Igor Šikuljak

Konstrukcija unapređenog sigurnosnog protokola za bežičnu mrežnu komunikaciju

U radu je predložen novi sigurnosni protokol za komunikaciju unutar Home Wi-Fi mreža. Za trenutno postojeće protokole (WEP, WPA i WPA2) poznati su razni napadi koji mogu da naruše integritet mreže i samih podataka koji prolaze kroz nju. Najnovija istraživanja u ovoj oblasti su ukazala da za sigurnost mreže postaju odgovorni i sami klijenti, što je neprihvatljivo, jer bi za otklanjanje ovog problema bilo potrebno nekoliko godina. Stoga je najbolje rješenje konstruisanje novog protokola. Nakon izvršene analize WPA2 protokola, napravljen je niz simulacija novih protokola koji su međusobno testirani u pogledu brzine i sigurnosti. U radu je predstavljen model protokola u kome su otklonjene javno poznate sigurnosne rupe postojećih protokola, a dodatno se oslanja i na kompleksne matematičke probleme koji ne mogu biti rješavani u razumnom vremenskom intervalu u bližoj budućnosti.

Uvod

Predmet ovog rada je unapređenje postojećih sigurnosnih protokola za bezičnu mrežnu komunikaciju, tj. unapređenje sigurnosti komunikacije na Wi-Fi mrežama. Potreban nivo sigurnosti u bežičnim mrežama obezbjeđuju sigurnosni protokoli. Trenutno se za te svrhe u Personal rješenjima Wi-Fi mreža koriste protokoli WEP, WPA i WPA2. Kako su ovi protokoli, tehnološki gledano, nastali prije mnogo godina, oni danas ne mogu da sigurnost mreže održe na prihvatljivom nivou, te potencijalni napadač može pasivnim metodama doći do pristupnog ključa, a tako i ostvariti pristup svim trenutnim, budućim, pa čak i prethodnim aktivnostima klijenata u online svijetu. Napadač može imati i aktivni karakter, kada sadržaje koji prolaze kroz mrežu mijenja sa ciljem ostvarivanja pristupa različitim online servisima koje pojedinac koristi (društvene mreže, finansijski i mail servisi, itd.) i tako nanijeti ozbiljnu štetu na ličnom planu klijentima mreže.

Prvi sigurnosni protokol namjenjen za Wi-Fi je nastao 1997. godine i poznat je pod nazivom WEP. Danas je za „otkrivanje" šifre za pomenuti protokol dovoljan jedan minut praćenja i analiziranja saobraćaja na mreži uz optimalne uslove (Tews *et al*. 2007). Nakon što su Fluhrer *et al*. (2001) pokazali ranjivost RC4 kontinualnog šifrovanja koje koristi i WEP protokol, 2003. i 2004. godine pojavljuju se WPA i WPA2 sigurnosni protokoli. WPA protokol koristi TKIP enkripciju za koju je dokazano da je ranjiva (Vanhoef i Piessens 2013). WPA2 protokol koristi CCMP enkripcijski protokol baziran na AES enkripciji i isti se još uvijek smatra sigurnim jer ne postoje napadi koji su značajnije efikasniji od nasilnog pogađanja ključa. Problem kod WPA2 sigurnosnog protokola je u tome što se koristi enkripcija sa simetričnim ključem, a kako klijent i AP (Access Point, najčešće ruter) moraju međusobno dokazati da posjeduju identičnu šifru i na osnovu nje generisati ključ koji će biti korišćen u toku sesije, tako kroz nebezbjedni „etar" prolaze podaci koji mogu biti iskorišteni za pribavljanje pristupnog ključa. Taj dio komunikacije se naziva 4-Way Handshake i ranjiv je za različite vrste napada – PBKDF-2 bazirani napadi (Bouvette 2004), Rainbow tables (www.renderlab.net),

Igor Šikuljak (1998), RS/BiH, Vlasenica, Vuka Karadžića E/a br. 21, učenik 4. razreda gimnazije u SŠC „Milorad Vlačić" u Vlasenici

MENTOR: Dragan Toroman, Istraživačka stanica Petnica

predvidljivi GTK ključevi (Vanhoef i Piessens 2016). Najnovija sigurnosna rupa pronađena u WPA2 protokolu je pokazala potpunu ranjivost protokola kada se na njega vrše napadi koji primoravaju klijente da koriste više puta istu Nonce vrijednost (Vanhoef i Piessens 2017). Iako je ovaj propust moguće zakrpiti, problem stoji u tome što se zakrpa mora isporučiti svakom klijentu i AP-u, a to je proces koji može trajati godinama i postoji opasnost da nikada neće biti u potpunosti završen.

Cilj ovog rada je konstruisanje novog, sigurnijeg protokola za bežičnu mrežnu komunikaciju. Na osnovu analize nedostataka u trenutno postojećim sigurnosnim protokolima i zaključaka dobijenih u tom procesu, razvijane su simulacije različitih unapređenih sigurnosnih protokola koji su zatim poređeni u pogledu brzine i sigurnosti. Kao osnova za simulacije i referentni model uzet je WPA2 protokol, a zatim su simulirani osmišljeni sigurniji modeli. Dat je osvrt i na moguće izmjene u enkripciji koja se upotrebljava za redovnu komunikaciju na mreži. Rad je inicijalno bio orjentisan prvenstveno prema Home (Personal) rješenjima IEEE802.11 standarda, ali se ispostavilo da se rješenje iz ovog rada može primjeniti i na Enterprise klasu.

Metod

Kao što je već navedeno, protokol se može podijeliti u autentifikacijski (4-Way Handshake) i enkripcijski (AES-CCMP) dio. Enkripcijski dio ne predstavlja problem jer još uvijek nisu poznati praktični napadi, ali svakako treba razmišljati i o enkripcijskom unapređenju. Izvor svih do sada poznatih sigurnosnih problema jeste u autentifikacijskom dijelu komunikacije između klijenta i AP rutera. Na osnovu do sada poznatih ranjivih tački u autentifikacijskom dijelu komunikacije pristupljeno je konstruisanju novih metoda autentifikacije, a zatim i kreiranju simulacija mreža koje koriste takve metode sa ciljem vršenja mjerenja i testiranja istih.

Ispitivanje je vršeno na simulacijama jer su one omogućile da se izbjegne rad na donjim slojevima OSI modela – fizički, link i mrežni sloj. Ovakav pristup ne utiče na reprezentativnost podataka dobijenih u mjerenjima. Simulacije su implementirane pomoću programskog jezika Python 3. Razlog za odabir ovog programskog jezika jeste jednostavniji rad sa mrežnim soketima. Mreža se simulira po sistemu međuprocesne komunikacije između dva programa pomoću soketa, gdje je AP program sa eksplicitno određenim portom na host mašini, a klijenti su programi koji za sebe vežu neki od slobodnih portova. Podaci između AP-a i klijenata se prenose pomoću TCP protokola. Mjerenja su vršena na Raspberry Pi 3 Model B Ver. 1.2 mašini sa Broadcomm BCM2837 čipom radnog kloka 1.20 GHz i 1 GB LPDDR2 radne memorije na 900 MHz sa instaliranim Raspbian Stretch 32-bit operativnim sistemom. Mjerenja su vršena na ovakvom hardveru jer je on mnogo sličniji onome koji se nalazi u današnjim ruterima nego što su to PC računari. U toku vršenja mjerenja težilo se ka uspostavljanju što je moguće boljih uslova, takvih da ne dolazi do međusobne interferencije između ovih i drugih nerelevantih procesa na sistemu.

Iz simulacija je izbačen rad sa GTK ključevima jer je poznato da ti ključevi mogu izazvati sigurnosne prijetnje, a i njihova praktična korist nije mnogo značajna a ni česta. Rješenje za slučajeve kada je ipak potrebna multicast i broadcast komunikacija bi bilo u konstruisanju nekog podprotokola ili posebnog protokola. U ovom radu se nećemo dalje baviti ovim pitanjem.

Započeto je sa implementacijom simulacije WPA2 protokola. Rezultati dobijeni u mjerenjima kod ove simulacije su korišćeni kao referentni rezultati za kasnije implementacije novih protokola. Podaci koji se prenose između AP-a i klijenata u simulacijama su u potpunosti imitirani onako kakvi su u stvarnom protokolu, samo je korišten drugi protokol za prenos tih podataka (TCP). Na taj način druga poruka u 4-Way handshake-u u stvarnom protokolu izgleda ovako (prikazano u heksadecimalnom obliku):

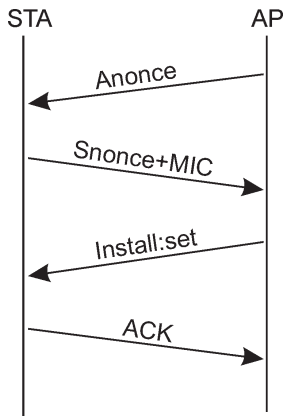
```
0000:  c4 6e 1f f5 ac d0 00 25 22 42 62 66 88 8e 01 03
0010:  00 75 02 01 0a 00 00 00 00 00 00 00 00 00 01 bb
0020:  e8 3f 84 b0 18 9a da 91 1d c6 c3 81 8c ad 11 7e
0030:  3e cf 9d 4c 23 ff 98 14 4b af ab fb 9f 66 02 00
0040:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e3
0060:  a8 e9 d7 59 9d ba 55 e9 2f 29 e2 e5 86 5b b9 00
0070:  16 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04 01
0080:  00 00 0f ac 02 00 00
```

Ista poruka u simulaciji bi mogla imati sledeći izgled:

```
0000:  00 25 22 42 62 66 00 25 22 42 62 66 08 00 45 00
0010:  00 58 19 55 40 00 80 06 00 00 7f 00 00 01 7f 00
0020:  00 01 c0 16 15 b3 3e 1c 34 4f 00 e4 84 02 50 18
0030:  fa f0 ce c0 00 00 bb e8 3f 84 b0 18 9a da 91 1d
0040:  c6 c3 81 8c ad 11 7e 3e cf 9d 4c 23 ff 98 14 4b
0050:  af ab fb 9f 66 02 e3 a8 e9 d7 59 9d ba 55 e9 2f
0060:  29 e2 e5 86 5b b9
```

Legenda: *c4* – podaci vezani za EAPOL i TCP protokol, **bb** – SNonce, e3 – WPA key MIC

Server (AP) prolazi kroz beskonačnu petlju u kojoj se ispituje da li postoji zahtjev za autentifikaciju, ako postoji obavlja se 4-Way Handshake, a ako ne onda se provjerava da li neki klijent zahtijeva određene podatke i jedan paket se isporučuje klijentu (ne mora biti potpun podatak). Slijedi ponovna provjera koja je već opisana. Kao što se i već vidi iz prethodnog opisa, obavljanje 4-Way Handshake-a ima najveći prioritet i ne može biti prekinuto. Nakon toga, podaci se isporučuju klijentima ravnopravno, tako što ukoliko više klijenata potražuje podatke, isporučuje im se po jedan paket i zatim se nastavlja sa drugim klijentima i ponovo od početka sve dok se ne isporuče sve potraživane informacije. Ovaj proces biva prekinut u slučaju novog autentifikacijskog zahtjeva.



Slika 1. WPA2. Oznake: AP – server (access point), STA – klijent (station)

Figure 1. WPA2 (AP – Access Point, STA – station)

Imajući u vidu već navedene izmjene, simulirani handshake, odnosno komunikacija između servera i klijenta za vrijeme autentifikacije šematski izgleda kao što je prikazano na slici 1.

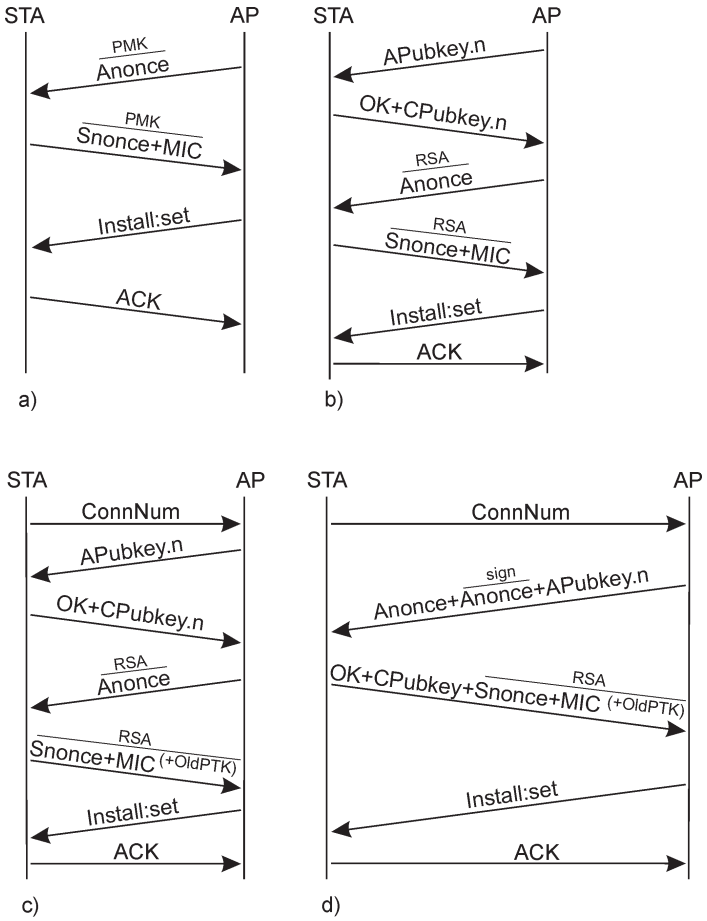
Šifrovanje podataka je standardom jasno određeno i u simulaciji ispoštovano. U kasnijim simulacijama će biti korišćene i druge poznate enkripcije. Kada budu korišćene dvije enkripcije, sve se obavlja po standardu, jedino je ovdje određen redoslijed šifrovanja.

Simulacije novih protokola

Autentifikacija

U prvoj simulaciji je urađeno enkriptovanje prve dvije poruke sa PMK ključem – Anonce i Snonce+MIC. Za enkriptovanje ovih poruka je korišćena AES-CCMP enkripcija, ona se koristi i za enkripciju standardne komunikacije kod WPA2 protokola, tako da je za implementiranje ovoga protokola potrebna samo mala izmjena postojećeg koda. Preostale dvije poruke nije potrebno enkriptovati jer ne prenose osjetljive podatke. U WPA2 protokolu su se u tim porukama osim install:set i ACK prenosili i podaci vezani multicast komunikaciju (GTK ključ i njegov MIC), ali, kao što je već ranije navedeno, ovakva komunikacija bi bila izbačena iz novih protokola jer predstavlja sigurnosni rizik. Ovakav protokol bi unaprijedio sigurnost mreže trenutno, jer bi onemogućio sve postojeće koncepte napada protiv mreže, jedini napad koji bi ostao jeste MITM, a on je napad na komunikaciju a ne direktno na mrežu. Problem je u tome što ovaj protokol unosi nove slabosti, a to je korišćenje PMK ključa za enkriptovanje prve dvije poruke. To se suprostavlja osnovnom principu koji su na umu imali kreatori WPA2 protokola – PMK se ne smije koristiti u osjetljivoj 4-Way Handshake komunikaciji. Protiv ovog bi mogao nastati statistički napad koji bi se oslanjao na to da se kroz enkriptovane podatke prenosi MIC ili slično. Šematski prikaz ovog protokola se može vidjeti na slici 2a.

U drugoj simulaciji se uvodi rad sa enkripcijom koja koristi asimetrične ključeve. Prepustiti kompletnu komunikaciju samo RSA enkripciji nije dobar potez, jer se asimetrične enkripcije oslanjaju na matematičke probleme koji su ipak rješivi uz uportebu veoma velike računarske



Slika 2.
Apstrakcija osmišljenih protokola:
a) WPA2++
b) WPA2++RSA
c) WPA2++RSA&PTKchaining
d) WPA3.0

Figure 2.
Abstraction of the designed protocols:
a) WPA2++
b) WPA2++RSA
c) WPA2++RSA&PTKchaining
d) WPA3.0

snage. Ipak, prednost korišćenja RSA enkripcije jeste u tome što javni ključevi mogu biti razmjenjeni i kroz nebezbjedni „etar". Osjetljivi podaci koji se prenose u prvoj i drugoj autentifikacijskoj poruci sada su zaštićeni RSA 2048-bitnom enkripcijom. To zahtijeva prethodnu razmjenu javnih ključeva potrebnih za RSA enkripciju, tako da sada prije poruka karakterističnih za 4-Way Handshake imamo jos dvije poruke. U prvoj poruci se prenosi javni ključ od AP-a, koji klijent po prijemu potvrđuje na osnovu njegovog otiska (fingerprint) koji zajedno sa PSK unosi korisnik mreže. Ovo je ujedno i zaštita koja onemogućava MITM tip napada na mrežu. U drugoj poruci se nalazi potvrda ispravnosti prenosa i klijentov javni ključ. Šematski prikaz ovog protokola se može vidjeti na slici 2b.

Treća simulacija se bavi unapređenjem rješenja predstavljenog u drugoj simulaciji, pod pretpostavkom da RSA enkripcija ne predstavlja veću prepreku za napadača. Ideja je u međusobnom povezivanju autentifikacijskih komunikacija za svakog klijenta posebno, tako da svaki sledeći PTK ključ bude zaštićen neophodnim poznavanjem PTK ključa prethodne sesije. To se postiže tako što se prethodni PTK ključ koristi kao dodatni argument u računanju MIC-a a i novog PTK ključa. Na ovaj način su onemogućeni svi postojeći napadi na 4-Way Handshake osim u inicijalnom jer svaki sledeći „zavisi" od prethodnog. Za potrebe kontrole ovog procesa bilo je potrebno uvesti jos jednu poruku u autentifikacijsku komunikaciju u odnosu na prethodnu simulaciju, tu poruku šalje klijent AP-u i u njoj je sadržana informacija koja govori da li je to ponovna autentifikacja ili je prva. Šematski prikaz ovog protokola se može vidjeti na slici 2c.

Četvrta simulacija optimizuje rad rješenja predstavljnog u prethodnoj simulaciji. U prvoj poruci se i dalje prenosi poruka o rednom broju autentifikacije. Sledeća poruka prenosi neenkriptovan ANonce, javni ključ AP-a i ANonce potpisan privatnim ključem – na ovaj način se poruka štiti od izmjena. Ako se vrši ponovna autentifikacija klijent ne mora da provjerava otisak javnog ključa. Treća poruka sadrži potvrdu ispravnosti prethodnog dijela autentifikacije, STA javni ključ i SNonce+MIC zaštićene RSA enkripcijom. Ponovo, u zavisnosti od prve poruke, MIC i PTK mogu biti sačinjeni i od starog PTK ključa. Posljednje dvije poruke su Install:set i ACK. Šematski prikaz ovog protokola se može vidjeti na slici 2c.

Enkripcija

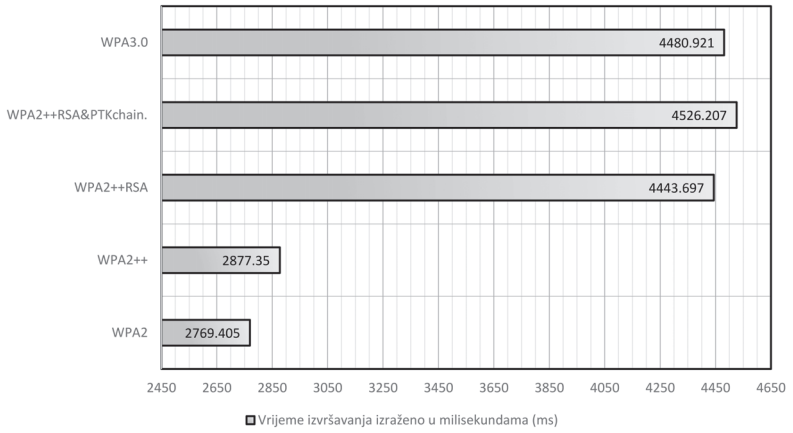
Razmatrana su tri oblika enkriptovanja podataka međusobno poređena kroz tri simulacije. Prvo je simulirana trenutno korišćena enkripcija u WPA2 protokolu – AES-CCMP. Zatim je simuliran prenos podataka zaštićenih RSA enkripcijom. U trećoj simulaciji se podaci enkriptuju prvo sa AES-CCMP, a zatim i sa RSA enkripcijom.

Rezultati i diskusija

Izmjereno je vrijeme potrebno za izvršavanje autentifikacionog dijela komunikacije za svaku od ranije predstavljenih simulacija. Na slici 3 su predstavljeni prosjeci trajanja autentifikacije na po 512 mjerenja.

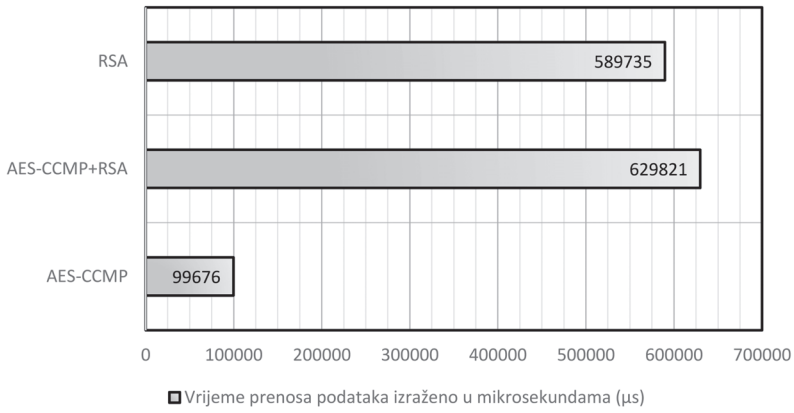
Rješenje koje je predstavljeno pod nazivom WPA3.0 jeste najsigurnije rješenje, ali se na osnovu rezultata vidi da je njegovo izvršavanje duže za 62% u odnosu na WPA2 protokol. Poznato je da reautentifikacija u WPA2 protokolu izaziva probleme određenim servisima koji zahtjevaju konstantnu konekciju na internet. Prema dobijenim rezultatima, osnovano je očekivati da će slični problemi biti učestaliji kod predstavljenog WPA3.0 protokola. Prva autentifikacija i dalje ima upitnu sigurnost jer je poznat metod kojim bi se ovaj protokol mogao svesti na nivo WPA2 protokola, međutim, nezamislivo je da će u bližoj budućnosti biti moguće to uraditi u nekom prihvatljivom vremenskom intervalu.

Iako to nije bio cilj ovog rada, ispostavilo se da prikazano sigurnosno rješenje ima većinu odlika koje su zastupljene i u Enterprise klasi. Ovaj protokol posjeduje dva nedostatka u odnosu na postojeće enterprise sisteme, koji se mogu riješiti. Prvi je zaštita od novih korisnika koji su „nekako" došli do šifre i fingerprint-a, što se može postići korišćenjem MAC filtriranja. U enterprise mrežama odgovarajući proces ovome je dodavanje novog korisnika (username + password) u RADIUS bazu. Drugi je sprječavanje slučaja da treća osoba, u slučaju poznavanja dva podatka potrebna za ostvarivanje konekcije na mrežu, pokuša da se predstavi kao validan klijent mreže (MAC Spoofing) i u prvoj poruci WPA3.0 handshake-a zatraži inicijalnu autentifikaciju. Odbrana od ovoga je u maloj izmjeni prve i četvrte poruke WPA3.0 autentifikacije. Da bi klijent zatražio ponovnu inicijalnu komunikaciju, u pr-



Slika 3. Vrijeme izvršavanja autentifikacija u simulacijama

Figure 3. Execution time for authentications in the simulations (in ms)



Slika 4. Vrijeme potrebno za prenos jednog paketa podataka u simulacijama

Figure 4. Time needed to transmit one data set in the simulations (in ms)

voj poruci mora poslati kod koji mu je u ranijoj inicijalnoj autentifikaciji dodijelio AP u trećoj poruci, gdje je on bio zaštićen RSA enkripcijom.

Takođe, izmjerena su i vremena potrebna za prenos slučajno generisanih 128 bajtova podataka kroz tri modela enkripcije od AP-a do klijenta. Na slici 4 su predstavljeni prosjeci trajanja prenosa podataka na po 256 mjerenja.

Iz dobijenih rezultata se vidi da su metodi enkripcije koja uključuju RSA enkripciju sporiji oko 6 puta u odnosu na trenutno korišćenu AES--CCMP enkripciju. Kako su brzine 6 puta sporije od današnjih one ne bi bile prihvatljive. AES--CCMP enkripcija se jos uvijek smatra sigurnom jer ne postoje napadi koji omogućavaju „probijanje" enkripcije znatno brže od bruteforce napada. Zbog toga je sigurno nastaviti koristiti ovu enkripciju za prenos podataka.

Budući rad

U daljem radu na ovoj temi potrebno je implementirati ovdje predstavljeni WPA3.0 protokol za upotrebu u realnim uslovima. Tako se mogu dobiti rezultati koji mogu pomoći u dodatnom unapređenju protokola ili čak dovesti do konstruisanja boljeg protokola. Moguće je izvršiti implementaciju mijenjanjem postojećih open source user space daemon-a: hostapd (za ulogu AP-a) i wpa_supplicant (klijent) (Malinen 2013).

Zaključak

Rješenje predstavljeno u ovom radu u slučaju korišćenja u realnim uslovima pružilo bi dovoljan nivo bezbjednosti, kako za Home WiFi rješenja, tako i za Enterprise klasu uz prilagođavanje. Ipak, činjenica nepostojanja elegantnog, sigurnog i vremenski efikasnog rješenja ukazuje na to da je potreban dalji rad na ovom polju. U tijelima koja su zadužena za rad na ovim protokolima – IEEE i Wi-Fi Alliance – vlada inertnost. Nakon javnog objavljivanja KRACK napada, njihov stav je bio da je samo potrebno zakrpiti otkrivene rupe i korisnici Wi-Fi tehnologije mogu biti spokojni, potpuno zanemarujući činjenicu da će taj proces trajati godinama, možda decenijama. Istorijski gledano, ovo je bio sasvim očekivan potez, jer su iste organizacije počele da rade na zamjeni WEP protokola novim protokolom tek kada se „provaljivanje" WEP-a svelo na jedan čas rada na prosječnom računaru. Na pojavljivanje novog protokola se čekalo nesto više od jedne godine, i u tom periodu korisnici su bili potpuno nezaštićeni. Ispravan pristup bi bio da su počeli raditi na novom protokolu pri prvoj nagovijesti da je moguć enkripcijski napad brži od klasičnog bruteforce napada. Sledeći problem jeste u tome što su sva tri trenutno postojeća protokola konstruisana sa određenim nivoom kompatibilnosti unazad. Stav autora je da za kompatibilnost unazad nema mjesta u sigurnosnom sektoru IT-a (primjer – naslijeđeni propusti u WPA (TKIP) protokolu iz WEP protokola). Ipak, ovo zahtijeva detaljnu diskusiju na višem nivou. Naknadno je Wi-Fi alijensa objavila da će u toku 2018. godine dizajnirati novi, WPA3 standard. Vjerovatno da se taj protokol neće početi masovnije koristiti u skorije vrijeme, jer veliki dio uređaja (prvenstveno ruteri i mobilni telefoni) nikada neće dobiti zakrpe koje bi im omogućile podršku za novi protokol.

Literatura

Bouvette T. 2004. Aircrack-ng. Dostupno na: http://www.aircrack-ng.org

Fluhrer S., Mantin I., Shamir A. 2001. Weaknesses in the Key Scheduling Algorithm of RC4. U *Selected Areas in Cryptography* (ur. S. Vaudenay i A. M. Youssefs). Springer, str. 1-24.

Malinen J. 2013. Hostapd and wpa_supplicant. Dostupno na: http://w1.fi/

Tews E., Weinmann R. P., Pyshkin A. 2007. Breaking 104 bit WEP in less than 60 seconds. Dostupno na: https://eprint.iacr.org/2007/120.pdf

Vanhoef M., Piessens F. 2013. Practical Verification of WPA-TKIP Vulnerabilities. U *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, str. 427-436.

Vanhoef M., Piessens F. 2016. Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys. U *25th USENIX Security Symposium*. Austin: USENIX, str. 673-687.

Vanhoef M., Piessens F. 2017. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. U *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. Dalas: ACM, str. 1313-1328.

www.renderlab.net. Church of Wifi WPA-PSK Lookup Tables. Dostupno na https://www.renderlab.net/projects/WPA-tables/

Igor Šikuljak

Construction of an Enhanced Security Protocol for Wireless Network Communication

In this paper a new security protocol for communication within the Home Wi-Fi network is proposed. For the currently existing protocols (WEP, WPA, and WPA2), various attacks are known that can undermine the integrity of the network and the data flowing through it. The latest research in this area has indicated that each client is also responsible for the safety of the network as a whole. This is unacceptable, as it would take several years or even longer to eliminate this problem, so the best solution is to construct a new protocol. After analyzing the WPA2 protocol, a series of simulations of new protocols were tested in terms of speed and security. The paper presents a protocol model in which the publicly known security holes of existing protocols are removed. Additionally, it relies on complex mathematical problems that cannot be resolved within a reasonable time interval in the near future.