

# Analiza sigurnosti SSL saobraćaja u bežičnim računarskim mrežama

Marko Šarac, Mladen Veinović, Saša Adamović, Dalibor Radovanović, Aleksandar Jevremović

Fakultet za informatiku i računarstvo

Univerzitet Singidunum

Beograd, Srbija

[msarac@singidunum.ac.rs](mailto:msarac@singidunum.ac.rs), [mveinovic@singidunum.ac.rs](mailto:mveinovic@singidunum.ac.rs), [sadamovic@singidunum.ac.rs](mailto:sadamovic@singidunum.ac.rs),  
[dradovanovic@singidunum.ac.rs](mailto:dradovanovic@singidunum.ac.rs), [ajevremovic@singidunum.ac.rs](mailto:ajevremovic@singidunum.ac.rs)

**Sadržaj** — U radu su predstavljeni i analizirani aktuelni problemi u primeni SSL protokola u računarskim mrežama. Prikazani su rezultati istraživanja o napadima na računarske sisteme. Analizirane su savremene metode zaštite i ukazano je na njihove nedostatke. Prvi deo rada iznosi aktuelne probleme zaštite računarskih mreža i predstavlja aktuelna rešenja. Drugi deo rada fokusira se na problem koji postoji u trenutno zastupljenim metodama zaštite savremenih računarskih mreža. Problem je analiziran kroz dve metode napada. Na osnovu istraživanja obavljenog u toku pisanja rada organizovana su dva seminara o podizanju svesti o problemima savremenih računarskih mreža. Na osnovu diskusija i anketa urađenih za vreme seminara došlo se do novih saznanja koja su analizirana i predstavljena kroz rad. Cilj ovog rada je da ukaže na aktuelnost problema i da doprinos u rešavanju sigurnosnih nedostataka.

**Ključne riječi:** Bežične računarske mreže, SSL, HTTP, HTTPS

## I. UVOD

Sa pojavljivanjem prvog Wi-Fi standarda teško je bilo pretpostaviti u kojoj meri i kojom brzinom će se razvijati bežične mreže. Ubrzo po pojavljivanju otkrivena je mana u sistemu zaštite bežičnih mreža. Greška se nalazila u WEP kriptografskom metodi što je detaljno opisano i analizirano u radu [6]. Zbog naglog rasta broja kućnih i poslovnih korisnika bežičnih računarskih mreža, kao i zbog lakoće instalacije i korišćenja, problem je postajao sve izraženiji. Usled toga, predloženo je novo rešenje u vidu WPA2 bezbednosnog standarda, koji koristi AES šifarski mehanizam umesto ranjivog RC4 TKIP sistema. Predloženo novo rešenje nije kompatibilno sa prethodnim. Na taj način, vlasnicima starih sistema bila je uskraćena bezbednost ukoliko se nisu odlučivali za nabavku novih uređaja koji su podržavali WPA2 standard. U radu se razmatraju problemi koje „legitimni” korisnici mogu izazvati u bežičnim računarskim mrežama baziranim na najnovijem WPA2 sigurnosnom standardu.

Razmatra se više međusobno povezanih problema:

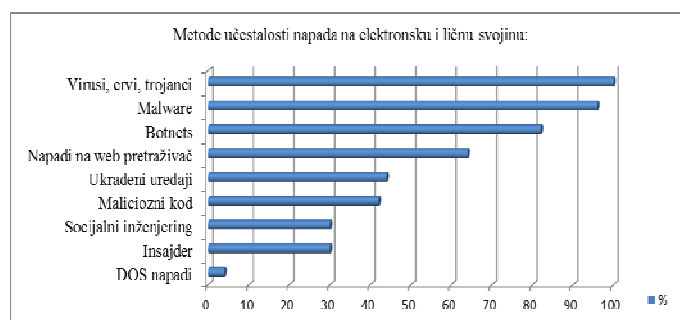
- Aktuelni napadi na elektronsku i ličnu svojinu
- Istraživanje zaštite koju nudi SSL, primena i napadi u bežičnim računarskim mrežama
- Nedostaci HTTPS uspostavljanja veze

- Napadi na HTTPS saobraćaj
- Analiza anketa sa održanih savetovanja
- Predlog rešenja za odbranu od napada

U prethodnom periodu organizovana su dva predavanja o problemima u zaštiti bežičnih računarskih mreža. Predavanja su bila na bazi jednodnevnih seminara sa različitim ciljnim grupama. Prvi seminar organizovan je za grupu srednjoškolaca i studenata, dok je drugi seminar organizovan za grupu postdiplomskih studenata, kao i za zaposlene u javnom i privatnom sektoru. Seminari su i rad podržani su od strane Ministarstva za nauku i tehnološki razvoj Republike Srbije u okviru projekta TR32054. Cilj oba seminara bio je edukacija, ukazivanje na probleme, ali i uzorkovanje grupa koje su učestvovala u samom seminaru.

## II. PODACI O NAPADIMA NA ELEKTRONSKU I LIČNU SVOJINU

Dobro je poznato da sve više poslova i delova našeg života zavise od računara i obavljanja zadataka preko računarskih mreža. Zbog toga sve više istraživača obavlja analize i istraživanja vezana za bezbednost računarskih sistema i poslovnih transakcija. Kroz naredne primere biće prikazane globalne statistike najčešćih napada na računarske sisteme, zastupljenost različitih napada, koliko finansijsku štetu organizaciji nanose, kao i koliko je dana prosečno potrebno organizaciji da postane svesna da je napadnuta.



Slika 1. Učestalost napada na elektronsku i ličnu svojinu

Na sl.1 je predstavljena klasifikacija po učestalosti napada. Klasifikacija je predstavljena po istraživanju koje je obavio

Ponemon institut u avgustu 2011. godine[1]. Kao što se iz same ilustracije vidi najveći broj napada se čini posredstvom virusa, crva, trojanaca, malwera, dok su maliciozni kodovi i insajderi rede zastupljeni tip napada. Međutim, upravo ti ređi napadi čine najveću finansijsku štetu organizaciji.

Prema podacima sa sl.2, a po istraživanju Ponemont instituta maliciozni kod identifikovan je kao najveći uzročnik finansijskih troškova u okviru organizacije, dok su virusi, crvi i trojanci koji su identifikovani kao najčešći tip napada odneli svega 8% ukupnih finansijskih troškova organizacije u oblasti zaštite i napada.



Slika 2. Finansijski troškovi zaviso do tipa napada

Organizacija često smatra da uspešno funkcioniše i pravilno radi i sa insajedrom u svojim redovima. Ovakav tip napada je teško otkriti i oduzima najviše vremena. U proseku je potrebno više od 45 dana za identifikaciju insajdera. Maliciozni kod takođe je čest uzrok problema koji je teško identifikovati i najčešće je potrebno preko 40 dana dok organizacija postane svesna da ima problema sa malicioznim kodom. Ovaj tip napada je najveći uzročnik finansijskih gubitaka organizacije.

### III. ISTRAŽIVANJE ZAŠTITE KOJU NUDI SSL, PRIMENA I NAPADI U BEŽIČNIM RAČUNARSKIM MREŽAMA

Sa brzim razvojem mrežnih aplikacija, problem bezbednog prenosa postaje veoma važan. Zbog toga je SSL protokol sve više u širokoj upotrebi u različitim mrežnim servisima. Ovaj protokol sam po sebi nije savršen i u praksi sa njim često postoje problemi. Ovaj deo rada ukazuje na problem koji postoji u procesu SSL uspostavljanja veze. Prva mana kod uspostavljanja veze je što se u početnoj fazi koristi otvorena komunikacija pa postoji mogućnost neovlašćenog praćenja sadržaja. Druga mana je implementacija SSLa u aplikaciju. Zbog razmatranja faktora o radu mrežne veze, obično se koristi prekidač veze zasnovan na HTTP protokolu koji prebacuje saobraćaj na HTTPS.

Na primenu SSL-a značajno utiču i razvoj e-trgovine i rad u „oblaku“. Njegovom primenom garantuje se bezbednost komunikacionog procesa, a koriste se mehanizmi autentifikacije od kraja do kraja, šifrovanje poruka, provera integriteta poruke i drugi mehanizmi zaštite. Najveći svetski proizvođači koriste SSL kako bi štitili svoje klijente. Primera radi, Google štiti sigurnost razmene mailova kao i prijave svojih korisnika preko SSL protokola. Poslednjih par godina

značajan rast beleži i korišćenje sistema rada u „oblaku“. Razmena podataka se u najvećem broju slučajeva obavlja putem SSL protokola. VeriSign, kao najveće autorizaciono telo za izdavanje SSL sertifikata, čak garantuje sigurnu uslugu svim korisnicima nove Microsoft Windows Azure platforme u „oblaku“[2]. Kada se radi u „oblaku“ svi podaci korisnika i sva obrada podataka obavlja se na udaljenoj lokaciji pa je samim tim neophodno da veza funkcioniše savršeno, ali i da ostane bezbedna kako ne bi došlo do kompromitovanja podataka. Bankarski sektor je napadačima najzanimljiviji ali i sektor na koji su korisnici usluga najosetljiviji i gde očekuju najveću bezbednost. Savremeno elektronsko bankarstvo se uglavnom oslanja na SSL protokol kao odgovarajući model zaštite.

Ipak pokazalo se da SSL nije savršen za svaki tip primene. Još 2003. realizovani su napadi na SSL protokol i dokazane su greške u uspostavljanju veze koje su omogućavale napad preuzimanja sesije. U 2009. godini Michael Howard je uspešno realizovao napad korišćenjem alata Webmitm [1] – alat za Linux okruženje koji uspešno dešifruje podatke iz SSL protokola. Iste 2009. godine na internacionalnoj bezbednosnoj konferenciji predstavljeno je rešenje koje prosleđuje saobraćaj sa HTTPS na HTTP saobraćaj koji se dalje mnogo lakše obrađuje i prisluškuje. Kod ovih napada klijenti ne primećuju razliku u uslugama i servisima koje koriste.

Proizvođači Internet pretraživača unapređivali su zaštitu svojih klijenata koja se zasniva na upozorenjima na nevalidne sajtove kao i na lažne sertifikate. Kompanije za antivirusna rešenja razvile su rešenja za zaštitu od ARP prevara, koja se najčešće koriste pri napadima. Međutim, pored svih zaštita i inicijativa proizvođača programa često su nastajali bezbednosni propusti koji se i danas koriste.

Ovaj rad bazira se na analizi bezbednosnih propusta koji se javljaju pri SSL uspostavljanju veze. Analiza je rađena primenom dva metoda. Prvi metod zasniva se na karakteristikama otvorenog teksta u fazi uspostavljanja veze kao nedostatku klijent sertifikacione autentifikacije, preuzimanju sesije preko ARP obmane i DNS poplave u okviru mrežnog segmenta. Napadač podmeće falsifikat serverskog sertifikata i predstavlja se kao proksi ili gateway nakon čega dolazi u mogućnost za napad. Posledica je da napadač može da dešifruje sve podatke prenete putem https-a. Drugi metod zasniva se na korišćenju defekta SSLa i zaobilaznja istog u praktičnoj primeni. Na početku se ARP prevaram napadač predstavlja kao lažni proksi ili gateway. Napadač uspostavlja HTTPS vezu sa pravim serverom i ta komunikacija se dalje obavlja sa pravim sertifikatom, dok se veza za obmanutim klijentom obavlja preko HTTP saobraćaja čiji je saobraćaj lako pratiti i obrađivati. Napadač direktno šalje otvoren tekst klijentu sa HTTP strane dešifrovanjem šifrovanih podataka, tako da on može da pristupi svim komunikacijama podataka.

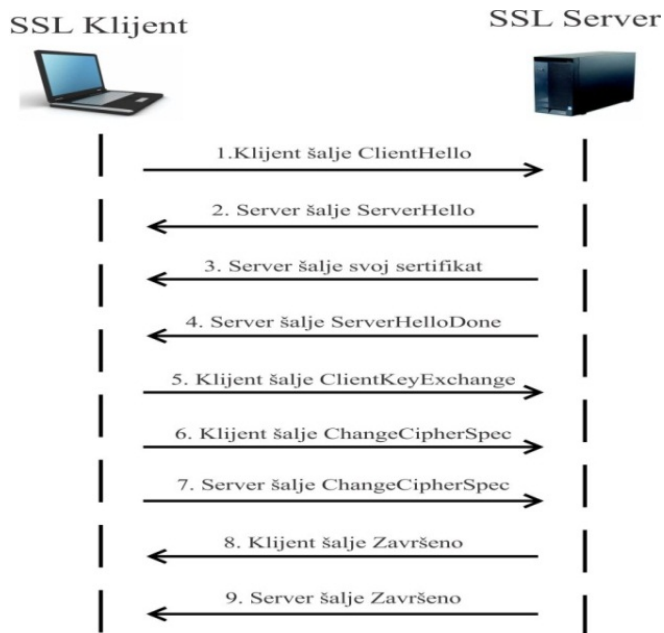
U eksperimentalnoj analizi obrađeno je u odnosu na specifičnosti nekoliko napada po prethodno opisanim scenarijima. Analizirani su verovatnoća uspeha napada i mogućnost klijenta da primeti da je do napada uopšte i došlo. Nakon eksperimenata obavljene su i dva kursa obuke, nakon kojih su rađene analize obučanih klijenata za detekciju napada i predstavljeni su rezultati grupe pre i nakon obuke.

#### IV. NEDOSTACI HTTPS USPOSTAVE VEZE

Secure Sockets Layer (SSL) je protokol za sigurno slanje poruka (komuniciranje) putem Interneta. Omogućava slanje poverljivih podataka (npr. broj kreditne kartice) putem Interneta u šifrovanom i sigurnom obliku. Prva verzija SSL protokola je SSL 3.0. Koristi se za širok spektar aplikacija. Uključena je u Internet standardima IETF. Trenutna, verzija SSL protokola u širokoj upotrebi je TLS (SSL 3.1). Proces SSL uspostave veze je jasno definisana u RFC2246, kao što je prikazano na sl.3. SSL od aplikativnog sloja prima poruku koju treba poslati, rastavlja je u manje delove pogodnije za šifrovanje, dodaje kontrolni broj, šifrjuje, eventualno vrši kompresiju, a zatim te delove šalje. Primalac prima delove, vrši se dekompresija, dešifrovanje, proveru kontrolnih brojeva, sastavljaju se delovi poruke i na kraju se predaju aplikativnom sloju. Na taj način se putem SSL-a ostvaruje zaštićeni kanal kroz nebezbednu mrežu. Ukoliko su klijent i server neaktivni duže vreme ili razgovor sa istim atributima zaštite potraje predugo, atributi se menjaju.

##### A. Osnove uspostavljanja SSL veze

Na primeru klijent-server komunikacije prikazan je proces uspostavljanja SSL veze.



Slika 3. Uspostavljanje SSL veze

1. Klijent šalje ClientHello: Klijent šalje SSL pozdravnu poruku i pokazuje na početak uspostavljanja SSL veze.

ClientHello poruka uključuje veličinu paketa, SSL verziju, slučajni broj koji generiše ključ klijenta, broj sesije, sve kriptografske pakete koji klijentski pretraživač može da podrži, metod kompresije koji može biti usvojen.

2. Server šalje ServerHello: Na primljenu ClientHello poruku poslatu od strane klijenta server odgovara sa porukom ServerHello. Poruka uključuje SSL verziju koju server najviše može da podrži, slučajni broj koji generiše server, broj sesije postavljen od strane servera, metode kompresije koje mogu biti usvojene.
3. Server šalje svoj sertifikat: Server šalje svoj autorizacioni lanac, koji uglavnom uključuje i sertifikat servera kao i viši sertifikat.
4. Server šalje ServerHelloDone: Server pokazuje da je sve autentifikacione informacije poslao klijentu u potpunosti.
5. Klijent šalje ClientKeyExchange: Nakon što klijent prođe proveru sertifikata koji je dobio od servera, klijent će generisati pre-master ključ, i korišćenjem javnog ključa sertifikata servera šifrovati pre-master ključ.
6. Klijent šalje ChangeCipherSpec: Klijent pokazuje da će sledeći mrežni paketi biti šifrovane od strane uspostavljenih ključeva za šifrovanje, a klijent generiše master ključ koji se koristi u komunikaciji kroz pre-master ključ i informacije koje su se razmenile ranije.
7. Klijent šalje Završeno: Klijent pokazuje da završava poruku u fazi uspostave veze.
8. Server šalje ChangeCipherSpec: Server pokazuje da će sledeća poruka biti šifrovana ključem koji je uspostavljen u toku kriptološke sinhronizacije.
9. Server šalje Završeno: Server pokazuje da je završio poruke u fazi potvrde uspostave veze.

Nakon ovih koraka, komunikacija obe strane je šifrovana simetričnim šifarskim sistemom primenom uspostavljenog simetričnog tajnog ključa. Šifrovana komunikacija obezbeđuje sigurnost prenetih podataka između klijenta i servera[3].

##### B. Analiza nedostataka

Sadržaj podataka je otvoren pri SSL uspostavi veze, tako da napadač neovlašćenim pristupom i praćenjem može da dobije paket podataka. Kod SSL-a je moguć napad preuzimanja sesije. Klijent potvrđuje verodostojnost servera u koraku tri koji prenosi serverski sertifikat, ali sertifikat se prenosi u otvorenom tekstu i lako se može presretnuti i neovlašćeno koristiti. Kada napadač presretnete poruku i dobije serverski sertifikat, može ga iskopirati i napraviti sopstveni lažni sertifikat, a zatim popuniti informacije sa podacima servera. Pri tom postavlja sopstveni javni ključ i potpis u sertifikat i dalje šalje falsifikovani sertifikat. Kada korisnici prihvate lažni sertifikat tada napad postaje uspešan. Dakle, postoji nedostatak u koraku tri pri SSL uspostavi veze, sl.4.

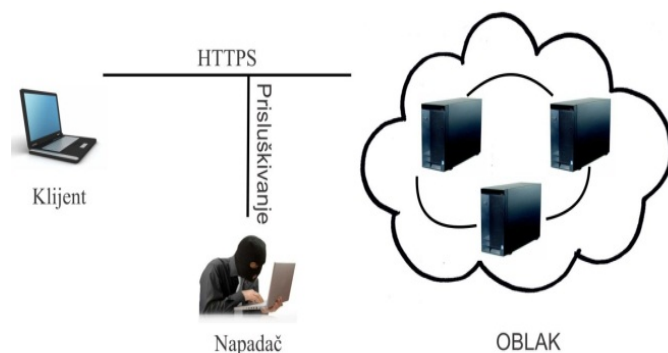
Kao još jedna mana može se iskoristiti i samo poverenje korisnika u SSL i bezbednost sistema. Nakon brojnih analiza došlo se do zaključka da preko 95% korisnika ne obraća pažnju pri ukucavanju Web adrese i ne unosi samostalno HTTPS zahtev. Čak i kada korisnici koriste HTTPS zaštićeni pristup sajtu oni najčešće u svom pretraživaču ne unose adresu sa HTTP ili HTTPS delom, već jednostavno unose adresu u obliku: [www.sajt.com](http://www.sajt.com). Svi Internet pretraživači će prvo pokušati da uspostave HTTP vezu kao pretpostavljeni tip veze. Tek nakon što se uspostavi veza sa serverom, serveri podešeni za sigurnu vezu će poslati uputstvo sa redirekcijom na sigurni sajt u obliku <https://www.sajt.com>. Takođe čest je slučaj i da sam sajt u određenim delovima funkcioniše na osnovnom HTTP nivou bez zaštite (ukoliko se radi o prezentacionim materijalima koji ne zahtevaju interakciju korisnika), da bi tek nakon potrebe za interakcijom korisnika zahtevali sigurnu vezu za potrebu autentifikacije. Ovi slučajevi najčešće su rešeni postavljanjem istaknutih dugmića koji iniciraju sigurnu vezu. Većina saobraćaja funkcioniše preko običnog HTTP saobraćaja iz razloga što HTTPS saobraćaj dodatno opterećuje servere šifrovanjem informacij. Zavisno od slučaja do slučaja usporenja koja korisnik primećuje iznose od 2 do 100 puta. Iz ovog razloga sistemi su automatizovani pa samo bitni podaci koriste HTTPS saobraćaj. Zbog ovakvih i sličnih automatizovanih rešenja koja olakšavaju svakodnevno korišćenje Interneta i njegovih servisa sve manje korisnika obraća pažnju da li je uspostavljena obična HTTP ili sigurna HTTPS veza. Sa strane korisnika sve izgleda isto bez obzira na to da li je veza uspostavljena unosom cele adrese ili samo dela adrese. Sa strane mrežnog saobraćaja stvari ipak funkcionišu drugačije.

## V. NAPAD NA HTTPS SAOBRAĆAJ

### A. Napad prisluškivanjem saobraćaja

Kako se inicijalni prenos podataka odvija u otvorenom tekstu pri SSL uspostavi veze, napadač može da dostavi podatke za ARP prevaru između klijenta i servera. Napadač presreće HTTPS zahtev od klijenta, i povezuje se sa samim serverom. Kada server pošalje sertifikat za autentifikaciju, napadač može da napravi sertifikat koji je sam potpisao, a zatim ga prosledi klijentu. Korisnici imaju tendenciju da izaberu prihvatanje lažnog sertifikata čak i ukoliko ih programski paketi upozoravaju na moguću prevaru. Ovo dodatno olakšava napad, pa napadač lako uspostavlja SSL komunikacioni link. Napad sadrži sledeće korake: lažiranje ARP saobraćaja omogućava umetanje napadača na relaciju server klijent. Tada napadač može da prati saobraćaj, tj. pakete između klijenta i servera. Nakon ARP napada sledi DNS napad i prisluškivanje porta 443 preko koga se uspostavlja SSL saobraćaj. Kada napadač primeti SSL zahtev od strane klijenta, napadač tada prihvata TCP zahtev i inicira SSL vezu sa serverom. Nakon uspešne konekcije na server napadač sprema lažni sertifikat koji sam potpisuje i podmeće klijentu kako bi dalje mogao da dešifruje sav saobraćaj koji prisluškuje. Kada klijent primi lažni sertifikat, može se desiti situacija u kojoj će Internet pretraživač upozoriti da se radi o lažnom sertifikatu ili na mogućnost napada. Nakon prihvatanja

lažnog sertifikata napad se smatra uspešnim jer i klijent i napadač šifruju sadržaj istim sertifikatom i imaju uspostavljenu SSL konekciju tako da se saobraćaj dalje može lako prisluškivati. Saobraćaj se može pratiti i pregledati u realnom vremenu.



Slika 4. Ilustracija prisluškivanja HTTPS saobraćaja

Danas postoji dosta specijalizovanih programa za ovu vrstu napada čija rešenja u sebe uključuju i ARP i DNS napad. Radi se o grafičkim rešenjima koja ne zahtevaju previše poznavanja računarskih mreža i protokola. Ova činjenica omogućava i slabije upućenim pojedincima da postanu napadači, ali omogućava i potencijalno veći broj žrtava. Većina proizvođača Internet pretraživača se protiv ove vrste napada bori primarno detekcijom i sve upadljivijim upozorenjima koja od klijenata zahtevaju veću interakciju, osim do sada uobičajne interakcije od jednog klika.

### B. Napad zaoblaženjem sigurne veze

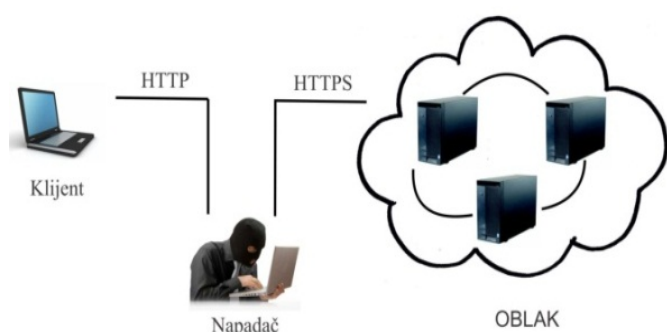
Slično prvom napadu, napadač može da prosleđuje pakete i prati HTTP saobraćaj ARP varanjem između klijenta i servera. Kada napadač primeti da će saobraćaj sa običnog HTTP biti preusmeren na HTTPS saobraćaj, prosleđuje lažni saobraćaj klijentu. Sa druge strane, uspostavlja se lažna HTTPS veza sa serverom. Veza se uspostavlja sa lokacijom koju je klijent stvarno i želeo da poseti, a klijentu se prosleđuje sadržaj željene stranice kako ju je napadač primio, ali se stranica prosleđuje u HTTP obliku bez sertifikata i šifrovanja tako da je sadržaj dalje lako pratiti. Kako su podaci koji se razmenjuju sa klijentom u HTTP obliku i ne postoji provera sertifikata, nema načina da Internet pretraživači uoče bilo kakvu nepravilnost i upozore klijenta, tako da se u ovom napadu od klijente i ne zahteva nikakva interakcija. Samim tim uspešnost ovog napada je znatno izvesnija.

Ovaj napada zahteva veće poznavanje sigurnosnih propusta i teže ga je implementirati. Napad je grafički predstavljen na sl.5. i odvija se kroz sledeće korake:

- Sprovođenjem ARP napada napadač se umeće između servera i klijenta tako što i serveru i klijentu šalje lažne ARP pakete koji obmanjuju i klijenta i server.
- Napadač prati HTTP saobraćaj između servera i klijenta, prisluškujući i analizirajući saobraćaj.



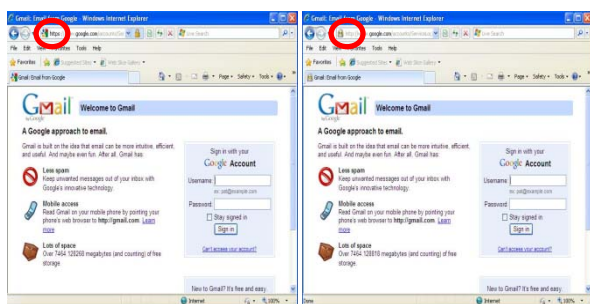
- Napadač postaje aktivan tek kada primeti zahtev za HTTPS saobraćajem <a href="https://...">, nakon čega zahtev menja sa <a href="http://...">. Takođe se pravi lista svih adresa koje su zamenjene radi dalje lakše analize i manipulacije.
- Ukoliko napadač kasnije primi HTTP zahtev od klijenta na osnovu zapisa zna da treba da uspostavi HTTPS komunikaciju sa serverom.
- Nakon uspostavljanja HTTP zahteva sa klijentom, saobraćaj je otvoren (nezaštićen), a jedina manifestacija napada koju klijent može da primeti, ukoliko obrati pažnju, je sam zapis URL adrese u Internet pretraživaču. Pri normalno korišćenju sigurni saobraćaj bi u svojoj URL adresi sadržao https, dok će u slučaju napada u URL adresi sadržati samo http.



Slika 5. Preusmeravanje HTTP i HTTPS saobraćaja

Programi koji su korišćeni u drugoj metodi za APR i DNS napad su isti kao i u prvoj metodi, dok je za uklanjanje HTTPS saobraćaja na strani klijenta korišćen sslstrip i Open SSL biblioteka.

Na sledećoj ilustraciji predstavljena je izgled pristupa Gmail servisu iz Internet pretraživača. Na levoj strani predstavljena je konekcija koja nije pod napadom dok je na desnom ekranu predstavljena konekcija koja se prisluškuje i pod napadom je.



Slika 6. Izgled ekrana bez napada i sa napadom na klijenta

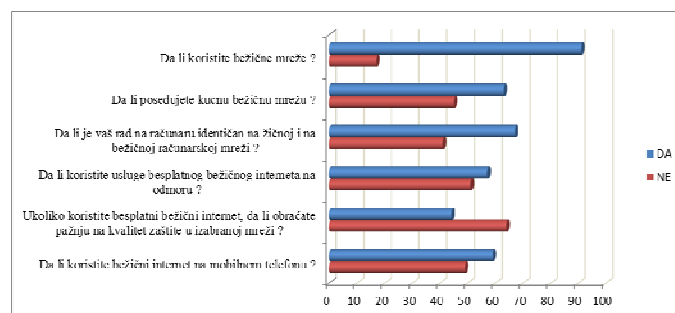
Kao što se iz ilustracije primećuje jako je teško utvrditi razliku između levog i desnog ekrana. Osim vizuelne razlike u jednom slovu klijenti u samom radu neće primetiti razliku u radu. Sa strane klijenta sve funkcionalnosti će ostati na istom

nivou dok će brzina učitavanja stranice biti gotovo identična u oba slučaja. Sve ovo utiče na to da je ovakav napad jako teško primetiti.

Prikazan napad je posebno interesantan u bežičnim mrežama, jer napadač ne mora imati fizički pristup lokalnoj mreži već se može nalaziti na bilo kojoj lokaciji u okviru dometa bežične mrežne stanice. Kako je analiza dobijana anketom predstavljena u sledećem segmentu rada pokazala, većina klijenata ne pravi razliku u radu u okviru žične i bežične računarske mreže. Analiza je takođe pokazala da većina klijenata ne vodi računa da li se saobraćaj u okviru bežične računarske mreže šifruje, čime dodatno olakšavaju posao potencijalnim napadačima.

## VI. ANALIZA PODATAKA PRIKUPLJENIH NAKON ODRŽANIH SAVETOVANJA

Na osnovu predstavljenih analiza i testova obavljena su edukativna predavanja i treninzi koji su imali preko 150 učesnika. Među učesnicima skupova našli su se studenti završnih godina fakulteta ali i poslovni ljudi. Održana su ukupno dva skupa u maju 2011 godine, jedan na teritoriji Srbije i drugi na teritoriji Bosne i Hercegovine. Objedinjeni rezultati anketa koje su učesnici popunjavali predstavljeni su na sledećoj slici.

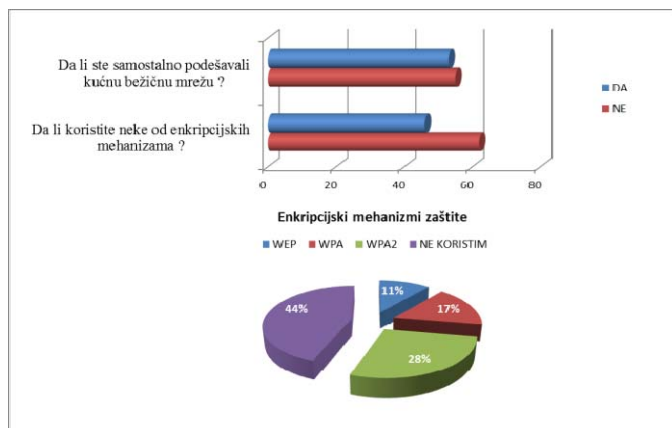


Slika 7. Rezultati ankete održane tokom seminara

Ono što je u uvodu ovog rada i predstavljeno, anketa učesnika skupa je potvrdila. Preko 90 % učesnika skupa odgovorilo je da koristi bežične računarske mreže. Preko 65% učesnika poseduje kućnu bežičnu računarsku mrežu i ne pravi razliku u radu na bežičnoj i žičnoj računarskoj mreži. Ono što je istaknuto u ovom radu i njegovim analizama je faktor bezbednosti na koji su posebno ranjivi klijenti bežičnih računarskih mreža. Istina je da se napadi na SSL koji su predstavljeni u radu mogući i u žičnim računarskim mrežama, ali se identitet napadača i postojanje napada mnogo teže detektuje u bežičnim računarskim mrežama. Istraživanje anketom pokazalo je da oko 60% ispitanika koristi usluge besplatnog interneta za vreme svog odmora. Prema mnogim analiza tada se najčešće dešavaju napadi na korisnike. Analiza je takođe pokazala da preko 60% ispitanika neće obratiti pažnju na činjenicu da koristi nepoznatu bežičnu računarsku mrežu, što će ih učiniti posebno ranjivim na napade i kompromitovanje podataka.

Kroz seminare je utvrđeno da preko 65% učesnika seminara poseduje kućnu bežičnu računarsku mrežu i da je

oko 50 % njih samostalno vršilo konfiguraciju. Međutim poražavajuća je bila činjenica da 44% učesnika koji su samostalno konfigurisali mrežu izabralo da ne štiti istu od mogućih napada.



Slika 8. Rezultati ankete učesnika seminara po pitanju zaštite bežičnih računarskih mreža

Kao što je već argumentovano i predstavljeno kroz praktičnu analizu u prethodnom radu autora pod nazivom [6] WEP predstavlja zastareli mehanizam zaštite koji ne nudi dovoljan nivo zaštite i vrlo se lako kompromituje. Pozitivan utisak analize ankete ostavila je činjenica da samo 11% anketiranih koristi stari i prevaziđeni WEP mehanizam koji pruža lažni osećaj sigurnosti.

Cilj savetovanja je svakako bio da se ova situacija promeni i da se podigne svest učesnika o potrebi za zaštitom lokalnih žičnih i bežičnih računarskih mreža. U toku savetovanja urađene su praktične demonstracije napada tako da su polaznici mogli i sami da se uvere koliko su neke od metoda, za koje su smatrali da su potpun bezbedne, podložne kompromitovanju. Takođe, značajno je podignuta svest za potrebom korišćenja kriptografskih mehanizama u bežičnim računarskim mrežama.

## VII. ZAKLJUČAK

Problem bezbednosti u žičnim i bežičnim računarskim mrežama svakako postoji. Cilj ovog rada i održanih seminara je upućivanje šireg auditorijuma u postojanje problema. Kroz rad je prikazano da i u najpouzdanijim metodama koje se koriste u najvećim sistemima, za koje većina smatra da su bezbedni, postoje mana koje zlonamerni korisnici mogu iskoristiti. Od situacije u kojoj su napade sprovodili retki

izuzetno upućeni i teorijski dobro potkovani pojedinci, došlo se do situacije da današnji alati za penetracijske testove ne zahtevaju previše znanja od korisnika. Ovakve alate koji su prevashodno napravljeni za penetracijsko testiranje i dijagnostikovanje računarskih mreža zlonamerni pojedinci koriste u cilju dobijanja lične koristi. Zbog svega navedenog autori rada smatraju bitnom tematiku bezbednosti i podizanje svesti o propustima koji mogu biti zlonamerno iskorišćeni.

## LITERATURA

- [1] Michael Howard, "Man-in-the-Middle Attack to the HTTPS Protocol", IEEE computer society, 2009, p.78-81.
- [2] S.Thomas. SSL and TLS Essentials. New york: Wiley Computing Publishing, 2004.
- [3] Moxie, Sslstrip. <http://www.thoughtcrime.org/software/sslstrip/>
- [4] T.Dierks and C.Allen, The TLS Protocol, IETF RFC 2246, 1999; [www.ietf.org/rfc/rfc2246.txt](http://www.ietf.org/rfc/rfc2246.txt).
- [5] Ponemon Institute© Research Report, Cost of Cyber Crime Study, August 2011
- [6] Analysis of the wireless network security IEEE 802.11 - The city of Belgrade, Saša Adamović Marko Šarac, Dalibor Radovanović, Infotech Jahorina, 2011/3
- [7] Certified Wireless Analysis Professional Official Study Guide (Exam PW0-205) bPlanet3 Wireless (Paperback - Oct 15, 2004)
- [8] 802.11 Wireless Networks: Security and Analysis (Computer Communications and Networks) by Alan Holt and Chi-Yu Huang (Hardcover - Jul 8, 2010)

## ABSTRACT

This paper presents and analyzes the current problems in computer networks. It presents the results of research on attacks in computer systems. We analyzed modern methods of protection and pointed to its shortcomings. The first part is the actual problems of protection of computer networks and is the current solutions. The second part focuses on the problem that there is currently represented in the modern methods of securing computer networks. The problem was analyzed by two methods of attack. Based on research conducted during the writing of the paper, authors organized two seminars on raising awareness about the problems of modern computer networks. Based on the discussions and surveys performed during the seminar, came to the new information which has been analyzed and presented through the paper. The aim of this paper is to present the actuality of the problem and to contribute in addressing security deficiencies.

## ANALYSIS OF SSL TRAFFIC SAFETY IN WIRELESS COMPUTER NETWORKS

Marko Sarac, Mladen Veinovic, Sasa Adamovic,  
Dalibor Radovanovic, Aleksandar Jevremovic