ne more izračunati m in znanega E in P. V resnici lahko s poslušanjem prometa zajame samo E, do vrednosti P, bi moral priti na kak drug način.

Po izmenjavi vrednosti s in točke E sledi preverjanje - obe strani preverita ali je $s \in [2, q]$ in ali je E veljavna točka na dani eliptični krivulji. V naslednjem koraku, vsaka stran zase izračuna K, kot prikazuje slika 4 in uporabi x koordinato točke K za izračun vrednosti $\kappa = H^\dagger(K)$. Za potrditev je izračunana še vrednost c (c_A ali c_B ustrezno), tako kot prikazuje slika 4. Za konec si obe napravi izmenjata izračunano vrednost c in preverita, da se vrednosti ujemata. S tem potrdita, da se izračunan κ ujema in proglasita κ za *Pairwise Master Key* (PMK). [7]

Preverimo še, da je izračunana točka K na obeh straneh res enaka. Kratek izračun pokaže, da velja:

$$K = r_A(S_B * \mathtt{P} + E_B)$$

$$= r_A(\mathtt{P} * r_B + \mathtt{P} * m_B - \mathtt{P} * m_B) = r_A * \mathtt{P} * r_B$$

po drugi strani pa

$$K = r_B(S_A * \mathtt{P} + E_A)$$

$$= r_B(\mathtt{P} * r_A + \mathtt{P} * m_A - \mathtt{P} * m_A) = r_B * \mathtt{P} * r_A$$

Kot že omenjeno zgoraj, po uspešnem dogovoru o PMK med napravama steče še *Four-way handshake* in s tem dogovor o šifrirnem ključu PTK (ali GTK), ki se uporablja za šifriranje paketov med uporabnikovo napravo in dostopno točko.

Poleg drugačnega načina izračuna PMK, pa se pri WPA3 pojavijo še nekatere druge novosti, in sicer:

- Dodaten nivo šifriranja sporočil/paketov med napravo in dostopno točko.
- Dodani so *Protection Management Frames* (PMF), in sicer z namenom šifriranja *management* paketov. S tem je napadalcu preprečen *Spoofing* management paketov, kot je npr. zahteva za deavtentikacijo.
- Dodan je mehanizem *Security Association* (SA), ki ščiti napravo in dostopno točko pred neavtenticiranimi *management* paketi.

V nadaljevanju, v razdelku 3.1 sledi varnostna analiza protokola WPA3, glede na predstavljen napad na WPA2 v razdelku 2.2.

3.1 Varnostna analiza

Poglejmo najprej protokol SAE, ki je novost in kaj z njim WPA3 pridobi. Če pogledamo *Dragonfly handshake*, opazimo da je ključno, da napadalec iz javnih podatkov ne more izračunati PMK. S pridobljenim PMK bi namreč napadalec lahko zlorabil *Four-way handshake*, podobno kot pri WPA2, o čemer smo govorili v razdelku 2.2. Poglejmo torej izračun PMK oz. K (slika 4). Tajni element pri izračunu K je r_A (oz. r_B), zato je pomembno, da napadalec ne pozna njegove vrednosti. Varnost r_A je kot že prej omenjeno zagotovljena s problemom DLP, saj zaradi njegove težavnosti napadalec iz E_A in P ne more izračunati M_A in posledično r_A. S tem je zagotovljen tudi t.i. *Forward secrecy* [9], ki v tem primeru pomeni, da tudi če napadalec uspe pridobiti P, s tem ne more pridobiti tudi m_A (ali m_B).

V nadaljevanju bo predstavljena še varnostna analiza protokola WPA3 na podlagi ranljivosti WPA2. Preverili bomo, kako se WPA3 spopade s težavami protokola WPA2 oz. katere težave uspešno odpravi in katere ne. V Tabeli 1 so povzeti napadi na WPA2 in podani odgovori ali je težava pri WPA3 odpravljana. V naslednjih podrazdelkih bomo za napade, ki so bili predstavljeni v razdelku 2.2 naredili varnostno analizo in dokazali uspešnost rešitve/ne rešitve problema pri WPA3.

3.1.1 Deauthentication napad:

Trditev 1. *Deauthentication napad pri WPA3 ni mogoč.*

Proof: Poglejmo najprej situacijo ko napadalec pošlje dostopni točki *deauthentication* paket v imenu uporabnika. Ker napadalec nima dostopa do šifrirnega

*Z malimi črkami so označena števila, z velikimi črkami točke na eliptični krivulji. $-m$ predstavlja inverz števila m v grupi G.

†H je zgoščevalna finkcija.

Napad	Odpravljen?
Deauthentication	Da
Handshake Capture Atack	Da
PMKID Hash Dictionary Attack	Da
Rouge Access Point	Delno
Evil Twin Attack	Ne
Handshake Capture En/Decryption	Da
KRACK Exploit	Da
ARP Spoofing	Delno
SSL Stripping	Ne
DNS Spoofing	Ne

Table 1. Napadi na WPA2 in odgovor ali jih WPA3 uspe odpraviti.

ključa, pošlje dostopni točki neavtenticirano zahtevo za deavtentikacijo. Pri protokolu WPA3 se ob prejemu neavtenticiranega *management* paketa sproži mehanizem *Security Association* (SA), ki od napadalca v tem primeru zahteva, da se v določenem časovnem intervalu odzove na dan izziv (angl. chellenge). Izziv je šifrira in od napadalca zahteva, da tudi odgovor šifrira. Ker napadalec nima dostopa do šifrirnega ključa, se ne more uspešno odzat na izziv, zato dostopna točka njegovo zahtevo za deavtentikacijo zavrže.

V obratni smeri je dokaz enak, saj tudi na strani napravi deluje SA mehanizem. ■

3.1.2 Handshake Capture Dictionary napad:

Trditev 2. *Handshake Capture Dictionary napad pri WPA3 ni mogoč.*

Proof: Za obrambo pred tovrstnimi napadi WPA3 uporablja protokol SAE, ki je bil predstavljen zgoraj. Težava WPA2 pri tovrstnih napadih je, da lahko napadalec po zajetju *Four-way handshake* za poljubno geslo omrežja (PSK) izračuna PMK. Pri WPA3 to ni mogoče, saj se za to uporabila SAE oz. *Dragonfly handshake*, ki zahteva prisotnost dostopne točke. Napadalec namreč tudi ob zajetju *Dragonfly handshake* ne more izračunati PMK, zaradi že prej opisane varnosti protokola SAE in njegove uporabe DLP problema nad eliptičnimi krvuljami. ■

3.1.3 PMKID *Hash Dictionary napad:*

Trditev 3. PMKID *Hash Dictionary napad pri WPA3 ni mogoč.*

Proof: Podobno kot prej, tudi tokrat velja da je WPA3 pred tovrstnimi napadi zaščiten s protokolom SAE in *Dragonfly handshake*om. PMKID hash je namreč med drugim izračunan tudi na podlagi PMK, ki pa ga tokrat napadalec ne more statično izračunat, saj dogovor o njem poteka preko protokola SAE. Ker je protokol SAE varen, je varen tudi PMK in posledično PMKID Hash Dictionary napad pri WPA3 ni mogoč. ■

3.1.4 Rouge Access Point napad: V primeru uporabe lažne (angl. rouge) dostopne točke, glede na cilj napadalca ločimo dva tipa napadov:

1) napad s katerim napadalec dobi geslo omrežja (angl. Key Acquisition) in
2) napad kjer napadalec zlorabi sejo med uporabnikom in dostopno točko (angl. AP Session Hijacking).

Pri prvem je cilj napadalca jasen, pri drugem pa napadalec želi uporabnikovo napravo prepričati, da v trenutni seji komunicira z originalno dostopno točko, medtem ko v resnici podatke do original dostopne točke posreduje preko napadalca. Kot že omenjeno v 2.2, v primerjavi z *Evil twin*, napadalec v tej situaciji nima dostopa do omrežnega gesla, temveč samo spremlja promet med uporabnikom in dostopno točko.

Trditev 4. *Pri WPA3 lahko napadalec z uporabno lažne dostopne točke pridobi geslo omrežja.*

Proof: Napadalec najprej zajame promet želene dostopne točke in shrani njen SSID in MAC naslov, ter način avtentikacije. Nato postavi lažno dostopno točko z istimi nastavitvami kot originalna in z uporabo poljubnega orodja za ojačitev signala, prisili uporabnikovo napravo, da se poveže z lažno dostopno točko. Pri tem seveda napadalec na lažni dostopni točki ne more nastaviti pravilnega gesla, saj ga ne pozna, zato lažna dostopna točka ob povezavi od uporabnika zahteva ponoven vnos omrežnega gesla (npr. naloži lažno spretno stran za vnos gesla). Če uporabnik vnese omrežno geslo je napadalčev cilj dosežen. ■

Trditev 5. *AP Session Hijacking brez omrežnega gesla pri WPA3 ni mogoč.*

Proof: Obstajata dve tehniki za zlorabo seje med uporabnikom in dostopno točko - z uporabo *ARP spoofing*a ali z zlorabo zamenjave brezžičnega kanala [11]. Za obrambo pred prvim, WPA3 uporablja nastavitev izolacije klijenta, več na povezavi [8] pod razdelkom *Client Isolation*. Pred drugim pa uporabnika ščitijo PMF paketi. Paketi v katerih se pošiljajo ukazi za zamenjavo WLAN kanala namreč spadajo pod *management* pakete (konkretno pod *spectrum management*), ki pa so pri WPA3 šifrirani in jih napadalec ne more ponarediti. ■

3.1.5 Evil twin napad:

Trditev 6. *Evil twin napad pri WPA3 je možen.*

Proof:

Kot že pokazano pri napadu 3.1.4, lahko napadalec tudi pri WPA3 pridobi geslo omrežja.

Za izvedbo *Evil twin* napada je postopek napadalca sledeč. Najprej prisluškuje prometu med izbrano dostopno točko in uporabnikovo napravo, da pridobi SSID, MAC in varnostni protokol uporabljen pri dostopni točki. Napadalec nato postavi ponarejeno

dostopno točko z istimi podatki in nastavitvami kot originalna dostopna točka. V tej situaciji ločimo dva primera, in sicer ko je uporabnik v trenutku napada povezan z originalno dostopno točko in situacijo ko to ne drži.

Če je uporabnik v trenutku napada že povezan v omrežje preko original dostopne točke, potem mora napadalec počakati, da uporabnik sam prekine povezavo. Pri WPA2 je lahko na tem mestu napadalec v uporabnikovem imenu pošiljal *da-uthentication* pakete, pri WPA3 pa kot smo že pokazali to ni mogoče.

V primeru, ko uporabnik v trenutku napada ni povezan z originalno dostopno točko oz. ko uporabnik enkrat prekine povezavo, lahko napadalec na lažni dostopni točki oddaja močnejši signal kot original dostopna točka in tako prisili uporabnikovo napravo, da se poveže z lažno dostopno točko. Naj omenim, da tudi če signal lažne dostopne točke ni močnejši od originalne, obstajajo orodja s katerimi napadalec lahko to ponaredi.

Ko je uporabnik enkrat povezan z lažno dostopno točko, protokol WPA3 na originalni dostopni točki na varnost uporabnika nima več vpliva. WPA3 torej še vedno dopušča možnost *Evil twin* napada. ■

3.1.6 KRACK napad:

Trditev 7. *KRACK napad pri WPA3 ni mogoč.*

Proof: Kot smo videli v podrazdelku 2.2.1, celoten KRACK napad temelji na možnosti ponovnega pošiljanja *Msg 3* v *Four-way handshake*u. Pri WPA3 so ravno s tem namenom dodani varnostni popravki, ki onemogočajo ponovno pošiljanje *Msg 3*, kar napadalcu onemogoči ponastavitev števcev, ki je potrebna za uspešen KRACK napad. ■

4 Primerjava WPA3 in WPA2

V prejšnjem razdelku smo videli, da je WPA3 uspel odpraviti nekaj pomanjkljivosti predhodnika WPA2. Dodatno varnost mu omogočajo predvsem *Dragonfly handshake* in uporaba šifriranih *management* paketov (PMF). Na sliki 5 lahko vidimo posodobljen diagram napada na WPA2, ki prikazuje katere poti so še vedno odprte pri protokolu WPA3. Z belo so označena stanja/napadi, ki niso mogoči pri WPA3.

Če povzamemo sliko 5 in ugotovitve iz prejšnjih razdelkov, vidimo da z dodatkom PMF *deauthentication* napad ni več možen. Prav tako v prvi fazi nista možna pasivna napada s slovarji, in sicer zaradi uporabe protokola SAE in *Dragonfly handshake*a. Napadalcu v prvi fazi preostane samo še postavitev lažne dostopne točke in poskus kraje omrežnega gesla s različnimi tehnikami, kot je *phishing*. Tu se je potrebno zavedati, da napadalec lahko od uporabnika izsili omrežno geslo tudi na druge načine, npr. *social engineering*. Najboljša obramba pred tovrstnimi napadi je predvsem izobrazba uporabnikov.

Ob morebitnem ukradenem geslu, se lahko napadalec pridruži omrežju ali pa postavi lažno/podvojeno dostopno točko (*evil twin*). Ker v prvi fazi napadalec pri WPA3 ne more več zlorabiti seje med uporabnikom in napadalcem in prisluškovati prometu, prav tako ne more izvesti KRACK napada s katerim bi lahko promet odšifriral. Tudi v primeru, da bi lahko prišel do stanja v katerem lahko izvede KRACK napad, pa je ta pri WPA3 preprečen z onemogočenim ponovnim pošiljanjem *Msg 3* pri *Four-way handshake*u.

WPA3 zagotavlja tudi t.i. *forward secrecy*, ki zagotavlja, da tudi če napadalec pozna trajne ključe (omrežno geslo) mu to ne omogoča izpeljavo trenutnih ključev oz. ključev trenutne seje (angl. session keys).

Omenili smo, da napadalec pri WPA3 še vedno lahko izvede *Evil twin* napad, ki ostaja največja pomanjkljivost protokola WPA3. Kako preprečiti *Evil twin* napad ostaja stvar raziskave, saj po uporabnikovi priključitvi na lažno dostopno točko, WPA3 ne more več braniti uporabnika pred napadalcem. Glede na želen cilj lahko napadalec, tako kot prikazuje slika 5, izbira med različnimi napadi in od uporabnika v končni fazi pridobi njegove občutljive informacije ali povzroči *DoS* na dostopni točki.

Ravno preprečevanje možnosti izvedbe *Evil twin* napada je tema članka Bartolija [1], ki predstavlja drugo verzijo protokola WPA3 iz leta 2019. Druga verzija protokola prinaša izboljšave v konfiguraciji dostopne točke in naprave uporabnika ter zahtevo po uporabi certifikata, ki bi zagotavljal identiteto dostopne točke. Ugotovitev omenjenega članka je, da je tudi v drugi verziji protokola mogoče napravo in dostopno točko skonfigurirati tako, da napadalec uspešno lahko izvede *Evil twin* napad.

Če povzamemo, WPA3 je uspel odpraviti kar nekaj pomanjkljivosti predhodnika WPA2, kljub temu pa jih nekaj še ostaja in s tem zahteva nadaljnje raziskave.

5 Zaključek

Ob vse večji prisotnosti naprav, ki uporabljajo brezžična omrežja so prisotne tudi vse večje zahteve po varnosti. Trenutno je v praksi za varnost pri brezžičnih omrežjih še vedno najbolj uporabljan protokol WPA2, bo pa s časom verjetno opravljen prehod na WPA3. V tem poročilu je bila opravljena varnostna analiza prve verzije protokola WPA3, nastale v letu 2018. Videli smo, da je WPA3 uspel odpraviti nekaj problemov WPA2, ne pa vseh. Med ne odpravljenimi najbolj izstopa možnost *Evil twin* napada, zato so v letu 2019 objavili drugi različico protokola WPA3, ki pa še vedno ne odpravi problema v celoti. Zdi se, da bosta zato WPA3 in WPA2 še nekaj časa hkrati v uporabi in da razvijalce protokola WPA3 čaka še nekaj dela.

Poleg neopravljenih pomanjkljivosti, prehod na WPA3 zavirajo tudi potrebe po novejši strojni opremi. Pred-

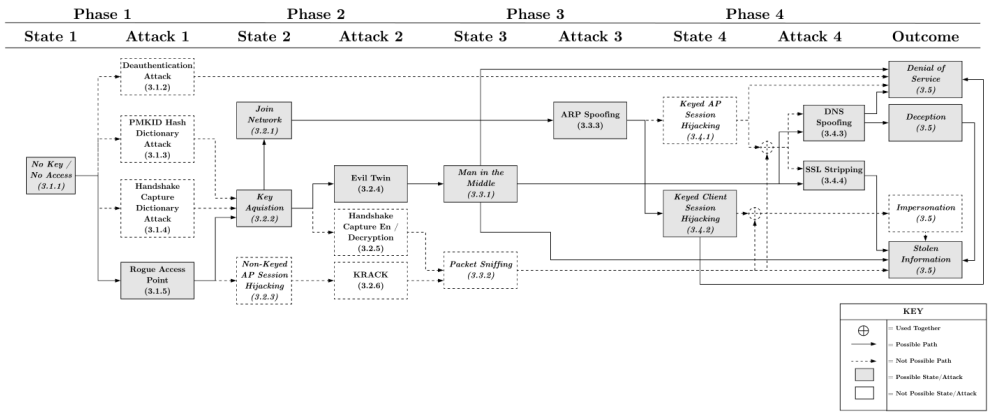

Figure 5. Odziv protokola WPA3 na napad na WPA2. [3]

vsem so to odraža pri *Protected management frame*ih, ki za delovanje potrebujejo novejše čipe, ki omogočajo njihovo delovanje in s tem delovanje WPA3. Prehod bo v praksi zahteval tudi posodobljeno strojno opremo na napravah uporabnikov, ki so zelo raznolike, zato bo potreben čas preden bodo vse posedovale ustrezne tehnologije in čipe.

Zanimivo vprašanje je tudi, ali bo prehod na WPA3 omogočal podobno pomanjkljivost, kot se pojavi pri magnetnih trakih na bančnih karticah. Te namreč z ohranjanjem starejših tehnologij še vedno omogočajo napadalcu zlorabo starejših ranljivosti. Pri dostopnih točkah, ki uporabljajo WPA3, bi to pomenilo še vedno dopuščanje uporabe protokola WPA2 z namenom ohranjanja delovanja starejših naprav. V tem primeru bi bilo s tem napadalcu potencialno omogočeno, da prisili napravo v uporabo WPA2 in nato izkoristi vse njegove pomanjkljivosti.

Sam predvidevam, da celoten prehod na WPA3 ne bo opravljen preden ta ne prepreči vseh pomanjkljivosti predhodnika, takrat pa bo verjetno tudi strojna oprema primerna za uporabo zgolj WPA3.

REFERENCES

[1] Bartoli, Alberto: *Understanding server authentication in WPA3 enterprise*. Applied Sciences, 10(21):7879, 2020.

[2] Ferreira, Rui AC: *A probability problem arising from the security of the temporal key hash of WPA*. Wireless personal communications, 70(4):1235–1241, 2013.

[3] Kohlios, Christopher P and Thaier Hayajneh: *A comprehensive attack flow model and security analysis for Wi-Fi and WPA3*. Electronics, 7(11):284, 2018.

[4] Stubblefield, Adam, John Ioannidis, and Aviel D Rubin: *A key recovery attack on the 802.11 b wired equivalent privacy protocol (WEP)*. ACM transactions on information and system security (TISSEC), 7(2):319–332, 2004.

[5] Tews, Erik, Ralf Philipp Weinmann, and Andrei Pyshkin: *Breaking 104 bit WEP in less than 60 seconds*. In *International Workshop on Information Security Applications*, pages 188–202. Springer, 2007.

[6] Vanhoef, Mathy and Frank Piessens: *Key reinstallation attacks: Forcing nonce reuse in WPA2*. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1313–1328, 2017.

[7] Vanhoef, Mathy and Eyal Ronen: *Dragonblood: Analyzing the dragonfly handshake of WPA3 and EAP-pwd*. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 517–533. IEEE, 2020.

[8] WatchGuard: *Manage security settings*. https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Wi-Fi-Cloud/manage_wirelessmanager/configuration/wifi_access/security_settings.html. Dostopano: 3.7.2021.

[9] Wikipedia contributors: *Forward secrecy — Wikipedia, the free encyclopedia*. https://en.wikipedia.org/w/index.php?title=Forward_secrecy&oldid=1031916403, 2021. [Online; Dostopano 8.7.2021].

[10] Wikipedia contributors: *KRACK — Wikipedia, the free encyclopedia*. https://en.wikipedia.org/w/index.php?title=KRACK&oldid=1022978946, 2021. [Online; Dostopano 8.7.2021].

[11] Wikipedia contributors: *List of WLAN channels — Wikipedia, the free encyclopedia*. https://en.wikipedia.org/w/index.php?title=List_of_WLAN_channels&oldid=1030396058, 2021. [Online; Dostopano 8.7.2021].

[12] Wikipedia contributors: *Wi-fi protected access — Wikipedia, the free encyclopedia*. https://en.wikipedia.org/w/index.php?title=Wi-Fi_Protected_Access&oldid=1031381932, 2021. [Online; Dostopano 8.7.2021].

[13] Wikipedia contributors: *Wired equivalent privacy — Wikipedia, the free encyclopedia*. https://en.wikipedia.org/w/index.php?title=Wired_Equivalent_Privacy&oldid=1019596881, 2021. [Online; Dostopano 8.7.2021].