HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

# Napadi krađom korisničkih sjednica

**CCERT-PUBDOC-2007-03-185**

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

**CARNet CERT**, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

**LS&S**, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

# Sadržaj

**1. UVOD ..... 4**

**2. NAJČEŠĆE NAPADANI PROTOKOLI ..... 5**

2.1. TCP ..... 5
2.2. UDP ..... 6
2.3. HTTP ..... 6

**3. VRSTE KRAĐA SJEDNICA ..... 6**

3.1. KRAĐA SJEDNICE NA MREŽNOJ RAZINI ..... 6
3.1.1. Krivotvorenje IP adrese ..... 7
3.1.2. Slijepa krađa sjednice ..... 7
3.1.3. Napad preusmjeravanjem prometa ..... 8
3.1.4. Pojačan promet TCP ACK paketima ..... 8
3.1.5. Prikrivanje tragova napada ..... 9
3.1.6. Krađa UDP sjednice ..... 9
3.2. KRAĐA SJEDNICE NA APLIKACIJSKOJ RAZINI ..... 10
3.2.1. Prisluškivanje ..... 10
3.2.2. Napad pogađanjem ID oznake ..... 10
3.2.3. Umetanje HTML koda ..... 11
3.2.4. Krađa sjednice XSS napadom ..... 11

**4. ZAŠTITA OD NAPADA KRAĐOM SJEDNICA ..... 11**

4.1. ZAŠTITA NA MREŽNOJ RAZINI ..... 11
4.1.1. Kriptirani prijenosni protokoli ..... 11
4.1.2. Sigurne postavke računalne mreže ..... 11
4.2. ZAŠTITA NA APLIKACIJSKOJ RAZINI ..... 12
4.2.1. Sigurne ID oznake ..... 12
4.2.2. Provjera korisnički unesenih podataka ..... 12
4.2.3. Gašenje neaktivnih sjednica ..... 12
4.2.4. Izmjena ID oznaka sjednice ..... 13
4.2.5. Ponovna autorizacija ..... 13
4.2.6. Otkrivanje napada pogađanjem ID oznake ..... 13
4.3. ALATI ZA OTKRIVANJE RANJIVOSTI ..... 13
4.3.1. MITM posredni poslužitelji ..... 13
4.3.2. Otkrivanje ranjivosti na mrežnom sloju ..... 13
4.3.3. Otkrivanje ranjivosti na aplikacijskom sloju ..... 13

**5. ZAKLJUČAK ..... 14**

**6. REFERENCE ..... 14**

# 1. Uvod

Napadač krađom korisničke sjednice preuzima kontrolu nad ukradenom sjednicom sa ciljem stjecanja neovlaštenog pristupa podacima i uslugama ili podmetanja krivotvorenih podataka. Pod pojmom sjednice, u kontekstu računalnih mreža, podrazumijeva se postojana veza na sjedničkom sloju, sloju mrežnog protokola, između ravnopravnih korisnika (eng. *peer*) ili između klijenta i poslužitelja. U većini primjena autorizacija korisnika odvija se prilikom stvaranja sjednice, što kradljivci sjednica iskorištavaju izvođenjem napada tijekom aktivnosti sjednice.

Komunikacijski protokoli najčešće izloženi napadima krađom korisničke sjednice su TCP, UDP i HTTP protokoli, ujedno i najzastupljeniji komunikacijski protokoli na Internetu. Napade je moguće podijeliti na one na mrežnoj i na aplikacijskoj razini. Napadi na mrežnoj razini odnose se na presretanje i izmjenu podatkovnih paketa i njima su izloženi TCP i UDP protokoli jer oni implementiraju korisničke sjednice. HTTP je protokol koji ne pamti stanja (eng. *stateless*) pa se korisničke sjednice implementiraju na razini pojedine aplikacije. Zbog toga su napadi krađom sjednice na aplikacijskoj razini manje univerzalni i uvelike ovise o ranjivostima napadnute web aplikacije.

Metode zaštite od napada krađom korisničkih sjednica su, kao i sami napadi, podijeljene na metode zašite u mrežnom i u aplikacijskom sloju. Metode zaštite na mrežnoj razini odnose se na korištenje enkripcije i podešavanje odgovarajućih postavki mreže. Na aplikacijskoj razini se od napada krađom korisničke sjednice moguće štititi stvaranjem sigurnih identifikacijskih oznaka sjednice i njihovom periodičkom izmjenom, sigurnosnim provjerama korisnički unesenih podataka, pravovremenim gašenjem neaktivnih sjednica, zahtijevanjem ponovne autorizacije korisnika prilikom pristupa osjetljivim sadržajima te postavljanjem zamki u vidu nepostojećih identifikacijskih oznaka.

# 2. Najčešće napadani protokoli

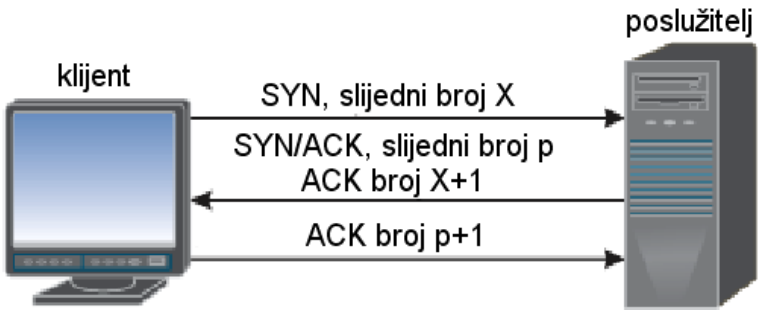
Tri protokola najčešće izložena napadima krađom korisničkih sjednica su TCP, UDP i HTTP. Osim navedenih protokola na ovakve napade ranjivi su svi protokoli koji ne koriste enkripciju, npr. telnet (eng. *TELetype NETwork*), FTP (eng. *File Transfer Protocol*) i DNS (eng. *Domain Name System*) protokol.

## 2.1. TCP

TCP (eng. *Transmission Control Protocol*) protokol jedan je od glavnih protokola korištenih na TCP/IP računalnim mrežama. IP protokol upravlja paketima dok TCP protokol omogućuje povezivanje dvaju korisnika i razmjenu nizova podataka (eng. *data stream*). Ovaj protokol jamči dostavu poslanih paketa te osigurava primitak podatkovnih paketa redoslijedom kojim su poslani.

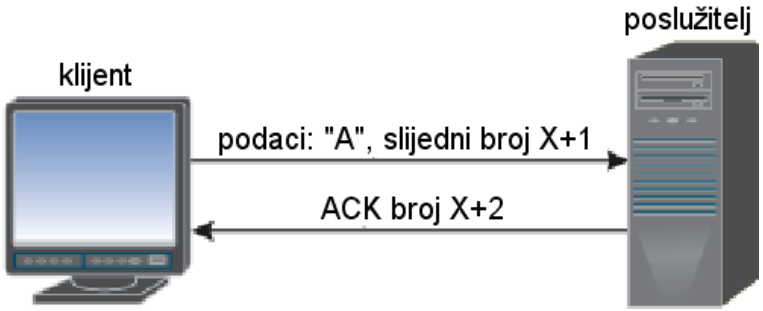
Kako bi osigurao ispravan redoslijed dostave paketa TCP protokol koristi potvrdne poruke (eng. *acknowledgement - ACK*) i označavanje niza paketa. Time je omogućeno stvaranje pouzdane dvosmjerne (eng. *full duplex*) veze. Uspostavljanje veze između klijenta i poslužitelja započinje usklađivanjem u tri koraka (eng. *three-way handshake*):

1. Klijent poslužitelju šalje sinkronizacijski paket (SYN) slijednog broja *X*.
2. Poslužitelj odgovara potvrdnim paketom (SYN/ACK) koji sadrži poslužiteljski slijedni broj *p* i ACK broj koji odgovara primljenom SYN paketu. ACK broj označuje koji je sljedeći slijedni broj kojega poslužitelj očekuje od klijenta, u ovom primjeru to je *X + 1*.
3. Klijent potvrđuje primitak SYN/ACK paketa slanjem ACK paketa koji sadrži sljedeći slijedni broj kojega očekuje od servera, u ovom primjeru to je *p + 1*.




**Slika 1:** Usklađivanje klijenta i poslužitelja u tri koraka

Nakon usklađivanja, komunikacija između klijenta i poslužitelja svodi se na razmjenu paketa i inkrementiranje slijednih brojeva kako bi se potvrdilo slanje i primitak paketa. Na primjer, klijent nakon usklađivanja poslužitelju šalje paket koji sadrži podatke, u primjeru na slici Slika 2 slovo „A“, i slijedni broj *X + 1*. Poslužitelj odgovara ACK paketom sa sljedećim slijednim brojem *X + 2* (*X + 1* plus jedan oktet za slovo „A“). Razdoblje u kojem se podaci između klijenta i poslužitelja razmjenjuju prema TCP protokolu naziva se TCP sjednicom.




**Slika 2:** Slanje podataka unutar TCP sjednice

### 2.2. UDP

UDP (eng. *User Datagram Protocol*) je bespojni (eng. *connection-less*) protokol koji se, kao i TCP protokol, izvodi na IP mrežama. Za razliku od TCP/IP skupa protokola, UDP/IP pruža malo mogućnosti uočavanja i ispravljanja pogrešaka, ali zato omogućuje izravno slanje i primanje UDP paketa (eng. *datagram*).
UDP ne koristi slijedne brojeve kao TCP i uglavnom se koristi za emitiranje (eng. *broadcast*) poruka ili za postavljanje DNS upita. Ovaj protokol se koristi i u primjenama u stvarnom vremenu, npr. kod daljinskog upravljanja ili računalnih igara za više igrača, kod kojih je značajnije dostaviti podatke u što kraćem vremenskom roku, a njihov redoslijed ili gubitak pojedinih paketa nije značajan. Zbog činjenice da se radi o bespojnom protokolu i zbog toga što nema napredne mogućnosti TCP protokola, UDP protokol je ranjiviji na napade krađom korisničke sjednice.
Razdoblje razmjene podataka između klijenta i poslužitelja prema UDP protokolu naziva se UDP sjednicom. UDP i TCP sjednica započinje autorizacijom korisnika i traje dok su ACK oznake ispravne. Krađa ovih sjednica provodi se preuzimanjem kontrole nad paketima koji se razmjenjuju između klijenta i poslužitelja.

### 2.3. HTTP

HTTP (eng. *Hyper Text Transfer Protocol*) je protokol koji leži iza WWW (eng. *World Wide Web*) mreže. On definira oblik i prijenos poruka te način na koji bi web poslužitelji i preglednici trebali reagirati na različite naredbe. Na primjer, unošenje URL adrese u web pregledniku uzrokuje slanje HTTP naredbe web poslužitelju koji na nju odgovara zatraženom web stranicom.
Ovaj protokol ne pamti stanja, drugim riječima svaka transakcija HTTP protokolom provodi se neovisno i bez znanja o prošlim transakcijama. Zbog toga HTTP sam po sebi ne može razlikovati korisnike. Kako bi se pratilo pojedinog korisnika i s njim povezane podatke, web aplikacije stvaraju vlastite sjednice unutar kojih se pamte spomenuti podaci. Otimanje korisničkih HTTP sjednica zbog toga je više vezano uz napadnutu web aplikaciju nego uz sam protokol.
HTTP sjednica započinje korisnikovim prijavljivanjem na web aplikaciji i traje do njegova odjavljivanja. Unutar sjednice pamti se identitet i svi parametri vezani uz korisnika vlasnika sjednice. Tijekom stvaranja sjednice dodjeljuje joj se identifikacijski ID broj i on se šalje zajedno s HTTP zahtjevima koji pripadaju toj korisničkoj sjednici.
Web aplikacije implementiraju upravljanje sjednicama unutar klijentske ili unutar poslužiteljske aplikacije. Ako je upravljanje sjednicama implementirano na strani klijenta, autorizacijski podaci i podaci o identitetu korisnika pohranjeni su u tzv. *cookie* podatkovne strukture. Klijent poslužitelju šalje ove podatke, zajedno s ID brojem sjednice, sa svakim HTTP zahtjevom. Ako je upravljanje sjednicama implementirano na strani poslužitelja isti ovi podaci pohranjeni su u pozadinskoj (eng. *back-end*) bazi podataka. ID broj sjednice u tom slučaju koristi se za povezivanje primljenih zahtjeva sa zapisima u bazi podataka, odnosno s pojedinim klijentom.

## 3. Vrste krađa sjednica

Krađa korisničke sjednice odvija se na mrežnoj i/ili na aplikacijskoj razini. Krađa na mrežnoj razini odnosi se na presretanje i izmjenu podatkovnih paketa koji se prenose između klijenta i poslužitelja tijekom TCP ili UDP sjednice. Krađa sjednice na aplikacijskoj razini svodi se na stjecanje ID oznake HTTP sjednice definirane unutar aplikacije. U većini slučajeva ovi napadi događaju se istovremeno. Na primjer, uspješna krađa TCP sjednice napadaču omogućuje pristup podacima potrebnih za napad na korisničku sjednicu na aplikacijskom sloju.

### 3.1. Krađa sjednice na mrežnoj razini

Krađe sjednica na mrežnoj razini napadačima su praktične jer ne postoji potreba prilagođavanja napada web aplikaciji. Napada se izravno tok podataka definiran TCP ili UDP protokolom.
Cilj napada na TCP sjednicu je onemogućavanje komunikacije između klijenta i poslužitelja krivotvorenjem podatkovnih paketa. Krivotvoreni paketi oponašaju vjerodostojne pakete poslane od strane poslužitelja i klijenta te održavaju iluziju neprekinute i vjerodostojne komunikacije među njima. Komunikacija između klijenta i poslužitelja prekida se ako poslužiteljev slijedni broj ne

odgovara klijentovom ACK broju ili ako klijentov slijedni broj ne odgovara ACK broju poslužitelja. Ovo stanje naziva se neusklađenošću (eng. *desynchronized state*) klijenta i poslužitelja i moguće ga je izazvati:

- krivotvorenjem IP adrese,
- slijepom krađom sjednice ili
- napadom preusmjeravanja prometa.

Neusklađenost TCP komunikacije klijenta i poslužitelja može uzrokovati pojačan promet TCP ACK paketima koji otkriva krađu sjednice. Zbog toga napadači različitim tehnikama pokušavaju prikriti tragove zlonamjernog djelovanja.

### 3.1.1. Krivotvorenje IP adrese

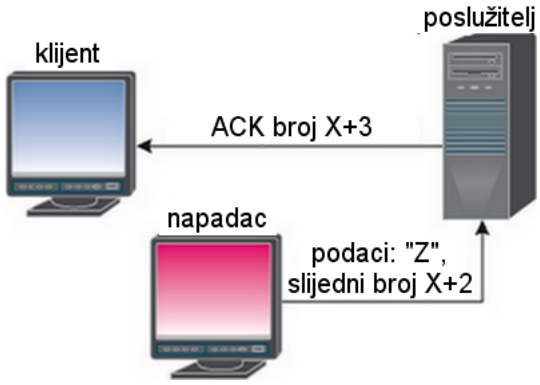
Slanjem podatkovnog paketa s krivotvorenom oznakom IP adrese izvorišta napadač primatelja paketa nastoji uvjeriti u njegovu vjerodostojnost. Za uspješno izvođenje ovakvog napada potrebno je saznati IP adresu klijenta te izmijeniti zaglavlja paketa kako bi se činilo da dolaze sa spomenute adrese. Krivotvoreni podatkovni paketi kod ovakvog napada usmjeravaju se na izvorištu, tj. napadač određuje njihovu rutu prema poslužitelju prije slanja.

Nakon uspješnog krivotvorenja IP adrese napadač utvrđuje sljedeći slijedni broj kojega poslužitelj očekuje. Pomoću tog broja u TCP sjednicu umeću se krivotvoreni paketi prije no što klijent stigne poslati paket s istom oznakom. Na ovaj način napadač desinkronizira komunikaciju između klijenta i poslužitelja. Slijedni i ACK brojevi nisu više usklađeni jer je poslužitelj primio paket kojega klijent nije poslao. Slanjem većeg broja krivotvorenih paketa odstupanje između klijenta i poslužitelja raste.

### 3.1.2. Slijepa krađa sjednice

Ako je izvorišno usmjeravanje paketa onemogućeno zlonamjerni korisnik može izvršiti napad slijepom krađom korisničke sjednice. Ovaj napad sastoji se od umetanja zlonamjerno oblikovanih podataka u TCP sjednicu. Napad se naziva slijepim zbog toga što napadač može slati podatke ili naredbe, ali nema uvida u odgovore na poslane podatke. Zlonamjerni korisnik u biti nagađa kakvi bi odgovori klijenta i poslužitelja na umetnute pakete mogli biti. Primjer zlonamjerne naredbe koju bi slijepi kradljivac sjednice mogao umetnuti je naredba za postavljanje korisničke zaporke čije uspješno izvođenje bi mu omogućilo pristup napadnutoj aplikaciji.

Na slici Slika 3 prikazana je slijepa krađa TCP korisničke sjednice. Napadač je u ovom primjeru prethodno otkrio sljedeći slijedni broj kojeg poslužitelj očekuje te, prije no što klijent uspije poslati paket s tim slijednim brojem, šalje paket kojeg poslužitelj prihvaća kao valjanog. Zlonamjerni korisnik može spriječiti ili usporiti klijenta u slanju paketa, npr. izvođenjem napada uskraćivanjem resursa, ili ga može pokušati preduhitriti. Time se izaziva neusklađenost klijenta i poslužitelja te sjednica prelazi u posjed napadača.




**Slika 3:** Slijepa krađa TCP sjednice

### 3.1.3. Napad preusmjeravanjem prometa

Napad preusmjeravanjem prometa (eng. *man in the middle*) izvodi se pomoću posebnog alata koji presreće svu komunikaciju između klijenta i poslužitelja (eng. *packet sniffer*). Time napadač ostvaruje pristup svim podatkovnim paketima koji pripadaju napadnutoj sjednici i može ih po volji mijenjati. Osnovna poteškoća u izvođenju ovog napada je preusmjeravanje paketa tako da na putu između klijenta i poslužitelja prolaze napadačevim računalom.

Jedan od načina preusmjeravanja prometa preko napadačeva računala je krivotvorenjem ICMP (eng. *Internet Control Message Protocol*) poruka. ICMP protokol je dodatak IP protokolu, a koristi se za slanje poruka o pogreškama vezanim uz dostavljanje paketa. Kradljivac sjednice koristi krivotvorene ICMP poruke kako bi klijenta i poslužitelja uvjerio da je ruta preko njegova računala bolja (u smislu da je brža, kraća, pouzdanija i sl.) od izvorne rute.

Drugi način preusmjeravanja prometa je krivotvorenjem ARP (eng. *Address Resolution Protocol*) tablica. Ove se tablice koriste za povezivanje lokalnih IP adresa sa sklopovskim ili MAC (eng. *Media Access Control*) adresama. Krivotvorenje se provodi slanjem lažnih ARP zahtjeva za ažuriranje tablica koji napadnutoj IP adresi pridjeljuju napadačevu sklopovsku adresu. Svi paketi namijenjeni spomenutoj IP adresi preusmjeravaju se tada prema napadaču, koji ih može po volji mijenjati i nakon toga proslijediti prema prvotnom odredištu.

Na slici Slika 4 prikazan je primjer krivotvorenja ARP tablice. Klijent A do trenutka napada nije komunicirao s klijentom B pa u ARP tablici nema njegov zapis. Zbog toga šalje ARP zahtjev za MAC adresom klijenta B, određenog njegovom IP adresom. Prije odgovora klijenta B napadač šalje krivotvoren ARP odgovor sa svojom MAC adresom, klijent A u ARP tablicu zapisuje spomenutu MAC adresu i na istu šalje podatke namijenjene klijentu B.


**Slika 4:** Preusmjeravanje prometa krivotvorenjem ARP tablice

### 3.1.4. Pojačan promet TCP ACK paketima

Jedna od posljedica krađe TCP sjednice je pojačan promet TCP ACK paketima (eng. *TCP ACK storm*). Neoprezan napadač može vrlo lako i brzo biti otkriven jer ovakav promet može ozbiljno poremetiti rad računalne mreže.

Pojačan promet TCP ACK paketima rezultat je neusklađenosti klijenta i poslužitelja koji zbog odstupanja očekivanih slijednih brojeva ne mogu razmjenjivati pakete. Kako bi se ponovno uskladili poslužitelj i klijent jedan drugome šalju ACK pakete s neodgovarajućim slijednim brojevima. Velik broj takvih paketa može zagušiti mrežu i sustavima za uočavanje i sprječavanje nedozvoljenih aktivnosti ukazati na krađu TCP korisničke sjednice.


**Slika 5:** Pojačan promet TCP ACK paketima

### 3.1.5. Prikrivanje tragova napada

Kako bi prikrio tragove krađe korisničke sjednice napadač može krivotvorenjem ARP tablica spriječiti rast prometa TCP ACK paketima. Krivotvorenjem ARP zahtijeva za ažuriranjem tablica zlonamjerni korisnik može IP adresama, potencijalnim izvorištima pretjeranog broja TCP ACK paketa, pridijeliti nepostojeće sklopovske adrese. U tom slučaju podatkovni ih paketi ne bi mogli doseći pa ne bi došlo do zagušenja mreže.


**Slika 6:** Prikrivanje tragova napada krivotvorenjem ARP tablica

Nakon napada zlonamjerni korisnik može ponovnim usklađivanjem klijenta i poslužitelja dodatno prikriti tragove zlonamjernih aktivnosti. Kako bi to učinio klijentov slijedni broj treba podesiti tako da odgovara sljedećem slijednom broju kojega poslužitelj očekuje. Ovo je moguće postići navođenjem korisnika na slanje točnog broja dodatnih okteta kojim bi se slijedni brojevi uskladili. Primjer krivotvorenog zahtjeva kojim se ovo pokušava:

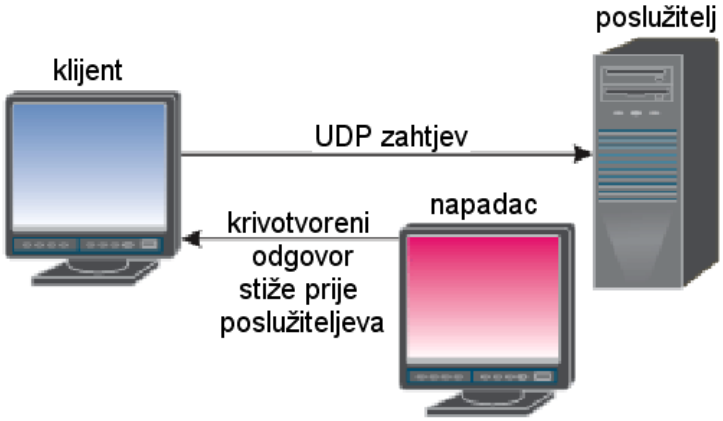
```
msg from root: power failure – try to type 13 chars
```

Osnovni nedostatak ovakvog prikrivanja tragova je potreba za sudjelovanjem napadnutog korisnika.

### 3.1.6. Krađa UDP sjednice

Krađa UDP korisničkih sjednica provodi se u osnovi na jednak način kao krađa TCP sjednica. Kako UDP protokol ne koristi slijedne niti ACK brojeve napadač jednostavno treba krivotvoriti odgovor poslužitelja na klijentov UDP zahtjev i dostaviti ga prije pravog odgovora. Ako zlonamjerni korisnik

uspije preusmjeriti komunikaciju preko svoga računala napad je još jednostavniji jer je tada moguće zaustaviti poslužiteljeve odgovore.




**Slika 7:** Krađa UDP korisničke sjednice

## 3.2. Krađa sjednice na aplikacijskoj razini

Na ovoj razini napadi se uglavnom provode krađom ID oznake sjednice, bilo za preuzimanje kontrole nad otvorenom sjednicom ili za neovlašteno otvaranje nove sjednice. ID oznaka sjednice može se nalaziti:

- Ugrađena u URL (eng. *Universal Resource Locator*) oznaku koju aplikacija prima putem 'HTTP GET' zahtjeva nakon klijentova klika na vezu ugrađenu u web stranici.
- Unutar polja formulara proslijeđenog aplikaciji. Uobičajeno je pohranjivanje identifikacijskih podataka sjednice u skrivenom polju formulara i njihovo prosljeđivanje 'HTTP POST' naredbom.
- U posebnim podatkovnim strukturama (eng. *cookies*).

ID oznake sjednice pohranjene na sva tri navedena mjesta dostupne su napadaču. Ako se oznaka nalazi ugrađena u URL oznaku moguće ju je pronaći pretraživanjem dnevničkih zapisa web preglednika, *proxy* poslužitelja ili vatrozida. Kod nesigurnijih web aplikacija moguće je unošenjem URL oznake iz dnevničkog zapisa web preglednika neovlašteno steći pristup istoj. ID oznakama sjednice poslanima unutar formulara 'POST' naredbom teže je pristupiti, ali kako se formulari šalju mrežom napadač njihovim presretanjem može doći do podataka potrebnih za krađu sjednice. Kradljivac korisničke sjednice podacima pohranjenima unutar *cookie* strukture može pristupiti izravno napadom na klijentovo računalo, na kojemu je pohranjena, ili presretanjem poruka koje ta struktura šalje i prima tijekom aktivnosti sjednice.

### 3.2.1. Prisluškivanje

Primjenom jednakih metoda kao kod krađe TCP korisničkih sjednica napadač može preusmjeriti promet preko svog računala. Ako se HTTP promet prenosi bez kriptiranja zlonamjerni korisnik može pregledavanjem presretnutih paketa steći ID oznaku korisničke sjednice. Nekriptirani promet u nekim slučajevima može prenositi korisnička imena i zaporke što napadaču značajno olakšava krađu ili neovlašteno pokretanje nove korisničke sjednice.

### 3.2.2. Napad pogađanjem ID oznake

Ako je ID oznaka sjednice predvidljivog oblika, zlonamjerni korisnik može izvršiti napad pogađanjem (eng. *brute force attack*) koji se svodi na iskušavanje velikog broja ID oznaka koje odgovaraju uočenom uzorku. Ovaj napad lako je automatizirati što olakšava iskušavanje velikog broja mogućnosti dok se ne pronađe valjana identifikacijska oznaka. Na primjer, u idealnim uvjetima napadač povezan Internet DSL (eng. *Digital Subscriber Line*) vezom može iskušati do 1000 ID oznaka u sekundi. Ako algoritam koji stvara identifikacijske oznake nije dovoljno nasumičan napadač može ovim napadom relativno brzo steći upotrebljivu oznaku.

### 3.2.3. Umetanje HTML koda

Napad umetanjem HTML koda za cilj ima podmetanje zlonamjerno oblikovanog programskog koda i njegovo izvođenje unutar web preglednika napadnutog korisnika. Tako pokrenuti HTML programski kod na ranjivom računalu pronalazi i napadaču šalje podatke potrebne za krađu korisničke sjednice.

### 3.2.4. Krađa sjednice XSS napadom

XSS (eng. *Cross-Site Scripting*) napad temelji se na izostanku sigurnosne provjere korisnički unesenih podataka unutar web aplikacije prije slanja odgovora klijentu. Cilj napada je navođenje web preglednika na pokretanje umetnutog programskog koda s ovlastima napadnute web aplikacije. Tako pokrenuti programski kod pronalazi i zlonamjernom korisniku dostavlja identifikacijsku oznaku sjednice. Uspješnost XSS napada uvelike ovisi o ranjivosti napadnute web aplikacije.

# 4. Zaštita od napada krađom sjednica

Metode zaštite od napada krađom korisničke sjednice moguće je, jednako kao i same napade, podijeliti na one koje djeluju u mrežnom i u aplikacijskom sloju. Ranjivosti mreže ili web aplikacije na napade krađom sjednice moguće je utvrditi pomoću posebnih programskih paketa.

## 4.1. Zaštita na mrežnoj razini

Zaštita od krađe korisničke sjednice na mrežnoj razini svodi se na zaštitu podatkovnih paketa od neovlaštenog pristupa. Ako zlonamjerni korisnik ne može interpretirati zaglavlja presretnutih podatkovnih paketa onda ih nije moguće izmijeniti tako da zadrže privid vjerodostojnosti niti je moguće uspješno krivotvoriti nove zlonamjerno oblikovane pakete.

### 4.1.1. Kriptirani prijenosni protokoli

Osnovna metoda zaštite paketa od neovlaštenog pristupa je korištenje kriptiranih prijenosnih protokola kao što su IPSec (eng. *Internet Protocol Security*), SSL (eng. *Secure Socket Layer*) i SSH (eng. *Secure Shell*) protokoli. Za uspješnu krađu sjednice zaštićene jednim od ovakvih protokola napadač u najmanju ruku mora poznavati korišteni enkripcijski ključ. Zbog toga se ključevi stvaraju takvima da ih je teško nasumično pogoditi i pohranjuju se tako da im je teško pristupiti bez odgovarajućih ovlasti.

Zbog toga što klijent i poslužitelj neispravno kriptirane pakete jednostavno zanemaruju, zlonamjerni korisnik treba, pored dekriptiranja presretnutih paketa, imati mogućnost valjanog kriptiranja paketa koje želi umetnuti u napadnutu sjednicu. Neispravnima se smatraju svi paketi koji nisu kriptirani ključem pridruženim danoj sjednici.

IPSec protokol osigurava sigurnu razmjenu paketa na IP mrežnom sloju. Definira dva načina enkripcije paketa: transportnu i tunelirajuću enkripciju. Kod transportne enkripcije kriptira se samo dio paketa koji prenosi podatke dok se zaglavlje paketa prenosi nekriptirano. Tunelirajuća enkripcija kriptira cjelokupni paket, podatke i zaglavlje. Oba načina enkripcije smanjuju mogućnost krađe sjednice, ali tunelirajuća enkripcija pruža znatno veću razinu sigurnosti zbog toga što napadaču otežava čak i otkrivanje izvorišta i odredišta pojedinog paketa. IPSec pruža zaštitu na mrežnoj razini zbog toga što kriptira podatke na razini paketa.

SSL protokol štiti privatne web dokumente koji se prenose SSL vezom. Većina web preglednika podržava ovaj protokol, a URL adrese koje zahtijevaju otvaranje SSL veze najčešće započinju nizom „https:“ umjesto uobičajenog „http:“ početnog niza. SSL pruža zaštitu na aplikacijskoj razini zbog toga što kriptira podatke prenošene unutar HTTP sjednice.

SSH protokol onemogućuje krivotvorenje IP adrese i napade izvorišnim usmjeravanjem podatkovnih paketa. Sjednicu zaštićenu ovim protokolom nije moguće ukrasti, a najviše što napadač može učiniti je njezino prekidanje.

### 4.1.2. Sigurne postavke računalne mreže

Osim zaštite paketa od neovlaštenog pristupa sjednicu je na mrežnoj razini moguće zaštiti sigurnijim postavkama mreže. Na primjer, krivotvorenje IP adresa i napade izvorišnim usmjeravanjem paketa

moguće je spriječiti odgovarajućim postavkama vatrozida i usmjerivača. Izvorišno usmjeravane pakete moguće je u određenim situacijama odbaciti, a u primjenama gdje je to prihvatljivo izvorišno usmjeravanje može se u potpunosti onemogućiti. Krivotvorenje ARP tablica moguće je onemogućiti korištenjem statičkih ARP tablica, a ako su dinamičke tablice nužne njihove promjene moguće je nadzirati posebnim alatima, poput *arpwatch* programskog paketa. Onemogućavanjem preusmjeravanja prometa pomoću ICMP poruka moguće je otežati izvođenje krađe sjednice preusmjeravanjem prometa.

## 4.2. Zaštita na aplikacijskoj razini

Zaštita korisničke sjednice na aplikacijskoj razini odnosi se na zaštitu identifikacijskog broja od krađe i od napada pogađanjem.

### 4.2.1. Sigurne ID oznake

Najbolji način zaštite sjednice na aplikacijskoj razini je korištenje sigurne ID oznake. To se odnosi kako na klijentski tako i na poslužiteljski dio web aplikacije. Neke od preporuka za stvaranje sigurne identifikacijske oznake su:

- Povećati duljinu ID oznake *cookie* strukture ili sjednice. Identifikacijska oznaka treba biti dovoljno duga kako zlonamjerni korisnik korištenjem automatiziranog napada nasumičnim pogađanjem ne bi uspio, za vrijeme trajanja sjednice, ispitati značajniji dio mogućih vrijednosti oznake. Uzimajući u obzir današnja procesorska i ograničenja u propusnosti računalnih mreža, preporuča se korištenje oznaka ne kraćih od 50 znakova.
- Koristiti što nasumičnije identifikacijske oznake. Iako se korištenje rednog broja korisnika kao identifikacijske oznake sjednice ili stvaranje slijednih ID oznaka u prvi mah čine smislenim i praktičnim rješenjima, takvim pristupom napadaču bi se uvelike olakšalo pogađanje valjane oznake, a samim time i krađa sjednice. Zbog toga se preporuča statističko testiranje nasumičnosti stvorenih ID oznaka prije njihove upotrebe. Pogađanje ID oznake stvorene nekim od nasumičnih algoritama trebalo bi biti izrazito teško.
- Zaštititi integritet ID oznake sjednice. Ako je identifikacijskoj oznaci sjednice dodana oznaka autentičnosti, provjerom ovih oznaka kod svakog paketa na strani poslužitelja moguće je uočiti neovlaštene izmjene. Primjer oznake autentičnosti je MD5 (eng. *Message-Digest algorithm 5*) suma izvorne oznake sjednice koju je poslao poslužitelj, klijentske IP adrese i vremenske oznake početka sjednice.
- Koristiti poslužiteljske ID oznake sjednice. Umjesto stvaranja identifikacijske oznake sjednice unutar web aplikacije moguće je istu stvoriti na aplikacijskom poslužitelju. Primjeri ovakvih oznaka su *ASPSessionID* i *JSESessionID* oznake koje su dokazano otpornije na napade krađom korisničke sjednice.
- Koristiti kriptirane ID oznake sjednice. Dodatna zaštita sjednice postiže se kriptiranjem identifikacijske oznake ili cjelokupne komunikacije unutar sjednice. Moguće je koristiti različite ID oznake za „sigurne“ i „nesigurne“ dijelove web stranice tako da se oznake koje se prenose zaštićenom SSL vezom razlikuju od oznaka prenošenih nezaštićenim vezama.

### 4.2.2. Provjera korisnički unesenih podataka

Poslužitelj bi trebao provoditi stroge sigurnosne provjere korisnički unesenih podataka primljenih od klijenta. Sve podatke unutar 'GET' i 'POST' treba nadzirati kako bi se smanjila mogućnost uspješnog umetanja HTML programskog koda ili izvođenje XSS napada.

### 4.2.3. Gašenje neaktivnih sjednica

Korisnici često dijele klijentska računala i zbog toga je nužno gašenje korisničkih sjednica nakon određenog perioda neaktivnosti. Sjednice koje se ne gase na ovaj način zlonamjernom korisniku ujedno omogućuju neograničeno vrijeme za izvođenje napada nasumičnim pogađanjem identifikacijske oznake.

#### 4.2.4. Izmjena ID oznaka sjednice

Dodatna metoda otežavanja napada nasumičnim pogađanjem identifikacijske oznake korisničke sjednice je njezina periodička izmjena. Time se HTTP sjednica prividno gasi i zlonamjernom se korisniku pruža kraći vremenski period za izvođenje napada.

#### 4.2.5. Ponovna autorizacija

Za pristup dijelovima web stranice koji su sigurnosno kritični moguće je zahtijevati ponovnu autorizaciju korisnika unutar aktivne HTTP sjednice. Ovo je nadogradnja metode korištenja različitih ID oznaka za pristup pojedinim dijelovima web stranice i pruža dodatnu razinu sigurnosti. U takvom slučaju napadač, čak ako i uspije ukrasti korisničku sjednicu, neće moći učiniti značajniju štetu, na primjer izvršiti novčanu transakciju kod bankovnih web aplikacija.

#### 4.2.6. Otkrivanje napada pogađanjem ID oznake

Uočavanjem napada nasumičnim pogađanjem identifikacijske oznake HTTP sjednice moguće je istu dodatno zaštititi od krađe. To je moguće učiniti stvaranjem ID oznaka nepostojećih sjednica koje djeluju kao zamka. U slučaju primanja zahtjeva s nekom od lažnih identifikacijskih oznaka sa sigurnošću je moguće utvrditi da se radi o napadu i poduzeti odgovarajuće mjere, kao što su onemogućavanje pristupa s napadačeve IP adrese ili gašenje kompromitiranog korisničkog računa.

### 4.3. Alati za otkrivanje ranjivosti

#### 4.3.1. MITM posredni poslužitelji

MITM (eng. *Man In The Middle*) posredni (eng. *proxy*) poslužitelji presreću podatkovne pakete upućene klijentu i one upućene poslužitelju i korisniku omogućuju njihovu izmjenu. Primjenom ovih alata moguće je utvrditi ranjivost računalne mreže na napade preusmjeravanjem prometa. Primjeri ovakvih alata su *Achilles* i *Paros* programski paketi koji omogućuju otvaranje odvojenih SSL sjednica prema poslužitelju i prema klijentu te krivotvorenje njihove međusobne komunikacije.

#### 4.3.2. Otkrivanje ranjivosti na mrežnom sloju

*Juggernaut* i *Hunt* programski paketi mogu biti korišteni za izvođenje napada krađom TCP sjednice. Spomenute pakete moguće je podesiti da prisluškuju mrežni promet određenih karakteristika (npr. pakete upućene pojedinom klijentu), da izvode automatizirane napade i napade krivotvorenjem ARP tablica te da prikrivaju tragove napada ponovnim usklađivanjem klijenta i poslužitelja.

#### 4.3.3. Otkrivanje ranjivosti na aplikacijskom sloju

*SPI Dynamics Cookie Cruncher* je alat namijenjen analizi ranjivosti na napade krađom korisničke sjednice aplikacijske razine. Ovaj paket provodi analizu *cookie* struktura podataka sa ciljem utvrđivanja mogućnosti predviđanja ili pogađanja vrijednosti identifikacijske oznake sjednice od strane zlonamjernog korisnika.

# 5. Zaključak

Brojni korisnici uviđaju i iskorištavaju prednosti poslovanja putem web aplikacija pa je učestalost i obim elektroničkog poslovanja u stalnom porastu. Sve više osjetljivih podataka se zbog toga prenosi Internetom te su financijske informacije i identifikacijski podaci izloženi neovlaštenom pristupu i zloupotrebi. Zlonamjerni korisnici spremni su uložiti znatan trud i vrijeme kako bi ostvarili pristup navedenim podacima pa se javlja velika potreba za zaštitom od napada krađom korisničkih sjednica.

Korisničke sjednice potrebno je od napada krađom štititi na mrežnom sloju, na razini podatkovnih paketa, i na aplikacijskom sloju, na razini web aplikacija. Na oba sloja potrebno je implementirati enkripciju: na mrežnom sloju kriptiraju se paketi, a na aplikacijskom sloju identifikacijske oznake korisničkih sjednica i *cookie* strukture podataka. Zaštitu na mrežnom sloju dodatno je moguće implementirati postavkama računalne mreže koje onemogućuju pojedine metode napada, kao što su krivotvorenje IP adresa, ARP tablica i ICMP poruka.

Kako bi se od napada zaštitile korisničke sjednice na aplikacijskoj razini potrebno je koristiti duge i statistički nasumične identifikacijske oznake sjednica te ih tijekom trajanja sjednice periodički izmjenjivati. Neaktivne sjednice potrebno je pravovremeno gasiti, provoditi sigurnosne provjere korisnički unesenih podataka i implementirati ponovnu autorizaciju korisnika unutar aktivne sjednice.

# 6. Reference


[1] Mark Lin: An Overview of Session Hijacking at the Network and Application Levels, GSEC Practical Assignment, 2005.

[2] Kevin Lam, David LeBlanc, Ben Smith: Theft On The Web: Preventing Session Hijacking, http://www.microsoft.com/technet/technetmag/issues/2005/01/SessionHijacking/, veljača 2007.

[3] Rupert Gill, Jason Smith, Andrew Clark: Experiences in Passively Detecting Session Hijacking Attacks in IEEE 802.11 Networks, Fourth Australasian Information Security Workshop, 2006.

[4] Session Hijacking, http://www.imperva.com/application_defense_center/glossary/session_hijacking.html, veljača 2007.

[5] Andrew Jaquith: The Security of Applications: Not All Are Created Equal, http://www.securitymanagement.com/library/atstake_tech0502.pdf, veljača 2007.