SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE ZNANOSTI
Ak. god. 2016./2017.

Dino Smrekar

Zaštita osobnih podataka na internetu

diplomski rad

mentor – dr. sc. Vjera Lopina

Zagreb, 2017.

Sadržaj

Uvod ... 1
1. Privatnost vs. sigurnost ... 2
2. Sigurnost u kućnom vs. u poslovnom okruženju ... 3
3. Stvaranje sigurne podloge ... 5
3.1. Softver i hardver ... 6
3.1.1. Operacijski sustavi ... 7
3.1.2. Live USB i live CD sustavi, Tails ... 8
3.1.3. Sandboxing ... 10
3.1.4. Antivirusni programi i vatrozidovi ... 11
3.2. Zaporke ... 13
3.2.1. Alati za čuvanje zaporki ... 14
3.3. Enkripcija podataka ... 15
3.3.1. PGP ... 17
3.3.2. DES ... 19
3.3.3. AES ... 22
3.4. Bežične mreže ... 24
3.4.1. VPN ... 26
3.4.2. Tor ... 27
4. Internetske usluge i njihovi rizici ... 29
4.1. Google ... 30
4.2. Usluge za online kupovinu ... 31
4.3. Društvene mreže ... 32
4.4. SSL, TLS i HTTPS protokoli ... 34
4.5. Pohrana podataka na internetu ... 35
4.5.1. Zadržavanje podataka ... 36
5. Načini online plaćanja ... 37
5.1. Kreditne kartice ... 37
5.2. Internetsko bankarstvo ... 38
5.3. Paypal i slični ... 40
5.4. Kriptovalute kao alternativni način plaćanja ... 41
6. Sigurnosni rizici ... 44
6.1. Socijalni inženjering, phishing i spam ... 44
6.2. Klasični virusi i ransomware ... 46
6.3. Javna računala ... 48

7. GDPR regulativa 49
Zaključak 51
Literatura 52
Sažetak 57

Uvod

Internet nam omogućuje pristup raznim sadržajima i uslugama bez potrebe napuštanja naših domova. Usluge poput online naručivanja, iznajmljivanja filmova ili internetskog bankarstva pojednostavljuju našu svakodnevicu i pružaju nam mogućnost znatne uštede vremena. Uvjet korištenja koji je pristupu tim uslugama zajedničkii u velikom broju slučajeva potreban su naravno, naši osobni podaci. Većina usluga zahtijeva naše osobne podatke, od minimuma poput imena i prezimena ili datuma rođenja i kućne adrese pa sve do izrazito osjetljivih podataka poput brojeva kreditnih kartica, preslika osobnih dokumenata i sličnog. Kako samim pristupanjem tim uslugama naše podatke šaljemo trećim stranama, od izrazite je važnosti što bolje osigurati se od neželjenih krađa ili curenja informacija.

Naravno, sigurnost naših osobnih podataka nije samo na nama, već i velikim dijelom na pružateljima usluga koji su obvezni pobrinuti se za to da naši podaci ne završe u krivim rukama. Postoje razni načini na koje nas pružatelji tih usluga mogu zaštititi, kao i mi sami, a svode se većim dijelu na prevenciju i inteligentne navike poput redovitog mijenjanja zaporki, uporabe enkripcije, izbjegavanja rizičnih stranica i korištenja zdravog razuma.

Rad će obuhvatiti sve vezano uz zaštitu osobnih podataka, većim dijelom u kućnom okruženju i pri korištenju online usluga, no spomenut ćemo i zaštitu podataka (dakako ne osobnih, iako po osjetljivosti na toj razini, a možda čak i kritičnijoj) u poslovnom okruženju.

Osvrnuti ćemo se na načine zaštite od prijetnji, ali i na same prijetnje kako bi imali kompletnu sliku o situaciji.

1. Privatnost vs. sigurnost

Važno je precizirati što je to privatnost, a što sigurnost. Ta dva pojma usko su povezana i u međusobnom odnosu. Kada pričamo o privatnosti, obično mislimo na čuvanje naših osobnih podataka od neželjenih promatrača - bilo to većim dijelom javne informacije o nama poput datuma rođenja, gdje smo se školovali, javne fotografije koje dijelimo na društvenim mrežama i slično ili osjetljiviji podaci poput bankovnih računa i ostaloga.
Ti podaci su samim stavljanjem na mrežu u poziciji gdje su ugroženi i gdje ne postoji 100% šansa da budemo sigurni u očuvanje njihove privatnosti.
Privatnost nije crno-bijela, već postoji više razina. Svima nam je poznato kako postavke za privatnost na društvenim mrežama omogućuju da odredimo kome će naši sadržaji biti dostupni, kao i činjenica da kada stvaramo račune na internetu u većini slučajeva pristajemo na uvjete korištenja tih usluga i pružatelju tih usluga dopuštamo baratanje našim podacima prema tim uvjetima. Očuvanje privatnosti izrazito je važna tema danas, pogotovo kada uzmemo u obzir da se velika većina internetskih usluga koje su besplatne financiraju na temelju pohranjivanja naših obrazaca ponašanja i interesa (koji su po mnogima privatna stvar), te pružanja specijaliziranih oglasa koji se temelje na njima, bez obzira na anonimnost prikupljenih podataka koje te stranice zagovaraju. Sigurnost, s druge strane, govori nam koliko je nešto (primjerice naši podaci) zaštićeno od pristupa promatrača tj. drugih osoba. Sigurnost je po mom mišljenju crno-bijeli pojam, te ima dvije krajnosti, onu gdje su naši podaci sigurni i onu gdje su kompromitirani. Za primjer bih uzeo društvene usluge gdje privatnost igra daleko veću ulogu zbog nijansi u kojima određujemo pristup podataka, dok kod sigurnosti možemo kao primjer uzeti usluge e-bankarstva ili online pohranjivanja osobnih podataka gdje nema nijansiranog pristupa već tim podacima pristupamo isključivo mi.

2. Sigurnost u kućnom vs. u poslovnom okruženju

Postoji velik broj razlika između sigurnosti u kućnom i sigurnosti u poslovnom okruženju. Ključna stvar u kojoj se razlikuju je dakako ta da u kućnom okruženju ne podliježemo nikakvim pravilima, tj. uvjetima kojih se moramo pridržavati kako bi osigurali podatke, dok u poslovnom okruženju većina tvrtki pridaje izrazito veliku važnost te određuje pravila i protokole kojih se zaposlenici moraju držati kako bi se osigurao integritet podataka.

Sljedeće statistike iz američkog istraživanja sigurnosti u poslovnom okruženju govore kakva je situacija i tko su najslabije karike u zaštiti podataka: „Preko osamdeset posto tvrtki tvrdi da je njihova najveća prijetnja sigurnosti nemar krajnjeg korisnika. Sedamdeset i pet posto tvrtki isto tako vjeruje da je nemar zaposlenika njihova najveća prijetnja sigurnosti. Tri posto svih američkih zaposlenika priznalo je da koristi isti set zaporki za online potrebe. Trećina ovog postotka je priznala da koristi čak manje od pet različitih zaporki za pristup između dvadeset i pet i pedeset web stranica, od kojih su neke poslovne i profesionalne stranice. Preko trideset i tri posto američkih tvrtki nema sigurnosni plan za unutarnje sigurnosne rizike, što znači da je osobna odgovornost najveći rizik u velikoj većini tih slučajeva.“[1]

[1]Promoting data securityintheworkplace. UAB. 2017.
URL: http://businessdegrees.uab.edu/resources/infographics/promoting-data-security-in-the-workplace/ (25.9.2017)

Slika 1. Osnovni faktori politike postupanja **s** podacima [2]

[2]9 KeyElementsof a Data SecurityPolicy. Travelers. 2017.
URL: https://www.travelers.com/resources/cyber-security/9-elements-of-a-data-security-policy.aspx (25.9.2017)

3. Stvaranje sigurne podloge

Od presudne važnosti je postavljanje osnovnih mjera sigurnosti i načina ponašanja kojih ćemo se držati kada baratamo s osjetljivim podacima, bilo to u kućnom ili poslovnom okruženju. Nabrojati ćemo najveće rizike, tj. radnje koje bi se trebale izbjegavati, te ih ukratko opisati:

1. Dijeljenje zaporki s drugima
2. Korištenje slabih zaporki ili istih zaporki na više različitih mjesta
3. Ostavljanje otključanog računala bez nadzora
4. Korištenje javnih računala
5. Prenošenje osjetljivih podataka na prijenosnim računalima
6. Spajanje na nezaštićene i nepoznate bežične mreže
7. Korištenje neprovjerenog softvera i internetskih usluga
8. Posjećivanje sumnjivih stranica na internetu
9. Otvaranje sumnjivih priloga i poveznica na mail porukama
10. Neažuriranje softvera, operacijskog sustava i antivirusnog softvera
11. Nekorištenje enkripcije
12. Neredovito stvaranje sigurnosnih kopija
13. Lažna sigurnost u vlastite informatičke sposobnosti

Pridržavanjem osnovnih mjera sigurnosti, izbjegavanjem navedenih pogrešaka i korištenjem zdravog razuma izbjegavamo izrazito velik broj rizika i brinemo se o sigurnosti osobnih podataka s naše strane. Dakako, to je samo djelić čitave slike i ne garantira nam potpunu sigurnost s obzirom da podatke pri korištenju na internetu stavljamo u tuđe ruke.
Bez obzira na kredibilitet i razinu sigurnosti usluga koje koristimo, pogreške se svugdje mogu omaknuti te nikada nismo 100% sigurni, što nam govore i brojni sigurnosni propusti kod tehnoloških divova poput Applea, Microsofta i raznih drugih kompanija gdje je u prošlosti došlo do curenja korisničkih podataka.

3.1. Softver i hardver

Kao što smo i naveli, izrazito je važna sigurna podloga koju ćemo koristiti za daljnje baratanje osjetljivim podacima. U softver spadaju svi programi koje pokrećemo na računalima, poput operacijskih sustava, internetskih preglednika, antivirusnih programa i ostalog.
Od izrazite je važnosti korištenje provjerenog softvera, te redovito ažuriranje nadogradnjama. Redovito ažuriranje je pogotovo važno kod softvera kojim pristupamo internetu.
Kako se s vremenom pronalaze sigurnosni propusti u svom softveru, najrizičnija skupina su dakako internetski preglednici zbog toga što njih najčešće koristimo i većini usluga pristupamo preko njih. Od zaporki, osobnih poruka i mail poruka, pa sve do bankovnih podataka i drugog, sve unosimo kroz internetske preglednike, čime oni postaju najveća meta kriminalcima. Velika većina ljudi se na to ne obazire, no još jedan izrazito veliki čimbenik sigurnosti internetskog preglednika su proširenja koja na njemu koristimo i kojima pri instalaciji dajemo ovlasti. Kada sve to zbrojimo eksponencijalno povećavamo rizik kojemu se izlažemo što više usluga i programa koristimo.
Pod hardver ubrajamo sve opipljive dijelove, poput računala, tipkovnica, mrežnih uređaja i svega ostalog. Kod te kategorije izrazito je važno osigurati pristup uređajima, te ga ograničiti neovlaštenim osobama, te primjerice u slučaju USB memorija koje koristimo na većem broju računala (od kojih neka mogu biti javna i neprovjerena) uvijek biti na oprezu zbog mogućeg prenošenja zloćudnog softvera.
Jedan od najpoznatijih primjera infekcije putem USB memorije u novije doba je Stuxnet, sofisticirani crv koji je 2010. uzrokovao izrazito veliku štetu iranskom nuklearnom programu te pokazao koliko moćni maliciozni programi zapravo mogu biti.
Nagađa se da iza tog napada stoje SAD i Izrael, te da je to najskuplji maliciozni program ikada proizveden.

3.1.1. Operacijski sustavi

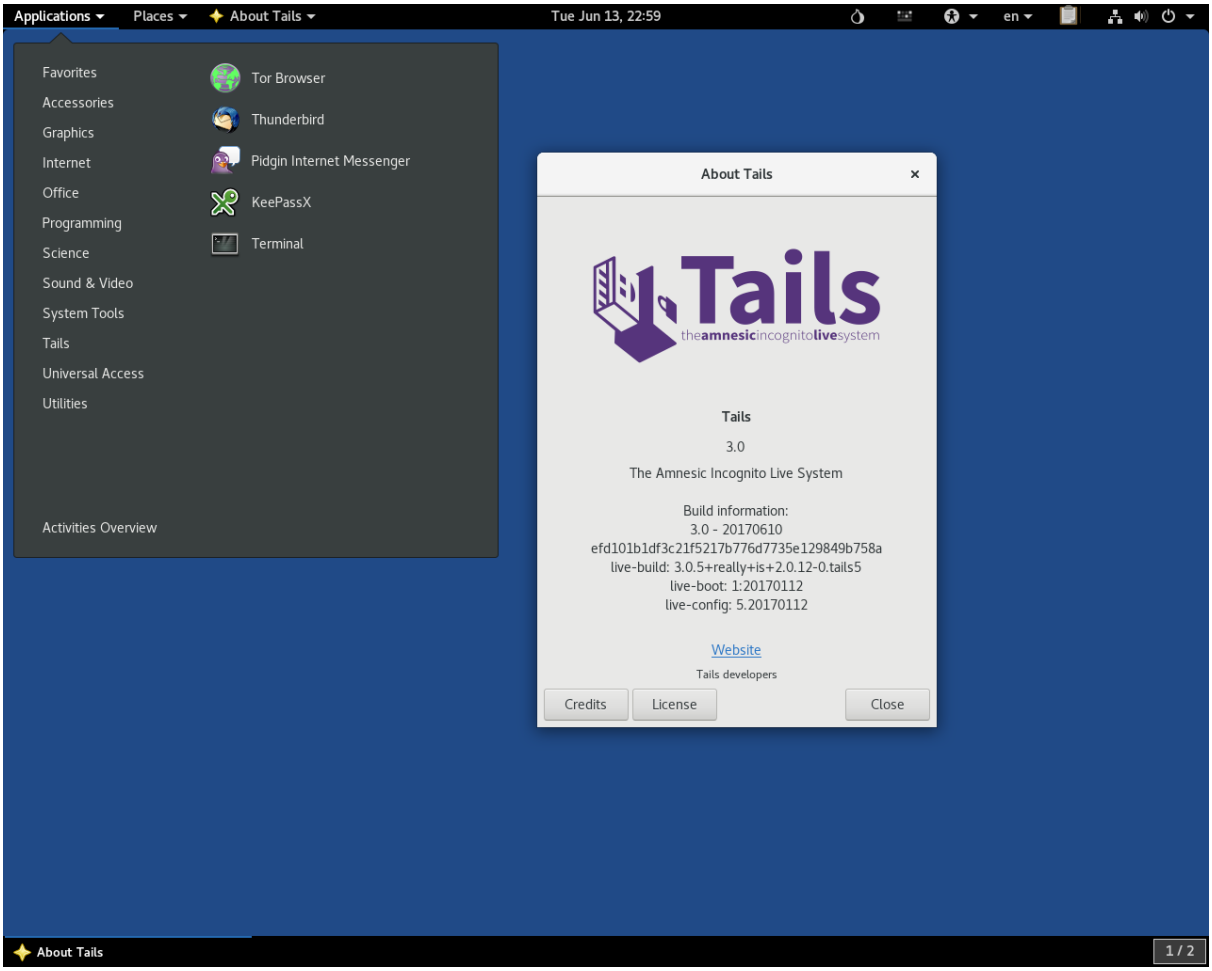
Najvažniji element tj. dio softvera preko kojega sve ostalo pokrećemo je dakako, operacijski sustav. Općenito, kada pričamo o operacijskim sustavima većina ljudi je čula za Linux, Apple macOS i Microsoft Windows. Uvriježeno je mišljenje da je od ta tri operacijska sustava najnesigurniji Windows. To ne znači da je Windows strukturalno nesigurniji od ostala dva i da ga je lakše hakirati, već dolazi od činjenice da je Windows daleko zastupljeniji te je samim time lukrativnije razvijati zloćudne programe za njega i veća je meta digitalnim kriminalcima.
Isto tako je izrazito važno koju verziju operacijskog sustava pokrećemo i da li ju redovito nadograđujemo. Tu dolazimo do ključne razlike između Appleovih i Microsoftovih operacijskih sustava i Linuxa. Ranije verzije Appleovih i Microsoftovih sustava (posebice Windows XP) na kojima su pokretani još uvijek milijuni računala diljem svijeta veliki su problem po pitanju računalne sigurnosti. Kako je za njih prekinuta podrška i sigurnosne zakrpe, nisu više adekvatni sustavi koje bi trebali koristiti u osobne, a kamoli u poslovne svrhe. Linux se po tome razlikuje samim time što je otvorenoga koda i korisnici sami mogu puno lakše uočiti i zatvoriti sigurnosne propuste.
Postoje i drugi operacijski sustavi u novije doba koji dobivaju na popularnosti, poput GoogleovogchromeOSa koji je većim dijelom baziran na Googleovom web pregledniku Chrome, ali prethodna tri koja smo nabrojali su najzastupljeniji.
No, izrazito je važno spomenuti operacijske sustave za mobilne uređaje zbog sve veće popularnosti pametnih telefona.
Tu su dakako AppleoviOS, Microsoftov Windows Mobile koji je u nestajanju zbog nedostatka popularnosti i najzastupljeniji i po mišljenju većine najfleksibilniji, Google Android.
Kao što je to stvar i s operacijskim sustavima za računala, i tu je najugroženiji Google Android zbog najšire zastupljenosti i otvorenosti sustava po pitanju mogućnosti instalacije neprovjerenih aplikacija. Osim toga, kod mobilnih uređaja veliku ulogu igra i sama činjenica da su prenosivi te ih lagano možemo izgubiti ili nam oni mogu biti ukradeni.

3.1.2. Live USB i live CD sustavi, Tails

Live CD ili live USB sustavi specifični su po tome što operacijski sustav pokrećemo s CD-a ili prijenosnih USB memorija i prijenosnih tvrdih diskova bez potrebe za instalacijom.
U početku su se koristili iz razloga što su nadogradnje za Linux sustave bile česte i većina korisnika je koristila vlastite CD snimače za snimanje operacijskih sustava.
U današnje doba koriste se za razne namjene, od testiranja operacijskih sustava, backupa podataka na sustavima kojima više ne možemo pristupiti te kao portabilni sustavi koje posvuda možemo nositi sa sobom i koristiti ih za siguran pristup uslugama i stranicama.
Razlika između live USB i live CD sustava je u tome što je u slučaju nepostojanja prostora za pohranu live CD sustav isključivo moguće čitati, dok live USB može pohranjivati izmjene na vlastiti prostor za pohranu s kojeg se pokreće. To ujedno utječe i na sigurnost samog sustava te se, kako bi osigurali najveću razinu sigurnosti predlaže live CD.
Jedna od najpoznatijih Linux live distribucija današnjice korištenih u svrhu sigurnosti je Tails. Tails je live sustav kojemu je cilj očuvati našu privatnost i anonimnost. Pomaže nam koristitiinternet anonimno i zaobići cenzuru gotovo bilo gdje i na bilo kojem računalu bez ostavljanja tragova, osim ako mi to suprotno ne odredimo.[3]
Korištenje Tailsa na računalu ne mijenja ili ovisi o postojećem operacijskom sustavu instaliranom na istom. Konfiguriran je s posebnom pažnjom kako ne bi koristio tvrde diskove od računala. Jedini prostor za pohranu koji koristi nalazi se u RAM-u, te se on automatski briše kada računalo ugasimo.[4]
Sustav nudi razne mogućnosti, poput enkripcije USB uređaja s kojih se pokreće te anonimnog pretraživanja Interneta pomoću TOR-a.
Informacija koja ide u prilog Tailsu i dokaz je njegove sigurnosti je ta da ga je koristio te advocira njegovo korištenje najpoznatiji svjetski zviždač, Edward Snowden.[5]

[3]About. Tails. 2017.
URL: https://tails.boum.org/about/index.en.html (25.9.2017)
[4]About. Tails. 2017.
URL: https://tails.boum.org/about/index.en.html (25.9.2017)
[5]Finley, Klint. Out inthe Open: InsidetheOperating System Edward SnowdenUsed to Evadethe NSA. Wired. 2014.
URL: https://www.wired.com/2014/04/tails/ (25.9.2017)

Windows također nudi opciju portabilnog pokretanja u obliku Windows To Go opcije, koja korisnicima poslovnih i edukacijskih verzija omogućuje prenošenje Windows instalacije na prijenosnim medijima, te pokretanje na računalima bez pristupanja internim diskovima za pohranu kako bi osigurali maksimalnu izolaciju.



Slika 2. Live operacijski sustav Tails[6]

[6]DistroWatch.com: Tails. 2017.
URL: http://distrowatch.com/table.php?distribution=tails (25.9.2017)

3.1.3. Sandboxing

Sandboxing (tzv. pokretanje aplikacija u pješčaniku) je strategija softverskog menadžmenta koja izolira aplikacije od kritičnih sistemskih resursa i drugih programa. Pruža dodatni sloj sigurnosti time što sprečava negativni utjecaj malicioznih i zloćudnih aplikacija na sustav.

Bez sandboxinga, aplikacija može imati neograničeni pristup svim sistemskim resursima i korisničkim podacima na računalu. Aplikacija u sandboxu u drugu ruku može pristupiti samo resursima u vlastitom „pješčaniku“ tj. sandboxu. Sandbox aplikacije je ograničena zona skladišnog prostora i memorije koja sadrži samo resurse potrebne programu. Ukoliko program treba pristupiti resursima ili datotekama van sandboxa, mora dobiti eksplicitno dopuštenje od sustava.[7]

Tehnologija sandboxinga prisutna je na stolnim računalima u obliku softverskih rješenja koja potpuno emuliraju čitave operacijske sustave u obliku tzv. virtualnih strojeva poput Oracle VirtuaBoxa i virtualizacijskih rješenja tvrtke VMware koje se koriste za poslovne svrhe ali i za osobnu uporabu poput primjerice pokretanja Windows operacijskog sustava unutar macOS okruženja.

Za razliku od prethodno navedenih virtualizacijskih alata koji emuliraju čitave sustave, postoje i sandbox alati poput aplikacije Sandboxie, koja pokreće aplikacije u odvojenim „kontejnerima“ kako oni ne bi mogli zapisivati na tvrdi disk i utjecati na korisničke podatke.

Korištenjem primjerice web-preglednika ili e-mail programa unutar sandboxa time znatno ograničavamo utjecaj malicioznih programa, jer će se ograničiti njihovo širenje u slučaju pokretanja.

Sandboxing u prošlosti nije bio implementiran u operacijskim sustavima nego su korisnici trebali preuzimati zasebne programe, no moderne verzije Windowsa i macOS-a imaju određene vrste implementacije, primjerice za aplikacije preuzete sa tržnica na tim operacijskim sustavima. Novije verzije web-preglednika isto tako koriste tehnologiju kako bi minimizirali štetu u slučaju malicioznih programa.

Moguće je da su trend započele moderne mobilne platforme koje po zadanom pokreću aplikacije u sandbox okruženju s obzirom na rastuću popularnost pametnih telefona i sukladno tome malicioznih programa za njih.

[7]SandboxingDefinition. TechTerms. 2016.
URL: https://techterms.com/definition/sandboxing (25.9.2017)

3.1.4. Antivirusni programi i vatrozidovi

Poslije sigurnosnih zakrpa najkritičniji dio softvera koji se brine za računalnu sigurnost su dakako antivirusni programi i vatrozidovi.

Antivirusni programi su klasa programa dizajnirana za sprečavanje, detektiranje i uklanjanje malicioznih infekcija na pojedinačnim računalima, mrežama i IT sustavima.

Ti programi, originalno dizajnirani za detekciju i uklanjanje virusa sa računala, također mogu štititi protiv širokog spektra opasnosti, uključujući drugih vrsta malicioznih programa, poput keyloggera, programa koji preuzimaju kontrolu nad preglednikom, trojanskih konja, crva, špijunskih alata, adwarea, botnet mreža i ucjenjivačkog softvera.[8]

Dijele se u više vrsta, od pojedinačnih antivirusnih programa pa sve do potpunih sigurnosnih rješenja koja integriraju funkcije poput vatrozidova, kontrola privatnosti, dodataka za preglednike i alata za pohranu zaporki.

Postoje besplatna i komercijalna rješenja, a razlikuju se po broju mogućnosti i efikasnosti kojom nas štite od sigurnosnih prijetnji.

Dostupni su za sve sustave, od Windowsa koji su najveća meta za zlućudni softver, macOSa i ostalih operacijskih sustava za stolna računala pa sve do mobilnih operacijskih sustava poput Androida koji je po pitanju ugroženosti usporediv s Windowsima zbog svoje široke zastupljenosti, te drugih.

Antivirusni programi uobičajeno se pokreću kao pozadinski proces, skeniraju računala, servere ili mobilne uređaje kako bi detektirali i ograničili širenje zlućudnog softvera. Mnogi antivirusni programi uključuju zaštitu u stvarnom vremenu kako bi štitili od potencijalnih ranjivosti u trenutku kada se one događaju, kao i sistemske skenove koji nadgledaju datoteke uređaja i sustava u potrazi za potencijalnim rizicima.[9]

Koriste više vrsta tehnika kojima pristupaju detekciji prijetnji:

Na temelju potpisa – svaki zlućudni program ima jedinstveni potpis.

Ta tehnika je bila korištena u začecima antivirusnih programa i uvelike je ovisila o redovito ažuriranoj bazi potpisa, te se u današnje vrijeme koristi tek kao mali dio zaštite od postojećih prijetnji s obzirom da nije sposobna detektirati nove.

---

[8]Rouse, Margaret. antivirus software (antivirus program). WhatIs. 2014.
URL: http://searchsecurity.techtarget.com/definition/antivirus-software (25.9.2017)

[9]Rouse, Margaret. antivirus software (antivirus program). WhatIs. 2014.
URL: http://searchsecurity.techtarget.com/definition/antivirus-software (25.9.2017)

Na temelju heuristike – uspoređuju se potpisi postojećih virusa sa novim, nepoznatim prijetnjama kako bi se detektirali novi, ili postojeći prerušeni u nove.

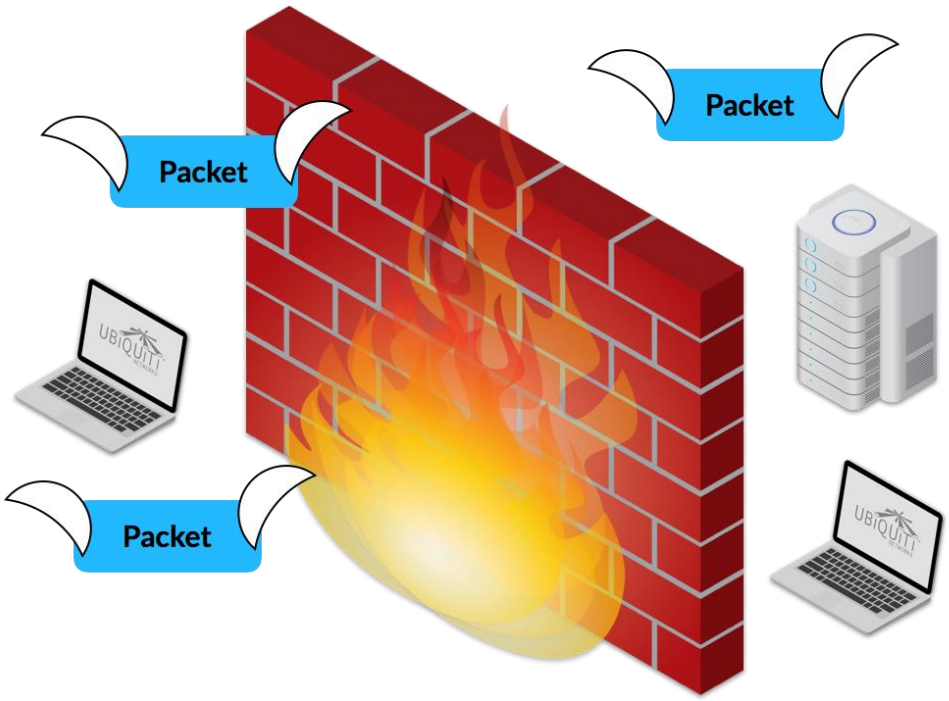
Na temelju ponašanja – kao što sam naziv govori, detektiraju prijetnje na temelju sumnjivog ponašanja, poput modificiranja sistemskih datoteka, brisanja korisničkih podataka i drugih radnji koje nisu uobičajene.

Dok je prva metoda većim dijelom pouzdana s obzirom da su prijetnje unaprijed utvrđene, druge dvije nisu potpuno precizne zbog lažnih dojava koje mogu izazvati programi koji se ponašaju poput malicioznih (primjerice alata za backup i modifikaciju sistemskih datoteka).

Druga vrsta programa za sigurnost koji se mogu pronaći u kombinaciji s antivirusnim ili kao samostojeći su vatrozidovi.

Vatrozid je mrežni sigurnosni sustav koji nadzire dolazeći i izlazeći mrežni promet i odlučuje da li će dopustiti ili blokirati određeni promet na temelju definiranog seta sigurnosnih pravila.

Vatrozidovi su prva linija obrane u mrežnoj sigurnosti više od 25 godina. Stvaraju barijeru između osiguranih i kontroliranih unutrašnjih mreža koje su pouzdane i nepouzdanih vanjskih mreža, poput interneta. Mogu biti hardverski, programski ili oboje.[10]



Slika 3. Ilustracija principa po kojem vatrozid funkcionira[11]

[10]WhatIs a Firewall? Cisco. 2017.
URL: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (25.9.2017)
[11]Intro to Networking - Network FirewallSecurity. UBNT Support. 2017.
URL: https://help.ubnt.com/hc/en-us/articles/115006615247-Intro-to-Networking-Network-Firewall-Security (25.9.2017)

3.2. Zaporke

Nekad u obliku skraćenice PWD, lozinka ili zaporka skup je tajnih znakova ili riječi korištenih kako bi pristupili računalu, web stranici, mrežnom resursu ili podacima. Zaporke pomažu u osiguravanju pristupa računalima ili podacima samo onima koji imaju pravo na pristup.[12]

Kako u moderno doba većini usluga na internetu pristupamo putem korisničkog računa u koji se prijavljujemo pomoću korisničkog imena ili e-mail adrese i zaporke, od izrazite važnosti je inteligentna primjena zaporki. S obzirom na velik broj računa kojima korisnici svakodnevno barataju, čest slučaj je korištenje jednostavnih zaporki, korištenje široko dostupnih informacija poput datuma rođenja ili imena i možda najveći problem, višestruko korištenje istih zaporki.

Prema istraživanju koje je provela kompanija KeeperSecurity koja razvija alate za čuvanje zaporki, statistike su izrazito zabrinjavajuće.

Najpopularnija zaporka, koja čini gotovo 17 posto svih 10 milijuna zaporki koje je kompanija analizirala je zaporka „123456“. „Password“ je također u top 10 zaporki, na 8. mjestu najučestalijih. KeeperSecurity je listu složio pomoću kolekcije zaporki koje su procurile tijekom povreda sigurnosti u 2016. godini. Top 25 zaporki čine preko 50% od svih 10 milijuna zaporki koje su bile analizirane.[13]

Upravo ta činjenica da su sve zaporke sakupljene iz kolekcije koja je sačinjena od prethodnih curenja podataka govori u prilog korištenju zasebnih zaporki za svaku uslugu koju koristimo s obzirom da na taj način dobivene zaporke elektronski kriminalci mogu ponovno upotrebljavati u obliku „rječnika“ kako bi pristupili drugim korisničkim računima koji koriste iste zaporke.

Osim metode rječnika, zaporke kriminalci mogu pokušati odgonetnuti pomoću tzv. „BruteForce“ metode koja se bazira na generiranju velikog broja zaporki kojima se zatim pokušava provaliti u korisnički račun. Te metode također mogu primjenjivati rječnike.

Zbog toga je od velike važnosti korištenje dužih nasumičnih zaporki s obzirom da se metoda oslanja na generiranje kombinacija znakova, a što veću kombinaciju nasumičnih znakova

[12]Whatis a Password. Computer Hope. 2017.
URL: https://www.computerhope.com/jargon/p/password.htm (25.9.2017)
[13]The Most CommonPasswordsof 2016. KeeperSecurity. 2016.
URL: https://keepersecurity.com/public/Most-Common-Passwords-of-2016-Keeper-Security-Study.pdf (25.9.2017)

korisnici koriste to će biti manja šansa da se ona odgonetne tj. metodi će trebati nerealno velik vremenski okvir ovisno o moći procesuiranja (stoljeća pri kompleksnijim zaporkama).
Mjerilo kojim određujemo koliko je zaporka nepredvidiva nazivamo entropijom zaporke.
Temelji se na setu znakova koji koristimo (koji se proširuje korištenjem malih slova, velikih slova, brojeva i simbola) kao i duljinom zaporke. Entropija zaporke predviđa koliko je teško probiti određenu zaporku pogađanjem, „bruteforce“ napadom, napadima rječnikom i drugim učestalim metodama.
Entropija zaporke uobičajeno se mjeri u bitovima; Zaporka koja je već poznata ima 0 bitova entropije; ona koju bi pogodili iz prvog pokušaja polovicu vremena imala bi 1 bit entropije. Entropija zaporke može se izračunati na način da pronađemo entropiju po znaku, koja je logaritam baze 2 broja znakova u setu znakova koji smo koristili, pomnožen brojem znakova u samoj zaporki.[14]

3.2.1. Alati za čuvanje zaporki

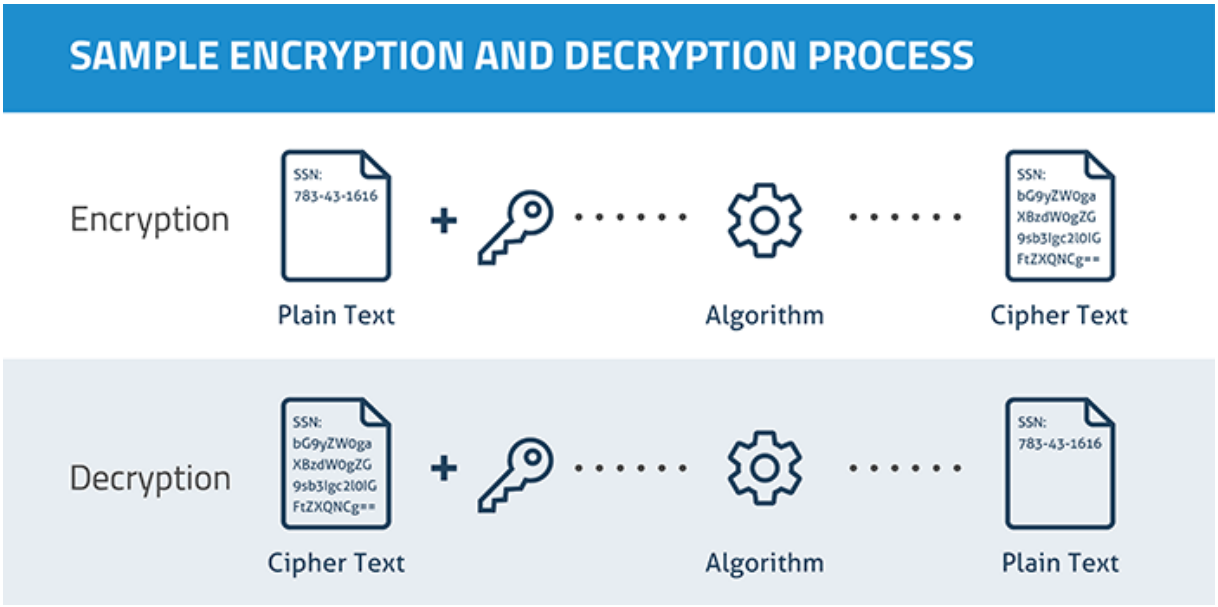
Nakon što za svaki račun napravimo kompleksnu zaporku koju će teško koji napadač pogoditi, dolazimo do problema gdje i kako tu zaporku pohraniti s obzirom da će rijetko tko zapamtiti velik broj nasumično generiranih znakova.
Način na koji možemo izbjeći pamćenje bezbroj navedenih zaporki, korištenje je alata za pohranu zaporki. Funkcioniraju na temelju enkriptirane datoteke u kojoj su najčešće u tekstualnom obliku pohranjene sve zaporke koje je korisnik unio.
Njoj se pristupa putem specijaliziranog programa unošenjem glavne zaporke, datoteke ključa ili kombinacijom obaju čime dobivamo pristup svim pohranjenim zaporkama.
Alati za čuvanje zaporki dostupnim su u raznim varijantama, besplatnim i komercijalnim, online i offline te su dostupni na svim popularnim operacijskim sustavima, bilo za osobna računala ili za mobilne uređaje.
Najpoznatiji alati za tu namjenu su program/usluga LastPass koji uključuje online skladištenje enkriptirane datoteke i program otvorenog koda KeePass, koji zaporke skladišti lokalno.
Oba alata zastupljena su na velikom broju platformi.

[14]Rouse, Margaret. Whatis password entropy? WhatIs. 2014.
URL: http://whatis.techtarget.com/definition/password-entropy (25.9.2017)

3.3. Enkripcija podataka

Enkripcija je konverzija elektroničkih podataka u drugi oblik, zvan šifrirani tekst, koji nije lako razumljiv ikome osim autoriziranih osoba. Primarna svrha enkripcije je zaštititi povjerljivost digitalnih podataka pohranjenih na računalnim sustavima ili prenošenih preko Interneta ili drugih računalnih mreža.[15]Enkripcija je bazirana na kriptografiji i ima dva tipa - javna i simetrična. Kod javne koriste se dva različita "ključa", jedan javni i jedan privatni.
Onaj javni dostupan je svima, ali samo uz privatni se može "otključati" informacija. Primjerice, ako šaljete e-mail poruku, koristite "privatni ključ" za enkripciju i potom te informacije putuju "javnim prostorom", ali do sadržaja informacije može se samo uz posjedovanje "privatnog ključa". Često korišteni primjeri su RSA algoritam, digitalni potpisi, VPN, SSL/TLS i program PGP... Današnje metode bazirane su na problemima gdje se brzo i jednostavno pomoću računala tekst šifrira ali je rješenje "teško", u matematičnom smislu.
Simetrična enkripcija je takva da pošiljatelj i primatelj koriste isti ključ za enkripciju, što uvelike pojednostavljuje cijeli proces, ali ga i čini bržim. Kao i nesigurnijim jer ako se presretne, moguće je "provaliti" u njega. Tip simetričnog ključa bio je DES (Data Encryption Standard), kojeg je kasnije zamijenio moderniji AES (Advanced Encryption Standard).[16]
Enkripcija se dugo već koristi od strane vojska i vladi kako bi omogućila tajnu komunikaciju. U današnje doba koristi se za zaštitu podataka unutar brojnih civilnih sustava, poput računala, mreža (primjerice Internetska prodaja), moblinih telefona, bežičnih mikrofona, bežičnih portafona, bluetooth uređaja i bankomata. Enkripcija se također koristi kod upravljanja digitalnim pravima kako bi ograničila uporabu materijala zaštićenog autorskim pravima i u zaštiti od reprodukcije softvera kako bi štitila od obrnutog inženjeringa i softverskog piratstva.[17]

[15]Rouse, Margaret. Whatisencryption? WhatIs. 2014.
URL: http://searchsecurity.techtarget.com/definition/encryption (25.9.2017)
[16]Deželić, Vanja. Što je enkripcija i zašto je bitna. ICT Business. 2017.
URL: http://www.ictbusiness.info/internet/sto-je-enkripcija-i-zasto-je-bitna (25.9.2017)
[17] Encryption. New World Encyclopedia. 2013.
URL: http://www.newworldencyclopedia.org/entry/Encryption (25.9.2017)



Slika 4. Primjer procesa enkripcije i dekripcije[18]

Slika 5. Enigma, njemački stroj za šifriranje i dešifriranje poruka u Drugom svjetskom ratu[19]

[18]Tokenization vs Encryption. Skyhigh. 2017.
URL: https://www.skyhighnetworks.com/cloud-security-university/tokenization-vs-encryption/ (25.9.2017)
[19]Lycett, Andrew. Enigma. BBC History. 2017.
URL: http://www.bbc.co.uk/history/topics/enigma (25.9.2017)

3.3.1. PGP

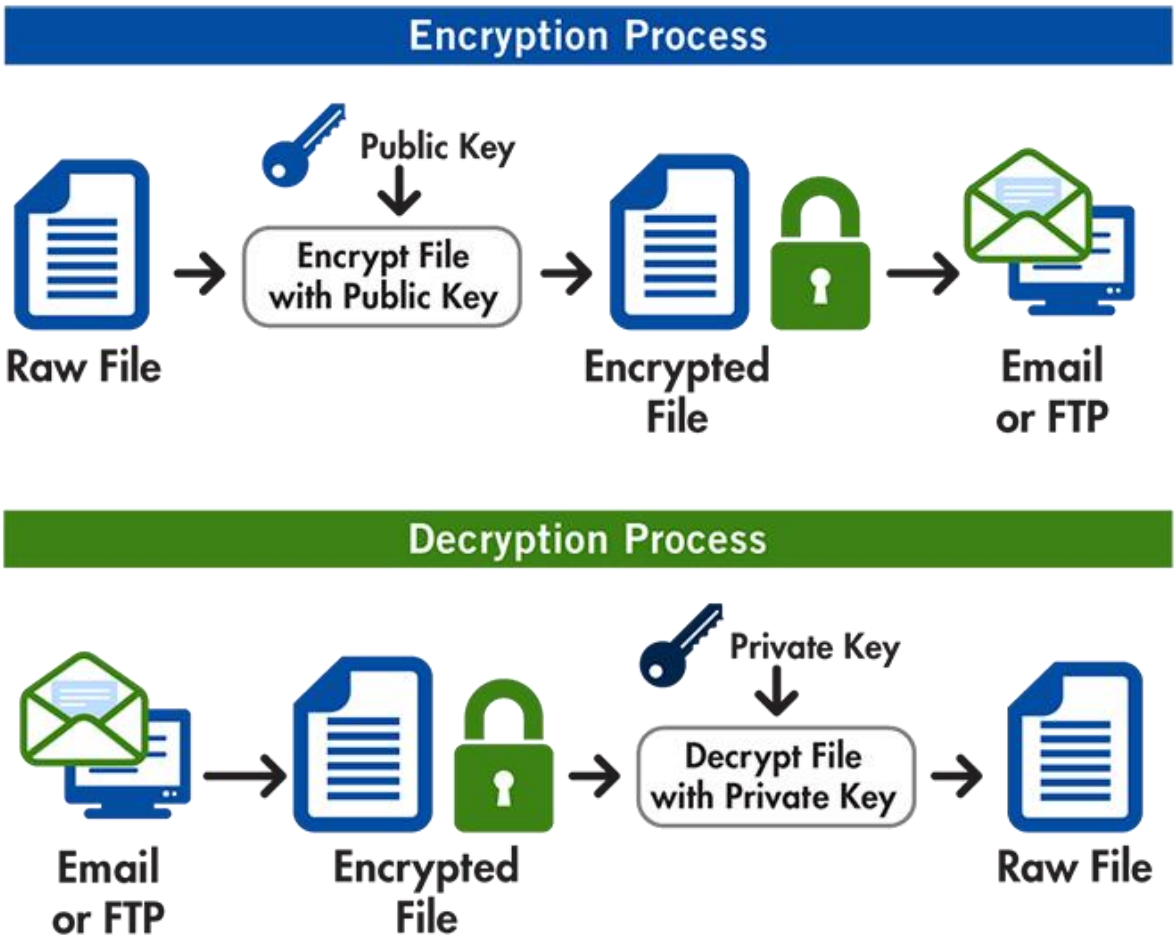
PGP (PrettyGoodPrivacy) je računalni program za kriptografsku zaštitu podataka koji je još davne 1991. godine razvio PhilZimmermann. Iako program s tim nazivom i namjenom još uvijek postoji, PGP je zbog svoje raširenosti među korisnicima u međuvremenu postao otvoreni standard pod imenom OpenPGP.[20]

PGP kombinira najbolje značajke klasične i kriptografije s javnim ključem.

On je hibridni kriptosustav. Kada korisnik nešifrirani tekst enkriptira s PGP-om, PGP prvo komprimira nešifrirani tekst. Kompresija podataka skraćuje vrijeme prijenosa i diskovni prostor i što je najvažnije, jača kriptografsku sigurnost. Većina tehnika kriptoanalize iskorištava uzorke pronađene u nešifriranom tekstu kako bi probilo šifru. Kompresija smanjuje broj tih uzoraka u nešifriranom tekstu, i time znatno poboljšava otpornost na kriptoanalizu. PGP zatim stvara sesijski ključ, koji je jednokratni tajni ključ. Taj ključ je nasumični broj generiran iz nasumičnih kretnji našeg miša i pritisaka na tipke koje unosimo. Sesijski ključ radi u kombinaciji s izrazito sigurnim, brzim klasičnim algoritmom za enkripciju kako bi zaključao nešifrirani tekst, pretvarajući ga u šifrirani. Kada se podaci enkriptiraju, sesijski ključ se enkriptira na javni ključ primatelja. Ovaj javni ključ – enkriptirani sesijski ključ se prenosi zajedno s šifriranim tekstom primatelju.[21]

PGP najčešće koristimo u e-mail prometu kako bi enkriptirali poruke i time ih zaštitili od neželjenih promatrača. On je samo dodatna mjera sigurnosti koju možemo implementirati kako bi zaštitili privatnost i osigurali siguran komunikacijski kanal, a dodatno nas štiti u slučaju kada je sigurnost narušena kod treće strane (primjerice pružatelja e-mail usluga) na način da bi napadač pri pristupu našim podacima, tj. porukama vidio niz nasumičnih znakova bez posebnog značenja. Osim u svrhu zaštite privatnosti osobnih korisnika, koristi se i u vojne te kriminalne svrhe poput špijunaže ili planiranja terorističkih napada, kako bi onemogućio čitanje osjetljivih podataka koji bi mogli izdati korisnike ili njihove namjere.

[20]PrettyGoodPrivacy (PGP). Nacionalni CERT. 2016.
URL: http://www.cert.hr/pgp (25.9.2017)
[21]How PGP works. Introduction to Cryptography. 1999.
URL: https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html (25.9.2017)



Slika 6. Ilustracija procesa enkripcije i dekripcijeunutar PGP-a[22]

[22]Open PGP. GoAnywhere MFT. 2017.
URL: https://www.goanywhere.com/managed-file-transfer/encryption/open-pgp (25.9.2017)

3.3.2. DES

DataEncryption Standard ili DES je standardna blok šifra razvijena od strane IBM-a koja se temelji na Feistel mreži korištenoj u velikom broju mrežnih aplikacija.[23]

Ukratko o Feistel mreži – ona je simetrična struktura koju koristimo u konstrukciji blok šifri, nazvana po njemačkom fizičaru i kriptografu HorstuFeistelu koji se bavio istraživanjem dok je radio za IBM u SAD-u.[24]Objavljen je 1975. za analizu, a kao standardni federalni algoritam u SAD bio je izabran 1976. godine i koristio se sve do pojave AES-a, 2001. godine, tj. njegove implementacije 2002. godine.[25]Iako je zastario i naslijedio ga je standard AES, važno je spomenuti DES kao uvod u blok šifre, s obzirom da dobro razumijevanje standarda AES započinje s dobrim razumijevanjem standarda DES.

Koristeći binarni ključ duljine bloka od 56 bita, DES enkriptira binarni nešifrirani blok teksta duljine bloka od 64 bita u binarni šifrirani blok teksta duljine bloka od 64 bita.

56-bitni ključ se produljuje na 64 bita za pohranu i distribuciju tako da se nakon svakih 7 bitova ključa umeće bit provjere, čime se unutar ključa može detektirati greška od jednog bita u svakom setu od 8 bita.[26]

Postoji 3 enkripcijska moda unutar DES-a - Electronic CodeBook (ECB) mod – kada svaki blok od 64 bita enkriptiramo pojedinačno, te ChainBlockCoding (CBC) iCipherFeedback (CFB) gdje svaki blok šifre ovisi o svim prethodnim blokovima poruke putem XOR šifre.[27]

---

[23]Blahut, Richard E. CryptographyandSecureCommunication. Google Knjige. 2014.
URL:
https://books.google.hr/books?id=MMH2AgAAQBAJ&pg=PA170&dq=des+encryption&hl=hr&sa=X&ved=0ahUKEwiu2a3GpcDWAhVGMBoKHYXPCCsQ6AEIVTAG#v=onepage&q=des%20encryption&f=false
(25.9.2017)

[24]Data Encryption Standard. 2013.
URL: http://www.umsl.edu/~siegelj/information_theory/projects/des.netau.net/Dataencryptionstandard.html
(25.9.2017)

[25]EncryptionTimeline. EncryptionPolicy. 2010.
URL: https://www.unc.edu/courses/2010spring/law/357c/001/EncryptionPolicy/HistoryEncryption.html
(25.9.2017)

[26]Blahut, Richard E. CryptographyandSecureCommunication. Google Knjige. 2014.
URL:
https://books.google.hr/books?id=MMH2AgAAQBAJ&pg=PA170&dq=des+encryption&hl=hr&sa=X&ved=0ahUKEwiu2a3GpcDWAhVGMBoKHYXPCCsQ6AEIVTAG#v=onepage&q=des%20encryption&f=false
(25.9.2017)

[27]Grabbe, J. Orlin. The DES AlgorithmIllustrated. 2006.
URL: http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm (25.9.2017)

Već se je u početku smatralo da standard sam po sebi nije dovoljno jak za naprednu primjenu poput vlada i vojske zbog mogućnosti „bruteforce“ napada koji bi uz dovoljno komputacijske moći mogao odgonetnuti ključ.

Godine 1998., dokazana je mogućnost probijanja DES-a kada je tim pod vodstvom Johna Gilmorea iz EFF-a sastavio stroj od 220 tisuća dolara koji je šifru uspio probiti u 56 sati.

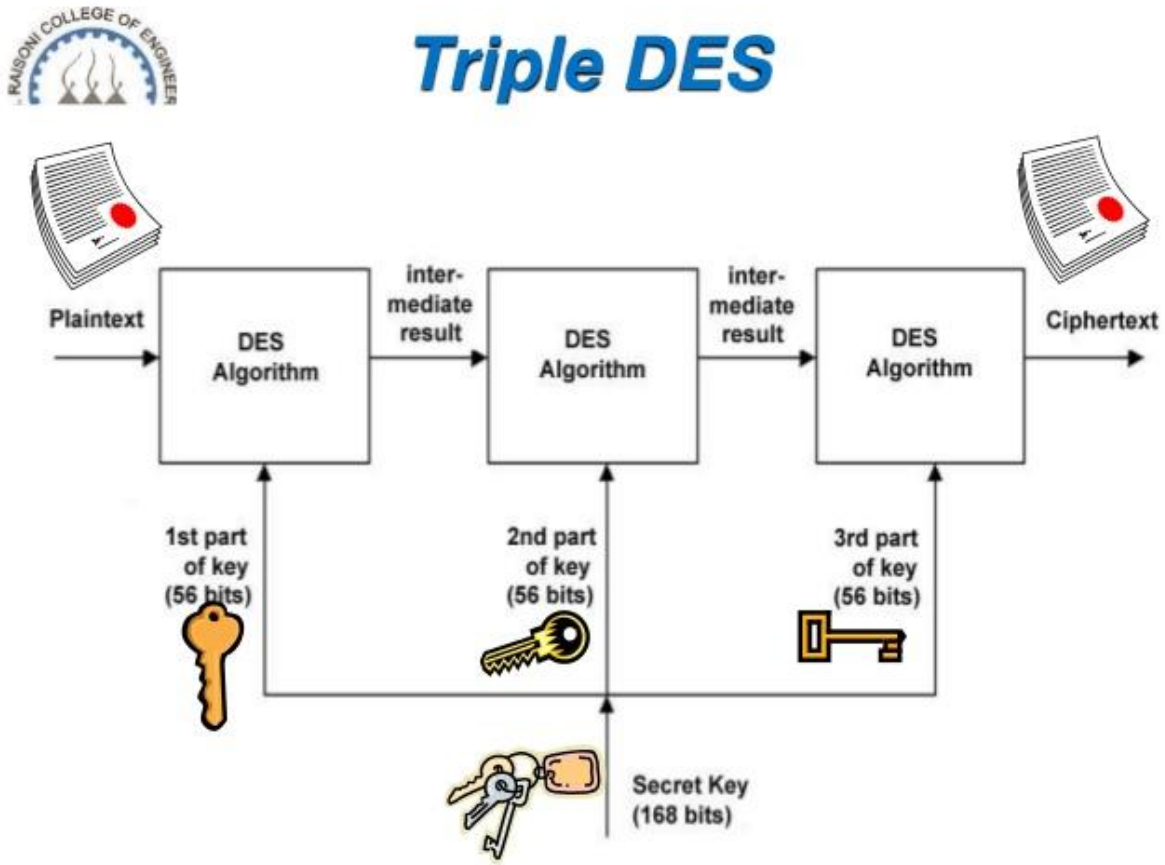
Računalo se zvalo DeepCrack i bilo je sastavljeno od 27 ploča od kojih je svaka imala 64 procesora, te je moglo testirati 90 milijardi ključeva u sekundi.[28]

To je dovelo do korištenja Triple-DES-a - standarda koji je zapravo običan DES, na kojem se primjenjuju dva 56-bitna ključa. Prvi, pri enkripciji, drugi koji se koristi za dekripciju, (iako u ovom slučaju netočni ključ čime se poruka još više ispremeta) te ponovno prvi ključ za treći krug enkripcije.[29]

Dakako, uz veću jačinu ključa, povećano je i vrijeme potrebno za proces enkripcije i dekripcije.

Klasičan DES je povučen iz uporabe 2005. godine, dok je triple-DES odobren za korištenje na osjetljivim vladinim informacijama do 2030. godine.[30]

[28]Grabbe, J. Orlin. The DES AlgorithmIllustrated. 2006.
URL: http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm (25.9.2017)
[29]Grabbe, J. Orlin. The DES AlgorithmIllustrated. 2006.
URL: http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm (25.9.2017)
[30]Rouse, Margaret. WhatisData Encryption Standard(DES). WhatIs. 2014.
URL: http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard (25.9.2017)



Slika 7. Ilustracija procesa enkripcije pomoću triple DES-a[31]

[31]TRIPLE DES Encryption/Decryption Online Tool. Enkosoft. 2017.
URL: https://enko.us/tools/triple-des-encryption-decryption-online-tool/ (25.9.2017)

3.3.3. AES

U siječnju 1997., američki National Institute ofStandardsand Technology (NIST) objavio je početak inicijative za razvoj novog enkripcijskog standarda, AES-a.

Novi enkripcijski standard postao bi FederalInformation Processing Standard (FIPS), čime bi zamijenio stari Data Encryption Standard (DES) i triple-DES.[32]

Za razliku selekcijskog postupka za DES, selekcijski proces za AES bio je otvoren za sve, pri čemu NIST nije analizirao sigurnost i efikasnost prijavljenih kandidata, već je to stavio u ruke kriptografske zajednice i javnosti i samo sakupljao rezultate.

Od 5 kandidata koji su se kvalificirali za detaljniju analizu, pobjedu je na kraju odnio Rijndael, kojeg su razvila dva belgijska kriptografa, JoanDaemen i Vincent Rijmen.

AES sadrži tri blok šifre: AES-128, AES-192 i AES-256. Svaka šifra enkriptira i dekriptira podatke u blokovima od 128 bita koristeći kriptografske ključeve od 128, 192 i 256 bitova.

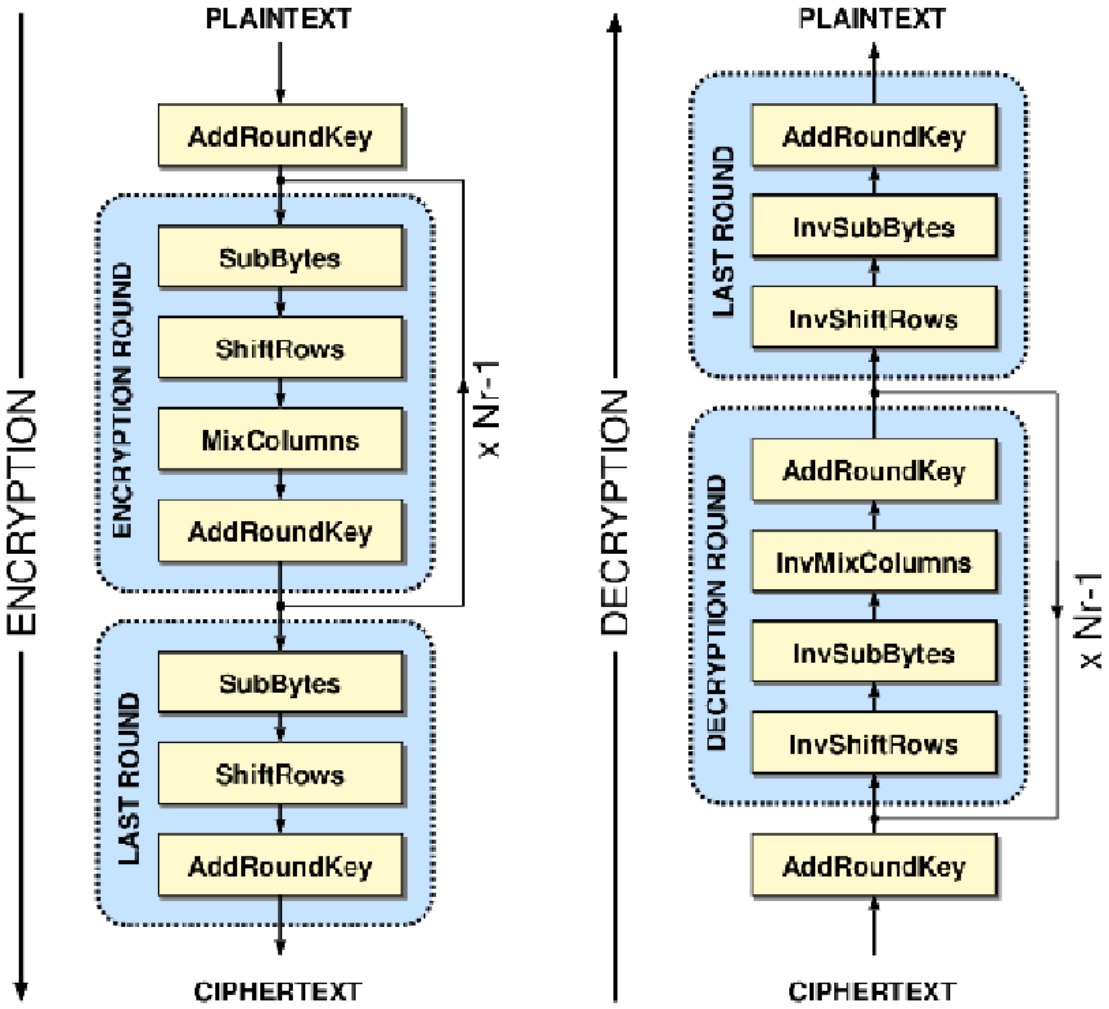
Simetričnog je oblika (poznatije kao tajni-ključ) te koristi isti ključ za enkripciju i dekripciju, tako da pošiljatelj i primatelj moraju znati i koristiti isti tajni ključ.

Sve dužine ključeva se smatraju dostatnima za zaštitu povjerljivih informacija do razine „Povjerljivo“, dok razina „Strogo povjerljivo“ zahtjeva korištenje ključeva dužine 192 ili 256 bita. Koristi se 10 krugova za 128-bitne ključeve, 12 krugova za 192-bitne ključeve i 14 krugova za 256-bitne ključeve – krug se sastoji od nekoliko koraka procesuiranja koji uključuju supstituciju, transpoziciju i miješanje unesenog nešifriranog teksta koji se zatim pretvara u konačni šifrirani tekst.[33]

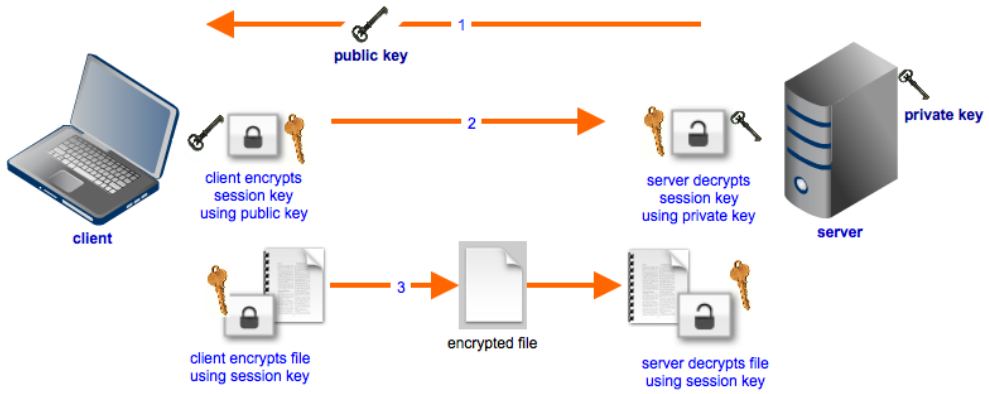
Do danas ne postoji efikasni napad kojim bi se šifra probila u razumnom roku te AES nalazi široku primjenu na internetu, bez obzira da li u osobne ili poslovne svrhe, te se korištenje AES-a savjetuje svima koji podatke žele na dokazan način zaštititi.

[32]Daemen, Joan. Rijmen, Vincent. The Design ofRijndael: AES - The Advanced EncryptionStandard. Google Knjige. 2013.
URL:
https://books.google.hr/books?id=fNaoCAAAQBAJ&printsec=frontcover&dq=aes+encryption&hl=hr&sa=X&ved=0ahUKEwjvv_eRpcDWAhWK2hoKHaufB0YQ6AEILTAB#v=onepage&q=aes%20encryption&f=false (25.9.2017)

[33]Rouse, Margaret. Whatis Advanced Encryption Standard (AES). WhatIs. 2014.
URL: http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard (25.9.2017)



Slika 8. Dizajn AES-a (128 bita) [34]



Slika 9. Ilustracija procesa enkripcije pomoću AES-a [35]

[34]Thebasic AES-128 cryptographicarchitecture. ResearchGate. 2012.
URL: https://www.researchgate.net/figure/230853805_fig1_Figure-1-The-basic-AES-128-cryptographic-architecture (25.9.2017)
[35]Villanueva, John Carl.What AES EncryptionIsAnd How It'sUsed To Secure File Transfers. Jscape. 2015.
URL: http://www.jscape.com/blog/aes-encryption (25.9.2017)

3.4. Bežične mreže

Osim žičanim pristupom, u moderno doba sve je zastupljenije pristupanje internetu putem bežičnih mreža. Bilo kod kuće ili dok šećemo parkom, gotovo u svakom trenutku imamo mogućnost spojiti se na neku bežičnu mrežu. Od izrazite je važnosti pobrinuti se da je mreža sigurna (u slučaju kućnih mreža) ili ukoliko to ne možemo garantirati mi ili pružatelj te mreže (primjerice u kafićima ili na drugim javnim mjestima) pobrinuti se da je naš pristup toj mreži osiguran i adekvatno enkriptiran.

Kada pričamo o osiguravanju bežičnog pristupa, u velikoj mjeri mislimo na lokalnu sigurnost (zaštita rutera i određivanje odgovarajuće jake zaštite bežičnom kanalu).

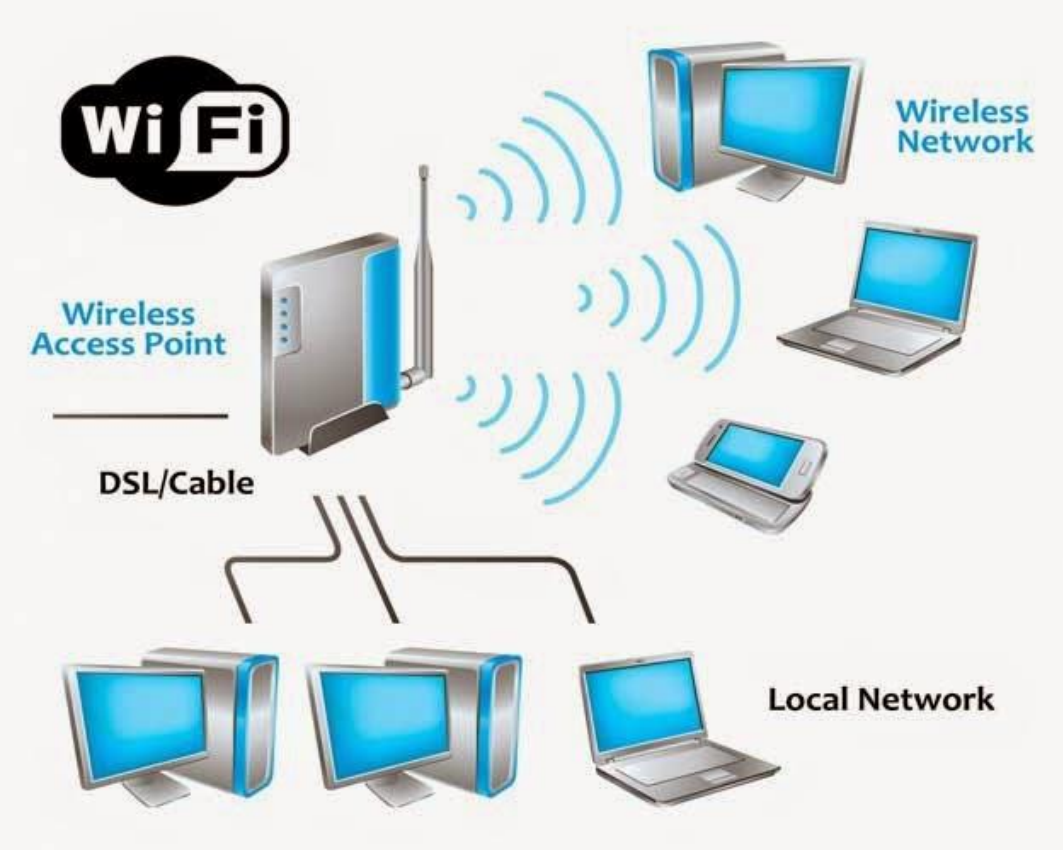
Kod rutera kojeg dobijemo od strane pružatelja internetskih usluga, u velikom broju slučajeva preporuča se postaviti drukčiju zaporku kojom pristupamo ruteru te drukčiju zaporku od one koja je unaprijed zadana, s obzirom da su te zaporke često javno poznate i objavljivane na internetu. Tipovi enkripcije koje možemo koristiti su Wi-Fi Protected Access (WPA) i WiredEquivalentPrivacy (WEP). WEP zaštita, uvedena 1997. godine i postavljena kao standard 1999. godine prvi je oblik enkripcije bežičnih mreža te je uveden u namjeri da se pruži ekvivalentna sigurnost kao i kada bi koristili žičan pristup.Prije korištenja WEP-a pristup bežičnim mrežama bio je gotovo nezaštićen te bi neovlaštena osoba pri spajanju na mrežu imala pristup svim podacima koji su bili u protoku kroz istu s obzirom da oni nisu bili enkriptirani. WEP za šifriranje koristi algoritam RC4 s ključevima dužine 40, 104, 128 ili 256 bita, a zaporke su najčešće u obliku heksadecimalnih vrijednosti brojeva 0-9 i slova A-F i ovisno o dužini ključa sastoje se od 10, 26 ili 58 znamenki.

S obzirom na jednostavnost enkripcije i razne slabosti pri autentifikaciji, WEP je ubrzo proglašen rizičnim za korištenje te je 2004. umirovljen od strane Wi-Fi Alliancea, iako se i dan danas koristi u izrazito velikom broju mreža (najčešće zemljama slabijeg razvoja) s obzirom na nepodržanost na novijim uređajima i neinformiranost korisnika.

WPA ili Wi-Fi Protected Access je nasljednik WEP-a kojemu je cilj korisnicima pružiti znatno veću razinu sigurnosti i ukloniti mane prethodnika.

U upotrebu je stupio 2003. godine kako bi što prije zamijenio WEP, a nadograđena verzija imena WPA2 u upotrebu je stupila 2004. godine.

Enkripcijska metoda WPA je TemporalKeyIntegrityProtocol (TKIP).
On uključuje funkciju miješanja po paketu, provjeru integriteta poruka, prošireni inicijalizacijski vektor i mehanizam ponovne dodjele ključa.
WPA2 nadomješta RC4 šifru i TKIP s dva jača enkripcijska i autentifikacijska mehanizma – AES-om i CCMP-om (CipherBlockChainingMessageAuthenticationCodeProtocol).
Kako bi ostao kompatibilan u slučaju da uređaj ne može koristiti CCMP, podržan je TKIP.[36]
Ostale poznatije metode kojima se možemo koristiti da bi što više osigurali bežičnu mrežu su skrivanje SSID-a (Service set identifier) koji je jedinstven svakom uređaju i služi za identifikaciju, te filtriranje MAC (mediaaccesscontrol) adrese, čime se omogućuje pristupanje uređajima samo s prethodno navedenim MAC adresama.
Obje metode imaju više manje minimalni utjecaj na sigurnost s obzirom da se vrlo lagano zaobilaze, ali mogu poslužiti kao dodatni sloj zaštite kako bi otežali posao potencijalnim napadačima.



Slika 10. Pojednostavljena ilustracija računalne mreže[37]

[36]Rouse, Margaret. WhatisWi-Fi Protected Access(WPA). WhatIs. 2014.
URL: http://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access (25.9.2017)
[37]WHAT IS A WLAN (WIRELESS LAN OR WIFI)? Winstudent. 2015.
URL: http://www.winstudent.com/what-is-a-wlan-wireless-lan-or-wifi/ (25.9.2017)

3.4.1. VPN

Osim zaštite pristupa lokalnoj mreži, od velike je važnosti i zaštita prometa na internetu.
Za tu svrhu postoje specijalizirani usluge poput VPN mreža ili TOR-a koji naš promet šalju kroz slikovito rečeno jednu vrstu tunela i time sprečavaju promatračima analizu paketa, s obzirom da su oni enkriptirani od pošiljatelja prema primatelju i potreban je pristup ili jednom ili drugom.
Jednostavno objašnjeno, VPN (Virtualprivate network) koristi se infrastrukturom javne mreže kako bi omogućavala povezivanje između geografski raštrkanih čvorova, umjesto da koristi dodatne fizičke priključke u svrhu korištenja za jednu mrežu, kao što je to slučaj kod WAN-a (Wide area network). Korisniku VPN izgleda kao privatna mreža, te joj i otud dolazi naziv virtualna, bez obzira što dijeli mrežu kablova s prometom stotina ili tisuća drugih korisnika.
Posjeduje sve karakteristike privatne mreže, kao primjerice ograničeni pristup samo autoriziranim korisnicima bez obzira što dijeli istu javnu infrastrukturu s drugim korisnicima.[38]
VPN možemo opisati kao mrežu koja nam omogućuje spajanje računala i njihovo ponašanje kao da su u LAN-u preko velikih distanci.
Većini VPN-a pristupamo pomoću klijenata na računalu ili uređaju na kojemu ga želimo koristiti unutar kojega se prijavimo korisničkim podacima, te on zatim izmjenjuje ključeve s vanjskim serverom kako bi se ustanovila autentičnost obje strane.
Postoji izrazito veliki broj VPN pružatelja usluga, besplatnih i plaćenih, a osim što nam omogućuju zaštititi naše podatke i očuvati privatnost, omogućuju nam simulirati da smo iz drugih država (ovisno o serveru na koji se spojimo) i time pristup internetskim uslugama koje nisu dostupne lokalno i izbjegavanje cenzura, te nas štite u slučaju uporabe javnih bežičnih mreža. Dakako, od velike je važnosti da li je pružatelj usluge legitiman i njihova politika vezana uz prikupljanje podataka o korisnicima.

[38]Fowler, Dennis. VirtualPrivateNetworks: MakingtheRightConnection. Google Knjige. 1999.
URL:
https://books.google.hr/books?id=dPIrx4Wlv1cC&printsec=frontcover&dq=vpn+what+is+it&hl=hr&sa=X&ved=0ahUKEwi7y_Dq-sDWAhXCWhoKHcHJBjMQ6AEIJDAA#v=onepage&q=vpn%20what%20is%20it&f=false (25.9.2017)

3.4.2. Tor

Mreža Tor je skupina volonterski vođenih servera koja služi kako bi korisnicima poboljšala privatnost i sigurnost na internetu. Korisnici Tora uporabljuju tu mrežu na način da se spajaju kroz seriju virtualnih tunela za razliku od izravne veze, time omogućujući kako organizacijama tako i pojedincima dijeljenje informacija preko javnih mreža bez kompromitiranja privatnosti. Samim time, Tor je efektivan alat za izbjegavanje cenzure, omogućujući korisnicima pristup inače blokiranim odredištima ili sadržaju. Tor softverski developeri također mogu koristiti kao kamen temeljac kako bi stvorili nove komunikacijske alate s ugrađenim mogućnostima privatnosti.[39]

Tor funkcionira na principu rada koji nazivamo onionrouting, razvijenom 90-ih godina u vojne svrhe, a sam naziv govori na koji način mreža radi.

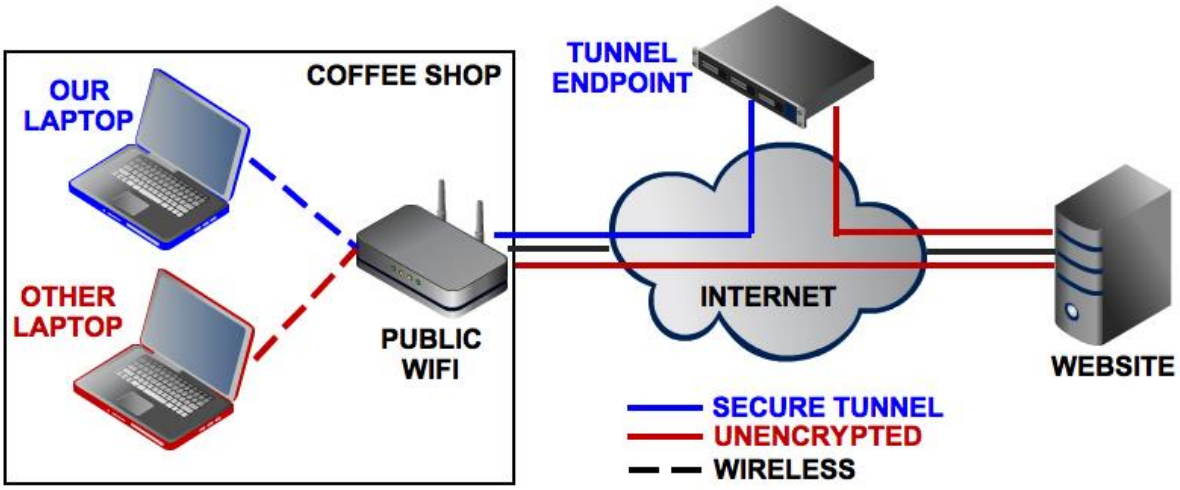
Sustav koristi višestruk broj posrednika za prijenos poruke, kod kojeg se poruka nalazi u podatkovnom paketu zvanom onion. U paketu, poruka biva enkriptirana sloj po sloj koristeći enkripcijske ključeve svih routera na komunikacijskoj putanji i ključem primatelja. [40]

Najčešći oblik implementacije Tor-a je u obliku modificirane verzije web-preglednika Firefox koja sadrži postavke da sam promet preusmjerava preko mreže Tor.

Iako je VPN daleko funkcionalniji i jednostavniji za korištenje, Tor također pronalazi svoju uporabnu vrijednost u slučajevima poput cenzure, ali se koristi i za kriminalne radnje poput trgovine drogama i sličnog.

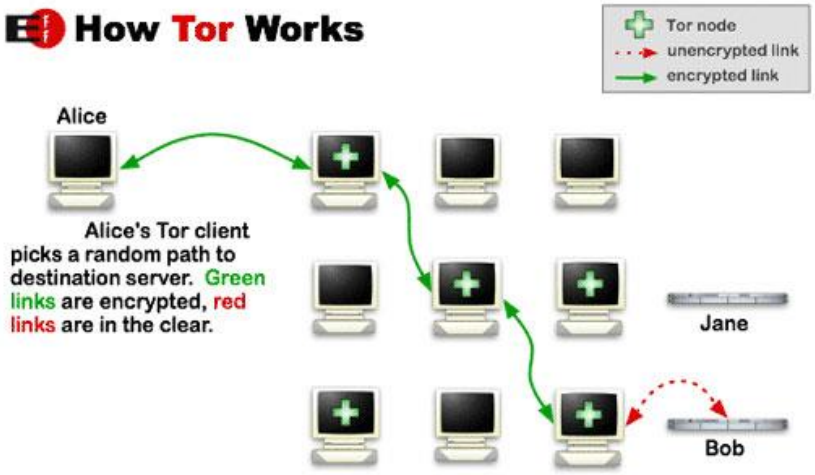
[39] Tor Project: Overview. 2015.
URL: https://www.torproject.org/about/overview.html.en (25.9.2017)

[40] Peng, Kun. AnonymousCommunicationNetworks: ProtectingPrivacy on the Web. Google Knjige. 2014.
URL:
https://books.google.hr/books?id=mVrNBQAAQBAJ&pg=PA116&dq=the+onion+router&hl=en&sa=X&redir_esc=y#v=onepage&q=the%20onion%20router&f=false(25.9.2017)



Slika 11. Ilustracija VPN

mreže[41]



Slika 12. Ilustracija mreže Tor[42]

[41] Paul, Ian. How—andwhy—youshould use a VPN any time you hop on theInternet. TechHive. 2017.
URL: https://www.techhive.com/article/3158192/privacy/howand-whyyou-should-use-a-vpn-any-time-you-hop-on-the-internet.html (25.9.2017)

[42]Yeung. Ken.Whatis Tor andwhydoesitmatter?Thenext web. 2013.
URL: https://thenextweb.com/insider/2013/10/08/what-is-tor-and-why-does-it-matter/ (25.9.2017)

4. Internetske usluge i njihovi rizici

Putem interneta možemo pristupiti velikom broju usluga širokoga spektra, od usluga za kupovinu poput ebaya i Amazona, društvenih mreža poput Facebooka i Twittera, e-mail usluga poput Gmaila i Outlooka pa sve do specijaliziranih usluga poput lokalne dostave hrane i sličnoga. Sve te usluge imaju zajedničku jednu stvar – u većini slučajeva koristimo osobne podatke i osjetljive podatke poput brojeva kreditnih kartica kako bi im pristupili.

Primjenom prethodno navedenih mjera sigurnosti, korisnik većim dijelom izbjegava mogućnost krađe podataka ali uvijek postoji opasnost da se pružatelja tih usluga kompromitira. Od nekorištenja enkripcije za podatke kupaca, unutarnjih curenja podataka zbog zaposlenika ili napada koji iskorištavaju slabosti u sustavu, korisnici se moraju itekako pouzdati u pružatelje tih usluga kada im na raspolaganje daju osobne podatke.

Neke od mjera sigurnosti kojima se osiguravamo čak i u tom slučaju su primjerice kod online backupa podataka enkriptiranje vlastitih podataka ukoliko to pružatelj ne nudi, ili korištenje prepaid kartica koje nam omogućuju korištenje prethodno određenog iznosa i ograničavaju moguću štetu u slučaju da se naši podaci kompromitiraju.

4.1. Google

Kao multinacionalna kompanija koja pruža široku lepezu besplatnih usluga, od najpopularnije tražilice na svijetu i web-preglednika Chrome, e-mail usluga, usluga za internetsku kupovinu i navigaciju pa sve do operacijskih sustava za stolna računala poput chromeOS-a i mobilnog operacijskog sustava Android, Google je često pod povećalom zbog enormne količine osobnih podataka kojima raspolaže. Kako kompanija veći dio dobiti ostvaruje kroz oglašavanje na temelju korisničkih interesa i pretraživanja, veliki problem je odrediti koliko zapravo zadiru u privatnost i koliko su naši osobni podaci sigurni, bez obzira na anonimnost svih prikupljenih informacija koju Google zagovara.

Tehnologija tj. metoda koja se u ovom slučaju primjenjuje poznatija je pod nazivom rudarenje podataka. Rudarenje podataka svoju najveću primjenu u poduzećima pronalazi u marketingu, IT sektoru, bankarstvu i osiguranju itd. ali u pravilu rudarenje se može koristiti u svim područjima gdje postoje velike količine podataka kako bi na osnovu istih utvrdili zakonitosti i obrasce među njima. Rudarenje podataka možemo primijeniti kod analize kupaca, primjerice, identificiranje profitabilnih kupaca, identificiranje kupaca i proizvoda kod poboljšanja unakrsne prodaje ili otkrivanje načina povećanja lojalnosti kupaca.[43]

Ignorirajući problem privatnosti naših podataka, Google-ove usluge su same po sebi izrazito sigurne zbog brojnih sigurnosnih rješenja koja su implementirana.

Od korištenja već navedene sandbox tehnologije u web-tražilici Chrome i sustavu chromeOS, korištenja dvostruke provjere autentičnostipomoću mobilnog telefona na Google korisničkom računu, redovitih asistencija koje služe osvještavanju korisnika po pitanju njihovih sigurnosnih navika na internetu pa sve do natjecanja u kojima se sudionike nagrađuje pri pronalasku mogućih sigurnosnih slabosti, Google-u je od izrazite važnosti izbjeći moguće sigurnosne propuste.

[43] Živković, Šime. Što je to rudarenje podataka (eng. Data mining). IMEF. 2016.
URL: http://imef.hr/sto-to-rudarenje-podataka-eng-data-mining/ (25.9.2017)

4.2. Usluge za online kupovinu

Online kupovina omogućuje kupcima direktnu kupovinu proizvoda ili dobara putem Interneta bez dodatnih alata, koristeći se samo web-preglednikom.

Postoje dvije vrste online kupovine, B2C (Business to consumer) i B2B (Business to business), a u ovom poglavlju ćemo kratko opisati B2C kao općenitu online kupovinu s kojom se susreću kućni korisnici i njegove prednosti i nedostatke u kontekstu primjene osobnih podataka. Najpoznatije usluge s kojima smo se vjerojatno svi u jednom trenu susreli su ebay, Amazon i Alibaba, a korisnici na njima mogu kupovati fizičke predmete ali i digitalne sadržaje poput pjesama ili filmova.

Kako bi bili u mogućnosti izvršiti transakciju, potrebno je imati pristup važećem obliku plaćanja, poput kreditnih kartica ili korištenjem usluga poput PayPala.

Prednosti su brojne, poput jednostavnosti korištenja, informiranosti pri kupovini (u obliku korisničkih opisa proizvoda), širokog asortimana i mogućnosti usporedbe cijena.

Dakako, iz aspekta zaštite osobnih podataka, skepsa je još uvijek prisutna pri online kupovini zbog toga što povjerenje polažemo u neopipljivu uslugu, bez sigurnosti koju imamo kada to radimo u fizičkim trgovinama.

Međutim, opasnosti su realne, a korisnici mogu biti metama prevara u kojima uopće ne dobiju traženu robu ili im procure povjerljive informacije poput brojeva kreditnih kartica.

Bez obzira na mjere sigurnosti s korisnikove strane, pri online kupovini je od presudne važnosti provjeriti legitimnost usluge (informirati se prije korištenja relativno nepoznatih usluga) te utvrditi njihovu politiku po pitanju privatnosti i koje tehnologije primjenjuju kako bi osigurali korisničke podatke.

4.3. Društvene mreže

Društvene mreže, tj. stranice društvenih mreža su online usluge pomoću kojih korisnici mogu stupiti u kontakt s drugim ljudima, bilo to prijateljima, poznatim osobama ili potpunim neznancima.

Prva stranica društvene mreže za koju se svi mogu složiti da je bila oblik društvene mreže kakve danas koristimo bila je stranica SixDegrees. Ime je dobila prema teoriji „šest stupnjeva odvojenosti“ i trajala je od 1997. do 2001. SixDegrees je korisnicima omogućavao stvaranje profila i omogućavao sprijateljavanje s drugim korisnicima. Čak je i omogućavao onima koji nisu bili registrirani kao korisnici da potvrde prijateljstva, te je na taj način spajao ljude.[44]

Slijedili su prethodnici današnjih klasičnih društvenih mreža poputFacebooka, Friendster – usluga koja je bila nešto između klasične društvene mreže i usluge za pronalaženje partnera, LinkedIn – mreža primarno fokusirana na poslovni aspekt umrežavanja i MySpace – društvena mreža fokusirana na mlađu publiku koja je bila fokusirana na popularne interese poput glazbe i filmova i često uporabljivana od strane muzičara u svrhu promocije.

2004., MarkZuckerberg je pokrenuo stranicu koja je danas gigant društvenih mreža, te služi kao uzor drugim uslugama postavljanjem trendova (gumb za like).

Facebook je danas društvena mreža broj jedan i broji preko dvije milijarde korisnika.[45]

U početku je Facebook bio ograničen na korištenje samo studentima sveučilišta Harvard, a Zuckerberg je tada uočio potencijal i uslugu stavio na raspolaganje ostatku svijeta.

2006. je popularnost dopisivanje tekstualnim porukama ili SMS-om ispiriralaJackaDorseya, BizaStonea, NoahaGlassa i Evana Williamsa da stvore Twitter, uslugu koja je bila jedinstvena po tome što je korisnicima omogućavala da šalju „tweetove“ od 140 znakova ili manje. Danas Twitter broji preko 500 milijuna korisnika.[46]

[44] Hale, Benjamin. TheHistoryofSocial Media: SocialNetworkingEvolution! HistoryCooperative. 2015. URL: http://historycooperative.org/the-history-of-social-media/(25.9.2017)

[45]The Top 20 Valuable Facebook Statistics. Zephoria. 2017.
URL: https://zephoria.com/top-15-valuable-facebook-statistics/ (25.9.2017)

[46] Hale, Benjamin. TheHistoryofSocial Media: SocialNetworkingEvolution! HistoryCooperative. 2015. URL: http://historycooperative.org/the-history-of-social-media/(25.9.2017)

Problematika vezana uz sigurnost društvenih mreža direktno je povezana s otvorenošću istih. Bez obzira na mogućnost ograničavanja sadržaja, korisnici su u konstantnoj opasnosti od raznih prijetnji – mlađi korisnici od prijetnji poput bullyinga od strane vršnjaka i vrebanja pedofila, a općenito svi korisnici od opasnosti poput krađe identiteta, slučajnog curenja podataka i malicioznih poveznica koje velikim dijelom nisu pod kontrolom stranica društvenih mreža. Od izrazite je važnosti korisnike, pogotovo djecu, educirati po pitanju sigurnog ponašanja na društvenim mrežama, te ih upozoriti na moguće posljedice njihovih radnji (primjerice objavljivanja fotografija ilegalnih ili neprofesionalnih radnji koje bi kasnije mogle naštetiti njihovoj javnoj slici). Isto tako, kao u slučaju Google-a, društvenim mrežama se predbacuju kritike zbog politika korištenja osobnih podataka u svrhu oglašavanja i daljnjeg prodavanja kompanijama, pri čemu u ovom slučaju društvene mreže imaju daleko veću količinu podataka osobnog karaktera, bilo to u obliku fotografija, osobnih poruka ili tzv. statusa tj. poruka javnog karaktera kojima korisnici mogu ograničiti vidljivost.

Slika 14. Javni profil Marka Zuckerberga na Facebooku[47]

[47]MARK ZUCKERBERG's profile - Facebook Picture. Stuffpoint. 2013.
URL: http://stuffpoint.com/facebook/image/315232/mark-zuckerbergs-profile-picture/ (25.9.2017)

4.4. SSL, TLS i HTTPSprotokoli

Netscape je 1994. razvio SecureSocketsLayer(SSL) protokol kao odgovor na rastuću zabrinutost vezanu uz sigurnost na internetu. SSL je prvotno razvijen za osiguravanje komunikacije između web preglednika i servera. Specifikacija standarda dizajnirana je na taj način da omogući drugim aplikacijama, poput TELNET-a i FTP-a korištenje SSL-a.[48] Transport LayersSecurity (TLS) protokol, SecureSocketsLayer (SSL) protokol, verzije 2.0 i 3.0, i Private Communications Transport (PCT) protokol temelje se na kriptografiji pomoću javnog ključa. U procesu autentifikacije, TLS/SSL klijent šalje poruku TLS/SSL serveru, te server odgovara s informacijama potrebnim kako bi se autentificirao. Klijent i server vrše dodatnu razmjenu sesijskih ključeva, te autentifikacija završava. Na kraju autentifikacije, komunikacija osigurana SSL-om može započeti između servera i klijenta koristeći se simetričnim enkripcijskim ključevima koje smo odredili tijekom procesa autentifikacije.[49]HTTPS je protokol nastao kombinacijom HTTP i SSL/TLS protokola. Omogućava potvrdu autentičnosti posjećene web stranice, zaštitu privatnosti te očuvanje integriteta podataka koji se razmjenjuju. U narednim godinama se očekuje kako će većina web stranica koristiti HTTPS protokol, a prema statistikama GoogleovogChrome web preglednika trenutno se preko 50% stranica prikazuje preko HTTPS protokola i na takvim, sigurnim stranicama korisnici provode 2/3 vremena ukupnog surfanja.[50]Navedeni protokoli služe kao dokaz legitimne komunikacije sa serverom te nas uvjeravaju u enkriptiranost podataka koje šaljemo, što je od kritične važnosti kod primjena poput internetske kupovine i svih usluga koje zahtijevaju korištenje osjetljivih podataka.Također, web-tražilice poput Google-a rezultate pretraživanja rangiraju prema tome koriste li web-stranice navedene protokole, te se kod svih imalo ozbiljnijih web-stranica implicira korištenje navedenih sigurnosnih protokola kako bi osigurali korisničke podatke.

[48]Historyof SSL. IBM KnowledgeCenter. 2017.
URL: https://www.ibm.com/support/knowledgecenter/en/ssw_i5_54/rzain/rzainhistory.htm (25.9.2017)
[49]Whatis TLS/SSL? Microsoft TechNet. 2003.
URL: https://technet.microsoft.com/en-us/library/cc784450(v=ws.10).aspx (25.9.2017)
[50]Gorinjac, Jasmin. Prelazak na HTTPS. Plus.hr Blog. 2017.
URL: https://www.plus.hr/blog/2017/01/26/prelazak-na-https/ (25.9.2017)

4.5. Pohrana podataka na internetu

Sve jeftinijim pristupom i povećavanjem brzina Interneta diljem svijeta došlo je do svojevrsnog buma usluga za pohranu podataka na internetu.

Prednosti su svima jasne, podatke skladištimo na serverima pružatelja tih usluga, te im na bilo kojem mjestu na kojem imamo pristup internetu možemo pristupiti kao da su oni lokalno skladišteni. Time ne ovisimo o lokalnim ograničenjima količine prostora (primjerice na mobilnim uređajima koji su bez obzira na velike pomake još uvijek poprilično ograničeni količinom prostora za pohranu koji nude), a podatke možemo dijeliti diljem uređaja – od računala i mobitela, pa sve do televizora i automobila.

Rizici kod pohrane podataka na internetu su očiti na prvi pogled – osobne podatke stavljamo u tuđe ruke, relativno van naše kontrole. Kao osobni korisnici, ne znamo gdje se točno nalaze naši podaci, tko ima pristup te drže li se pružatelji usluga politika privatnosti i sigurnosti.

Također, nismo samo podložni rizicima koji ugrožavaju našu privatnost i sigurnost – jednako tako možemo pri greškama od strane pružatelja ostati bez podataka u slučaju internih problema poput otkazivanja servera. To ne mora biti nužno trajni nestanak, ali i privremenim nestankom pristupa usluzi tj. našim podacima možemo biti oštećeni, pogotovo ako se radi o poslovnim podacima poput kritičnih projekata koje moramo unutar određenog vremenskog razdoblja kompletirati. Zbog toga je od izrazite važnosti uz online backup podataka imati i lokalnu kopiju kako bi se dodatno osigurali od gubitka podataka.

Postoje razne usluge – besplatne i plaćene, a od velike važnosti je detaljno proučiti njihove politike vezane uz baratanje našim podacima – odgovaraju li za eventualne štete, da li se obvezuju podatke izručiti vladama te koriste li enkripciju pri pohrani naših podataka. Zadnja stavka je od izrazite važnosti, te se bez obzira na korištenje enkripcije od strane pružatelja usluga predlaže korištenje vlastite enkripcije, pogotovo zato što je u prošlosti kod brojnih usluga bilo slučajeva gdje su podaci inkriminirani zajedno s ključevima, ili je došlo do curenja podataka korisničkih računa pomoću kojih pristupamo podacima, čime je enkripcija bila beskorisna.Jedan od takvih slučajeva dogodio se 2012., kada je hakiran najpoznatiji pružatelj usluga pohrane podataka na internetu – Dropbox. Došlo je do curenja 68 milijuna korisničkih računa zajedno sa zaporkama, te je korisnicima savjetovano mijenjanje zaporki bez obzira što su one u određenoj mjeri bili enkriptirane.[51]

[51]Gibbs, Samuel. Dropboxhackleads to leakingof 68m userpasswords on theInternet. TheGuardian. 2016.URL: https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach (25.9.2017)

4.5.1. Zadržavanje podataka

Zadržavanje podataka ili dana retention, odnosi se na trajnu pohranu podataka neke organizacije u svrhu usklađenosti ili za poslovne svrhe.

Organizacija može zadržati podatke radi nekoliko razloga. Neki od razloga su pridržavanje zakonskih regulativa ili povratak podataka kritičnih za poslovanje u slučaju gubitka podataka.

Minimalna razdoblja zadržavanja podataka razlikuju se od države do države a mogu se kretati u rasponu od 3 godine do trajno.[52]

Zbog toga je presudno koje podatke dajemo na korištenje pružateljima usluga kako bi izbjegli naknadne probleme, kao na primjer provale u web trgovinu koju smo koristili prije nekoliko mjeseci ili godina te unosili podatke poput brojeva kreditne kartice ili sličnog.

Kako bi izbjegli naknadne probleme, važno je korištenje provjerenih usluga na internetu i utvrđivanje njihovih politika vezanih uz baratanje našim podacima, ne samo kako bi se osigurali u sadašnjosti, već i u budućnosti.

[52]Rouse, Margaret. Whatis data retention. WhatIs. 2014.
URL: http://searchstorage.techtarget.com/definition/data-retention (25.9.2017)

5. Načini online plaćanja

Postoje razni načini plaćanja putem interneta, bilo direktno pomoću kreditnih kartica, putem bonova specijalno dizajniranih za korištenje na internetu, korištenjem usluga posrednika poput Paypala ili specijalno dizajniranim digitalnim valutama, poput Bitcoina.
Oni nam omogućuju korištenje usluga poput web-trgovine ili plaćanja računa, prijenosa novaca drugim korisnicima ili za primanje zarade.
Postoje razne prednosti i nedostaci vezani uz navedene načine plaćanja, a savršen oblik ne postoji jer se uvijek radi o dvije strane između kojih se vrši transakcija i prostora za pogreške ili čak prevare i krađu uvijek ima.
Kako bi izbjegli krađu podataka, ili se u slučaju krađe osigurali, predlaže se korištenje posrednika koji u slučaju problema interveniraju.

5.1. Kreditne kartice

Pri korištenju kreditnih kartica na internetuapsolutno je neophodno korištenje već prije navedenih enkripcijskih protokola kako bi podaci kartica ostali zaštićeni.
U slučaju primjene na internetu, metoda koja korisnike dodatno može zaštititi nabavka je dodatne, pre-paid kreditne kartice – kartice na kojoj unaprijed zadajemo, tj. uplaćujemo iznos novaca koji želimo potrošiti te se na taj način čak i slučaju krađe zaštićujemo od veće štete.
Također, neke banke pružaju mogućnost korištenja funkcionalnosti virtualne kreditne kartice, gdje korisnik dobiva jednokratni broj kojim vrši transakciju, nakon koje on više nije funkcionalan.
Dodatni sigurnosni standardi, kao što je Mastercard SecureCode, onemogućuju kriminalcima korištenje kreditnih kartica bez obzira što posjeduju njihove informacije.
Kada se registiramo i stvorimo vlastiti SecureCode, automatski ćemo kod zaključivanja kupovine od strane banke biti upitani za SecureCode svaki put kada kupujemo pomoću registrirane kreditne ili debitne kartice kod prodavača koji podržavaju SecureCode. SecureCode se brzo potvrđuje od strane banke i transakcija je provedena, pri čemu se kod

nikada ne dijeli s prodavačem.[53] Bez obzira na sve provedene mjere sigurnosti, uvijek se predlaže redovito provjeravanje izrezaka transakcija kako bi se uvjerili da nema neautoriziranih transakcija.

5.2. Internetsko bankarstvo

Internetsko bankarstvo (eng. Online banking) je financijski servis banke koji omogućava korisniku osobno i izravno obavljanje i pregled financijskih transakcija i stanja, a pritom koristi internet kao kanal distribucije po kojem se vrši bankarska aktivnosti.[54]

Da bi korisnik pristupio korištenju e-bankarstva on treba ugovoriti uslugu sa bankom. Banka naplaćuje naknade za otvaranje računa te klijentu daje na korištenje token uređaj. Pomoću tokena, koji ima svoj PIN, korisnik pristupa stranicama banke, te ima mogućnost obavljanja novčanih transakcija kao što su npr. plaćanje računa. Kod većine takvih transakcija trošak obrade je puno niži nego u poslovnici. Većina banaka, preko e-bankarstva, nude i usluge ugovaranja štednje, kupnju udjela u investicijskim korisnicima i slično.[55]

Pri korištenju internetskog bankarstva, uporabom tokena stvaramo dodatni sloj zaštite koji onemogućava kriminalcima uporabu kartice. Unosom PIN-a, uređaj generira jednokratni kod koji zatim koristi za pristup ili transakciju.

Token može biti u obliku fizičkog uređaja, ali i u obliku aplikacije za mobilni uređaj koji u banci autoriziramo prije daljnjeg korištenja pomoću jedinstvenog broja kojeg najčešće primamo SMS-om.

Osim tokena, autorizaciju je moguće vršiti TAN-om, koji funkcionira na principu prethodno određenih nizova znamenaka koji se jednokratno koriste u svrhu provođenja transakcije.

Najčešće je u obliku papira, ali može dolaziti i u obliku kartice.

Poslovni korisnici, s druge strane, često koriste tzv. smart kartice koje sadrže sve potrebne podatke za autorizaciju, no za razliku od tokena koji ne treba ništa osim pristupa internetu, smart kartice zahtijevaju specijalizirane čitače.

Kartice se temelje na PKI (PublicKeyInfrastructure) tehnologiji koja se zasniva na asimetričnoj kriptografiji, odnosno na paru javnih i tajnih ključeva za šifriranje podataka.[56]

---

[53]FrequentlyAskedQuestions. Mastercard. 2017.
URL: https://www.mastercard.us/en-us/frequently-asked-questions.html#securecode (25.9.2017)
[54]Internetsko bankarstvo. Wikipedia. 2014.
URL: https://hr.wikipedia.org/wiki/Internetsko_bankarstvo (25.9.2017)
[55]Internet bankarstvo – definicija. Moj-bankar. 2012.
URL: http://www.moj-bankar.hr/Kazalo/I/Internet-bankarstvo (25.9.2017)
[56]Internetsko bankarstvo. Wikipedia. 2014.
URL: https://hr.wikipedia.org/wiki/Internetsko_bankarstvo (25.9.2017)

5.3. Paypal i slični

Paypal je američka kompanija za elektronsku trgovinu osnovana u ožujku 2000. Specijalizirana je za internetske transfere novcem, te je nastala spojem kompanija X.com i Confinity.[57]

Nakon što je uočio kako Paypal postaje prvi izbor za kupce na internetskim aukcijama, div elektronske trgovine, eBay, kupio je Paypal za 1.5 milijarda dolara u listipadu 2002.

Kompanija korisnicima nudi mogućnost spajanja PayPal računa s bankovnim, čime transakcije i plaćanja čini efikasnijim od plaćanja novčanim nalozima i čekovima.

Kod određenih transakcija postoje naknade koje se utvrđuju na temelju novčane svote, vrste transakcije i valute koju koristimo.[58]

Paypal se osim korisničkih podataka brine i za zaštitu transakcija koje korisnici provedu.

U slučaju pokušaja prevara, poput prodavanja krivotvorenih proizvoda ili starih kao nove, ili oštećivanja proizvoda pri transportu, Paypal kao posrednik štiti kupca te mu omogućava traženje povrata novaca. Također, u slučaju neautoriziranog pristupa korisničkom računu, bez obzira bila to naša ili njihova krivnja, omogućuje prijavu istoga i povrat novca.

Također, kao i u klasičnom internetskom bankarstvu, postoji mogućnost korištenja tokena u obliku mobilne aplikacije.

Konkurenti Paypalu usluge su poput Google Walleta, WePaya i Skrilla, no s obzirom na tržišnu zastupljenost koja dolazi u obliku integracije s ebayom i velikom količinom drugih usluga koje se pouzdaju u plaćanje pomoću Paypala, teško ga je zaobići.

[57]PayPal. Britannica. 2017. URL: https://www.britannica.com/topic/PayPal (25.9.2017)
[58]PayPal. Britannica. 2017. URL: https://www.britannica.com/topic/PayPal (25.9.2017)

5.4. Kriptovalute kao alternativni način plaćanja

Posljednjih par godina u izrazitom rastu popularnosti, kao alternativni način plaćanja važno je spomenuti kriptovalute.

Kriptovalute su internetske digitalne valute zasnovane na kriptografiji, od kojih je najpoznatija i najzastupljenija Bitcoin.

Specificiran i u praksi dokazan, Bitcoin je objavljen 2009. godine u kriptografskoj mailing listi od strane osobe pod pseudonimom „SatoshiNakamoto“.

Projekt je open-source te je razvijan od velikog broja programera. Otvorenost koda također omogućava uvid u sigurnost softvera od strane bilo koje osobe stručne u tom području. Temelji se na peer-to-peer strukturi, te je time digitalni oblik plaćanja najsličniji gotovini.

Bitcoin nije upravljan od strane banaka te je kao takav dizajniran da bude što kompetitivniji po pitanju transakcija, sa daleko nižim ili u nekim slučajevima nepostojećim naknadama. Najčešće se koristi u online kupovini te kao investicijsko sredstvo.

Iako je konceptom izrazito praktična, valutu nije moguće koristiti u preko 99% slučajeva van internetske trgovine, te je veliku primjenu zbog relativne anonimnosti pronašlo u ilegalnim primjenama, poput trgovine zabranjenim supstancama i sličnog.

Korisnici valutu drže u tzv. walletima tj. novčanicima, a kod transakcija se primjenjuje asimetrična kriptografija kod koje se generiraju dva ključa – javni i privatni.

Postoje razni oblici novčanika, a osim osobnih računala pokriveni su i mobilni uređaji te postoje uređaji dizajnirani isključivo za svrhu pohranjivanja kriptovaluta.

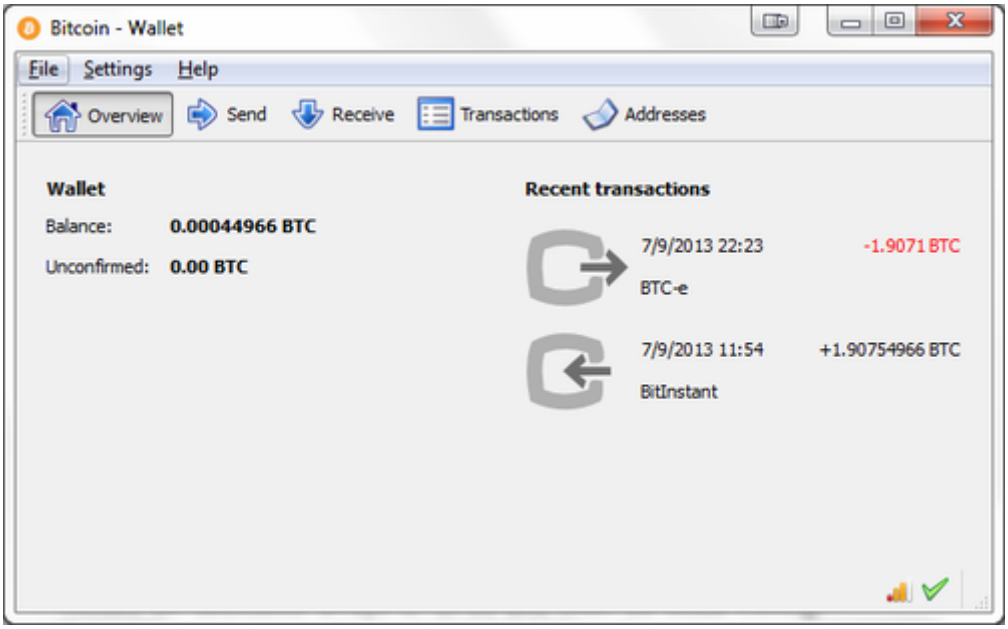
Kako bi došlo do razmjene valute, vlasništvo se prenosi putem alfanumeričkog niza koji je dobiven shemom haširanja i enkodiranja javnog ključa.

U prijenosu valute privatni ključ koristi se kao sigurnosna mjera. Uz njegovu pomoć generira se digitalni potpis koji dokazuje da je ključ u našem vlasništvu.

2017. mu je iznenadno porasla vrijednost i popularnost, te je zbog te pozornosti postao daleko zastupljeniji i javnost se je počela više interesirati.

Kako mu je u mjesec dana vrijednost porasla duplo s 2000 na 4000 dolara, upitno je koliko je on zapravo stabilan i primjenjiv u svrhe elektronske trgovine, bez obzira na naprednost tehnologije i razne prednosti koje on nudi.

Bitcoin je svakako pokrenuo trend kriptovaluta, i svakim danom pojavljuje se sve više konkurenata ali i primjena i korisnika.



Slika 15. Primjer softverskog Bitcoin novčanika za osobna računala[59]

Slika 16. Primjer fizičkog Bitcoin novčanika[60]

[59]Top 10 Bitcoin Desktop Wallets. Bitcoinmillionaire. 2014.
URL: http://blog.bitcoinmillionaire-app.com/2014/09/bitcoinmillionaire-top-10-bitcoin-desktop-wallets/ (25.9.2017)
[60]How To Store YourBitcoins. BitcoinGuides. 2016.
URL: http://bitcoindaily.org/bitcoin-guides/how-to-store-your-bitcoins/ (25.9.2017)

6. Sigurnosni rizici

Bez obzira na sigurnosne mjere, važno je znati s kojim oblicima rizika se na internetu možemo susresti, te na koji način oni funkcioniraju.
Postoji više oblika sigurnosnih rizika, dok su neki u obliku zlođudnih datoteka ili poveznica koje na temelju pokretanja mogu naštetiti našim računalima postoje i oblici poput društvenog inženjeringa kod kojega kriminalci na temelju lakovjernosti neke osobe mogu manipulacijom doći do željenih podataka.

6.1. Socijalniinženjering, phishing i spam

Oblik prijetnji s kojim ćemo se pri uporabi računala najčešće sresti željeli mi to ili ne je tzv. socijalni inženjering.Socijalni je inženjering niz tehnika pomoću kojih pojedinac, iskorištavanjem ljudskih pogrešaka i slabosti, utječe na drugog pojedinca kako bi ga naveo da učini nešto što nije u njegovom interesu. Socijalni se inženjering najčešće koristi u svrhu otkrivanja njihovih povjerljivih informacija ili dobivanja pristupa nekim drugim resursima do kojih napadač inače ne bi mogao doći.[61]
Napadači se često služe ovom tehnikom jer im za uspješan napad nije potrebno složeno probijanje korisnikove sigurnosne zaštite, korištenje ranjivosti njegovog softvera i sl. Pojam socijalnog inženjeringa je popularizirao poznati i osuđeni haker KevinMitnick, koji tvrdi kako je mnogo lakše nekoga prevariti služeći se socijalnim inženjeringom nego probiti njegov informacijski sustav.[62]
Phishing je oblik socijalnog inženjeringa tj. prevare pri kojem kriminalci koji se predstavljaju kao legitimne usluge pomoću falsificiranih e-mail poruka i lažnih web stranica prikupljaju korisničke podatke.
E-mail poruke koje izgledaju gotovo identično kao i one koje dobivamo od legitimnih usluga korisnike mogu navesti na slanje povjerljivih podataka pod izlikama poput izmjene usluga ili problema s korisničkim računom. Također, u porukama mogu biti poveznice koje nas

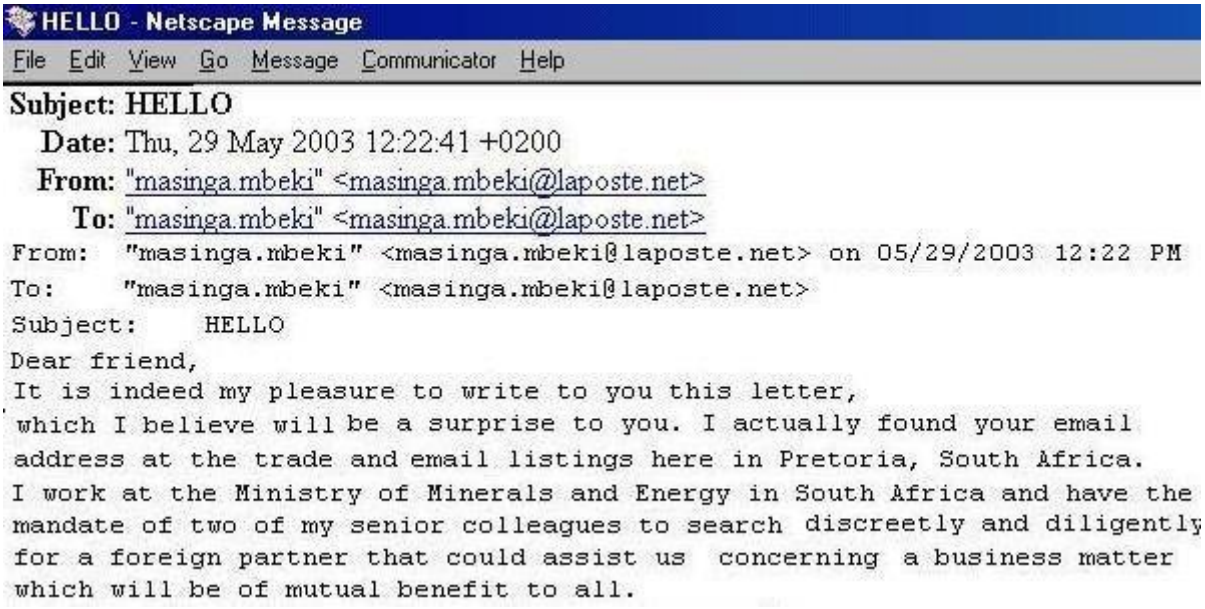
[61]O socijalnom inženjeringu. Nacionalni CERT. 2017.
URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)
[62]O socijalnom inženjeringu. Nacionalni CERT. 2017.
URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)

preusmjeravaju na web lokacije koje dizajnom i sadržajem imitiraju legitimne, poput bankovnih usluga. Na tim lokacijama se zatim prikupljaju korisnički podaci koje kriminalci dalje uporabljuju.

Spam je neželjena elektronička poruka poslana zbog namjere oglašavanja raznog propagandnog sadržaja ili u svrhu phishing napada ili kao sredstvo distribucije malver poveznica.[63]

Da bi spameri mogli slati neželjene poruke, potrebno im je pribaviti e-mail adrese potencijalnih primatelja. E-mail adrese se sakupljaju preko raznih chatova, Web stranica, newsgrupa ili virusom zaraženih računala. Najčešći način sakupljanja e-mail adresa je pomoću robotskih skupljača (eng. harvester) – bota koji na Webu traži e-mail adrese.[64]

Kod socijalnog inženjeringa najvažnije je koristiti se zdravim razumom s obzirom da nas niti jedna vrsta antivirusne zaštite neće zaštititi od nepažnje i dobrovoljnog slanja osobnih podataka. Također je od koristi uvijek primjenjivati spam filtere kod preglednika za elektronsku poštu i paziti kome dajemo adresu elektronske pošte.


HELLO - Netscape Message

File Edit View Go Message Communicator Help

Subject: HELLO
Date: Thu, 29 May 2003 12:22:41 +0200
From: "masinga.mbeki" <masinga.mbeki@laposte.net>
To: "masinga.mbeki" <masinga.mbeki@laposte.net>

From: "masinga.mbeki" <masinga.mbeki@laposte.net> on 05/29/2003 12:22 PM
To: "masinga.mbeki" <masinga.mbeki@laposte.net>
Subject: HELLO

Dear friend,
It is indeed my pleasure to write to you this letter,
which I believe will be a surprise to you. I actually found your email
address at the trade and email listings here in Pretoria, South Africa.
I work at the Ministry of Minerals and Energy in South Africa and have the
mandate of two of my senior colleagues to search discreetly and diligently
for a foreign partner that could assist us concerning a business matter
which will be of mutual benefit to all.

Slika 17. Primjer socijalnog inženjeringa u obliku poruke elektroničke pošte[65]

[63]O spamu. Nacionalni CERT. 2017. URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)
[64]O spamu. Nacionalni CERT. 2017. URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)
[65]Who startedtheNigerian Prince email scam?Quora. 2016.
URL: https://www.quora.com/Who-started-the-Nigerian-Prince-email-scam (25.9.2017)

6.2. Klasični virusi i ransomware

Računalni virus je računalni program koji svojom reprodukcijom može zaraziti računala na način da bez dopuštenja ili znanja samog korisnika računala kopira samog sebe u datotečni sustav ili memoriju ciljanog računalnog sustava. Izraz "virus" često se povezuje i s malicioznim programima poput adware-a (program za oglašavanje) i spyware-a (program za prikupljanje podataka), koji nemaju sposobnost reprodukcije kao virus. Virusi se najčešće šire s jednog računala na drugo u obliku izvršnog zlonamjernog koda putem Interneta, privitaka u e-mail porukama ili medija poput floppy diskete, eksternog hard diska, CD, DVD ili USB diska. Povećana je mogućnost širenja virusa u slučaju da se datoteke zaražene virusom nalaze na poslužitelju, kojem imaju pristup više korisnika.[66]

Da bi se virus replicirao pokretanjem izvršenja malicioznog koda, virusi se vežu za izvršne datoteke legitimnih programa. Tako se u slučaju pokretanja zaraženog legitimnog programa, istovremeno pokreće izvršavanje i virusnog koda.[67]

Prema svom načinu djelovanja, virusi se dijele se na dvije vrste, nerezidentne i rezidentne. Nerezidentni virusi se nalaze u RAM memoriji samo u vrijeme njihovog izvršenja, odnosno od njihovog pokretanja pa do završetka rada. Njihovo širenje se svodi na princip da dio njihovog koda pronalazi datoteke koje mogu biti zaražene na sustavu(npr. .exe., .doc i slično), a drugi dio koda kopira virusni kod u pronađenu datoteku.[68]

Virusi mogu koristiti razne tehnike kako bi izbjegli detekciju, a većina ih se oslanja na mijenjanje potpisa virusakako bi izbjegli ponovnu identifikaciju od strane antivirusnih programa – te viruse nazivamo još polimorfnima i metamorfnima – ovisno o načinu modifikacije.

Međutim, antivirusni programi koji se baziraju na principu heuristike (svi moderni) bez obzira na promjenu potpisa sposobni su detektirati tu vrstu virusa na temelju algoritma.

[66]O virusima. Nacionalni CERT. 2017.
URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)
[67]O virusima. Nacionalni CERT. 2017.
URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)
[68]O virusima. Nacionalni CERT. 2017.
URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)

Ransomware je naziv za skup malicioznih programa koji korisniku onemogućuju korištenje računala. Nakon zaraze ransomware može kriptirati datoteke ili onemogućiti korištenje na način da se pojavi početni ekran s određenom porukom koju nije moguće maknuti. Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje normalno korištenje računala. U zadnje vrijeme sve je više slučajeva u kojem se pojavljuje prvi navedeni slučaj u kojem malver kriptira korisničke podatke i u zamjenu za njihovo dekriptiranje traži uplatu određenih novčanih sredstava (tzv. cryptoransomware).[69]

Kako bi čak i u slučaju zaraze izbjegli kriptiranje korisničkih podataka, važno je uvijek imati sigurnosnu kopiju, te je držati na odvojenom mjestu kojem zlćudni softver ne može pristupiti – bilo na mreži ili lokalno (primjerice na eksternom tvrdom disku koji nije stalno spojen na računalo).

Slika 18. Primjer ransomware softvera koji enkriptira datoteke i ucjenjuje korisnika[70]

[69]Ransomware. Nacionalni CERT. 2017.
URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)
[70]File:Wana Decrypt0r screenshot.png. Wikipedia. 2017.
URL: https://en.wikipedia.org/wiki/File:Wana_Decrypt0r_screenshot.png (25.9.2017)

6.3. Javna računala

Često puta smo primorani koristiti se javnim računalima, bilo u kafićima, kod prijatelja ili u knjižnici na fakultetu. Ukoliko na tim računalima nisu provedene sigurnosne mjere koje bi spriječile zarazu pri višestrukom korištenju od različitih korisnika, podaci vrlo lako postaju inkriminirani, a pri uporabi prijenosnih USB memorija lako je prenijeti zarazu na vlastito računalo. Zbog toga se uvijek savjetuje pri korištenju javnih računala izbjegavati pristup osjetljivim podacima, izbjegavanje funkcionalnosti spremanja zaporki u web preglednicima i brisanje tragova jer bez obzira na nezaraženost sustava, tragovi korištenja ostaju.

Kako je korištenje javnih računala ponekad nemoguće izbjeći, nakon što ponovo imamo pristup osobnom računalu predlaže se uvijek izmijeniti zaporke, kako bi bili osigurani od krađe podataka.

Pružatelji javnih usluga poput kafića ili fakulteta s problemom višestruke uporabe koja svakim korisnikom povećava rizik od infekcije mogu se suočiti na način da na računalima ograniče pristup, bilo u obliku crne liste koja brani pristup određenim stranicama ili bijele liste koja omogućuje pristup samo određenima. Također mogu zabraniti instalaciju aplikacija i ograničiti korisničke ovlasti.

Još jedan od načina, koji se primjenjuje i u knjižnici našeg fakulteta, ograničavanje je pristupa samo korisnicima koji posjeduju jedinstveni elektronički identitet te na kraju korištenja brisanje svih izmjena i vraćanjem na početne postavke nakon svakog studenta.

Oblik prevencije koji nas također može zaštititi od zloćudnog softvera pokretanje je prethodno navedenih live USB ili live CD operacijskih sustava koji izbjegavaju pristup operacijskom sustavu na računalu, no njihova uporaba je često ovisna o pristupu BIOS-a od računala koji je u većini slučajeva zaštićen kako bi se zaštitio računalni hardver.

7. GDPR regulativa

Ulaskom u Europsku uniju na snagu su stupili univerzalni zakoni za sve članice koji služe zaštiti osobnih i poslovnih podataka. Jedna od njih je General Data Protection Regulation (GDPR) regulativa koja je usvojena 2016. godine a na snagu stupa 2018.

Ona zamjenjuje direktivu Data Protection Directive 95/46/EC Europske unije iz 1995. godine te je razvijena s ciljem osnaživanja i usklađivanja prava na privatnost i zaštitu osobnih podataka na internetu unutar Europske unije te obaveza zaštite podataka za poduzeća koja posluju s građanima Europske unije putem jedinstvene regulative koja zamjenjuje 28 zasebnih nacionalnih zakona.[71]

Ključne izmjene su:

- pravo na obavijest u slučaju neovlaštenog pristupa osobnim podacima: poduzeća i institucije moraju obavijestiti nacionalno nadzorno tijelo o neovlaštenim pristupima osobnim podacima koji mogu ugroziti privatnost pojedinaca te obavijestiti vlasnika podataka o svim povredama sigurnosti podataka kako bi mogli poduzeti odgovarajuće mjere
- državna tijela ovlaštena za zaštitu podataka će imati ovlasti za izricanje kazni poduzećima čije poslovanje nije usklađeno s GDPR regulativom do visine od 4% njihovih globalnih prihoda
- jedinstveni europski zakon za zaštitu podataka mijenja postojeće zasebne nacionalne zakone. Poduzeća se usklađuju s jednim zakonom umjesto s 28 različitih regulativa. Uštede za poduzeća se procjenjuju na otprilike 2,3 milijarde eura godišnje
- mehanizmi za zaštitu podataka moraju biti ugrađeni u proizvode i usluge u najranijoj fazi razvoja, a zaštita podataka se iz dobre poslovne prakse pretvara u standard[72]

[71] Vodič za EU regulativu u području zaštite podataka - General Data Protection Regulation. ESET. 2017. URL: https://encryption.eset.com/hr/wp-content/uploads/sites/30/2017/01/GDPR-regulativa-i-DESlock-rje%C5%A1enje.pdf (25.9.2017)

[72] Vodič za EU regulativu u području zaštite podataka - General Data Protection Regulation. ESET. 2017. URL: https://encryption.eset.com/hr/wp-content/uploads/sites/30/2017/01/GDPR-regulativa-i-DESlock-rje%C5%A1enje.pdf (25.9.2017)

GDPR osobne korisnike osigurava nizom uvjeta prema kojima tvrtke trebaju na siguran način baratati njihovim osobnim podacima, te tvrtke forsira na implementaciju suvremenih tehnologija poput enkripcije i ostalih praksi zaštite od samih početaka poslovanja.

Zaključak

Osobni podaci su u današnjem umreženom dobu u konstantnom toku.
Kako je čitav ciklus od korisnika, kanala kojim podaci teku do pružatelja usluga ugrožen prijetnjama na internetu, jasna je potreba edukacije i osvještavanja korisnika po pitanju stvaranja sigurne podloge putem koje će pristupati uslugama, te izbjeći moguće rizike koji vrebaju na svakom koraku.Jednostavnim koracima, od redovitog ažuriranja operacijskog sustava i softvera, korištenjem provjerenih usluga, dovoljno jakih zaporki i enkripcijskih standarda, te naposljetku korištenjem zdravog razuma, moguće je izbjeći veliku većinu prijetnji koje vrebaju na svakom koraku. Bez obzira bilo to u osobnom ili poslovnom okruženju, zaštita podataka na internetu od izrazite je važnosti kako za očuvanje vlastite privatnosti i sigurnosti, tako i za zaštitu poslovne od financijskih šteta ili u još gorem slučaju povrede ugleda, koji je u kontekstu poslovnog okruženja oduvijek bio najvažniji aspekt o kojem egzistencija kompanije ovisi.
Štoviše, adekvatna edukacija po pitanju pametnog korištenja sigurnosnih navika većim dijelom je univerzalna i primjenjiva na oba područja, te osobnim korisnicima pruža prednost u pronalasku radnih mjesta kod kojih je to od kritične važnosti.
Praćenje trendova poput društvenih mreža i internetskog bankarstva sa sobom uz brojne prednosti donosi i ranjivosti koje ugrožavaju naše podatke.
Čak i uz maksimalnu lokalnu zaštitu osobni korisnici još uvijek ovise o pružateljima usluga kod kojih se bez obzira na mjere koje poduzimaju po pitanju zaštite uvijek mogu dogoditi kršenja sigurnosti. Iako na te događaje ne možemo utjecati, inteligentnim i pravovremenim reakcijama štetu možemo minimizirati pomoću prethodno stečenog znanja, a redovitim izmjenama po pitanju zakona, kompanije prisiliti na implementiranje sigurnosnih mjera u skladu sa sadašnjim standardima, za neke od kojih se već sutra mogu pronaći ranjivosti koje je potrebno ukloniti. Zbog toga je u interesu korisnika i u interesu pružatelja usluga presudna konstantna edukacija i primjena kako starih, tako i novih mjera sigurnosti.

Literatura

1. 9 KeyElementsof a Data SecurityPolicy. Travelers. 2017. URL: https://www.travelers.com/resources/cyber-security/9-elements-of-a-data-security-policy.aspx (25.9.2017)

2. About. Tails. 2017. URL: https://tails.boum.org/about/index.en.html (25.9.2017)

3. Blahut, Richard E. CryptographyandSecureCommunication. Google Knjige. 2014. URL: https://books.google.hr/books?id=MMH2AgAAQBAJ&pg=PA170&dq=des+encryption&hl=hr&sa=X&ved=0ahUKEwiu2a3GpcDWAhVGMBoKHYXPCCsQ6AEIVTAG#v=onepage&q=des%20encryption&f=false (25.9.2017)

4. Daemen, Joan. Rijmen, Vincent. The Design ofRijndael: AES - The Advanced Encryption Standard. Google Knjige. 2013. URL: https://books.google.hr/books?id=fNaoCAAAQBAJ&printsec=frontcover&dq=aes+encryption&hl=hr&sa=X&ved=0ahUKEwjvv_eRpcDWAhWK2hoKHaufB0YQ6AEILTAB#v=onepage&q=aes%20encryption&f=false (25.9.2017)

5. Data Encryption Standard. 2013. URL: http://www.umsl.edu/~siegelj/information_theory/projects/des.netau.net/Dataencryptionstandard.html (25.9.2017)

6. Deželić, Vanja. Što je enkripcija i zašto je bitna. ICT Business. 2017. URL: http://www.ictbusiness.info/internet/sto-je-enkripcija-i-zasto-je-bitna (25.9.2017)

7. DistroWatch.com: Tails. 2017. URL: http://distrowatch.com/table.php?distribution=tails (25.9.2017)

8. Encryption. New World Encyclopedia. 2013. URL: http://www.newworldencyclopedia.org/entry/Encryption (25.9.2017)

9. EncryptionTimeline. EncryptionPolicy. 2010. URL: https://www.unc.edu/courses/2010spring/law/357c/001/EncryptionPolicy/HistoryEncryption.html (25.9.2017)

10. File:Wana Decrypt0r screenshot.png. Wikipedia. 2017. URL: https://en.wikipedia.org/wiki/File:Wana_Decrypt0r_screenshot.png (25.9.2017)

11. Finley, Klint. Out inthe Open: InsidetheOperating System Edward SnowdenUsed to Evadethe NSA. Wired. 2014. URL: https://www.wired.com/2014/04/tails/ (25.9.2017)

12. Fowler, Dennis. VirtualPrivateNetworks: MakingtheRightConnection. Google Knjige. 1999.
URL:
https://books.google.hr/books?id=dPIrx4Wlv1cC&printsec=frontcover&dq=vpn+what+is+it&hl=hr&sa=X&ved=0ahUKEwi7y_Dq-sDWAhXCWhoKHcHJBjMQ6AEIJDAA#v=onepage&q=vpn%20what%20is%20it&f=false (25.9.2017)

13. FrequentlyAskedQuestions. Mastercard. 2017.
URL: https://www.mastercard.us/en-us/frequently-asked-questions.html#securecode (25.9.2017)

14. Gibbs, Samuel. Dropboxhackleads to leakingof 68m userpasswords on the Internet. TheGuardian. 2016. URL:
https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach (25.9.2017)

15. Gorinjac, Jasmin. Prelazak na HTTPS. Plus.hr Blog. 2017.
URL: https://www.plus.hr/blog/2017/01/26/prelazak-na-https/ (25.9.2017)

16. Grabbe, J. Orlin. The DES AlgorithmIllustrated. 2006.
URL: http://page.math.tu-berlin.de/~kant/teaching/hess/krypto-ws2006/des.htm (25.9.2017)

17. Hale, Benjamin. TheHistoryofSocial Media: SocialNetworkingEvolution! HistoryCooperative. 2015. URL: http://historycooperative.org/the-history-of-social-media/ (25.9.2017)

18. Historyof SSL. IBM KnowledgeCenter. 2017.
URL:
https://www.ibm.com/support/knowledgecenter/en/ssw_i5_54/rzain/rzainhistory.htm (25.9.2017)

19. How PGP works. Introduction to Cryptography. 1999.
URL: https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html (25.9.2017)

20. How To Store YourBitcoins. BitcoinGuides. 2016.
URL: http://bitcoindaily.org/bitcoin-guides/how-to-store-your-bitcoins/ (25.9.2017)

21. Internet bankarstvo – definicija. Moj-bankar. 2012.
URL: http://www.moj-bankar.hr/Kazalo/I/Internet-bankarstvo (25.9.2017)

22. Internetsko bankarstvo. Wikipedia. 2014.
URL: https://hr.wikipedia.org/wiki/Internetsko_bankarstvo (25.9.2017)

23. Intro to Networking - Network FirewallSecurity. UBNT Support. 2017.
URL: https://help.ubnt.com/hc/en-us/articles/115006615247-Intro-to-Networking-Network-Firewall-Security (25.9.2017)

24. Lycett, Andrew. Enigma. BBC History. 2017.
URL: http://www.bbc.co.uk/history/topics/enigma (25.9.2017)

25. MARK ZUCKERBERG's profile - Facebook Picture. Stuffpoint. 2013.
URL: http://stuffpoint.com/facebook/image/315232/mark-zuckerbergs-profile-picture/ (25.9.2017)

26. Open PGP. GoAnywhere MFT. 2017.
URL: https://www.goanywhere.com/managed-file-transfer/encryption/open-pgp (25.9.2017)

27. O socijalnom inženjeringu. Nacionalni CERT. 2017.
URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)

28. O spamu. Nacionalni CERT. 2017. URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)

29. O virusima. Nacionalni CERT. 2017.
URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)

30. Paul, Ian. How—andwhy—youshould use a VPN any time you hop on the Internet. TechHive. 2017.
URL: https://www.techhive.com/article/3158192/privacy/howand-whyyou-should-use-a-vpn-any-time-you-hop-on-the-internet.html (25.9.2017)

31. PayPal. Britannica. 2017. URL: https://www.britannica.com/topic/PayPal (25.9.2017)

32. Peng, Kun. AnonymousCommunicationNetworks: ProtectingPrivacy on the Web. Google Knjige. 2014.
URL:
https://books.google.hr/books?id=mVrNBQAAQBAJ&pg=PA116&dq=the+onion+router&hl=en&sa=X&redir_esc=y#v=onepage&q=the%20onion%20router&f=false (25.9.2017)

33. PrettyGoodPrivacy (PGP). Nacionalni CERT. 2016.
URL: http://www.cert.hr/pgp (25.9.2017)

34. Promoting data securityintheworkplace. UAB. 2017.
URL: http://businessdegrees.uab.edu/resources/infographics/promoting-data-security-in-the-workplace/ (25.9.2017)

35. Ransomware. Nacionalni CERT. 2017.
URL: http://www.cert.hr/socijalni_inzenjering (25.9.2017)

36. Rouse, Margaret. antivirus software (antivirus program). WhatIs. 2014.
URL: http://searchsecurity.techtarget.com/definition/antivirus-software (25.9.2017)

37. Rouse, Margaret. Whatis Advanced Encryption Standard (AES). WhatIs. 2014.
URL: http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard (25.9.2017)

38. Rouse, Margaret. Whatis Data Encryption Standard (DES). WhatIs. 2014.
URL: http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard (25.9.2017)

39. Rouse, Margaret. Whatis data retention. WhatIs. 2014.
URL: http://searchstorage.techtarget.com/definition/data-retention (25.9.2017)

40. Rouse, Margaret. Whatisencryption? WhatIs. 2014.
URL: http://searchsecurity.techtarget.com/definition/encryption (25.9.2017)

41. Rouse, Margaret. Whatis password entropy? WhatIs. 2014.
URL: http://whatis.techtarget.com/definition/password-entropy (25.9.2017)

42. Rouse, Margaret. Whatis Wi-Fi Protected Access (WPA). WhatIs. 2014.
URL: http://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access (25.9.2017)

43. SandboxingDefinition. TechTerms. 2016.
URL: https://techterms.com/definition/sandboxing (25.9.2017)

44. Thebasic AES-128 cryptographicarchitecture. ResearchGate. 2012.
URL: https://www.researchgate.net/figure/230853805_fig1_Figure-1-The-basic-AES-128-cryptographic-architecture (25.9.2017)

45. The Most CommonPasswordsof 2016. KeeperSecurity. 2016.
URL: https://keepersecurity.com/public/Most-Common-Passwords-of-2016-Keeper-Security-Study.pdf (25.9.2017)

46. The Top 20 Valuable Facebook Statistics. Zephoria. 2017.
URL: https://zephoria.com/top-15-valuable-facebook-statistics/ (25.9.2017)

47. Tokenization vs Encryption. Skyhigh. 2017.
URL: https://www.skyhighnetworks.com/cloud-security-university/tokenization-vs-encryption/ (25.9.2017)

48. Top 10 Bitcoin Desktop Wallets. Bitcoinmillionaire. 2014.
URL: http://blog.bitcoinmillionaire-app.com/2014/09/bitcoinmillionaire-top-10-bitcoin-desktop-wallets/ (25.9.2017)

49. Tor Project: Overview. 2015.
URL: https://www.torproject.org/about/overview.html.en (25.9.2017)

50. TRIPLE DES Encryption/Decryption Online Tool. Enkosoft. 2017.
URL: https://enko.us/tools/triple-des-encryption-decryption-online-tool/ (25.9.2017)

51. Villanueva, John Carl. What AES EncryptionIsAnd How It'sUsed To Secure File Transfers. Jscape. 2015.
URL: http://www.jscape.com/blog/aes-encryption (25.9.2017)

52. Vodič za EU regulativu u području zaštite podataka - General Data Protection Regulation. ESET. 2017.
URL: https://encryption.eset.com/hr/wp-content/uploads/sites/30/2017/01/GDPR-regulativa-i-DESlock-rje%C5%A1enje.pdf (25.9.2017)

53. WhatIs a Firewall? Cisco. 2017.
URL: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html (25.9.2017)

54. Whatis a Password. Computer Hope. 2017.
URL: https://www.computerhope.com/jargon/p/password.htm (25.9.2017)

55. WHAT IS A WLAN (WIRELESS LAN OR WIFI)? Winstudent. 2015.
URL: http://www.winstudent.com/what-is-a-wlan-wireless-lan-or-wifi/ (25.9.2017)

56. Whatis TLS/SSL? Microsoft TechNet. 2003.
URL: https://technet.microsoft.com/en-us/library/cc784450(v=ws.10).aspx (25.9.2017)

57. Who startedtheNigerian Prince email scam? Quora. 2016.
URL: https://www.quora.com/Who-started-the-Nigerian-Prince-email-scam (25.9.2017)

58. Yeung. Ken. Whatis Tor andwhydoesitmatter? Thenext web. 2013.
URL: https://thenextweb.com/insider/2013/10/08/what-is-tor-and-why-does-it-matter/ (25.9.2017)

59. Živković, Šime. Što je to rudarenje podataka (eng. Data mining). IMEF. 2016.
URL: http://imef.hr/sto-to-rudarenje-podataka-eng-data-mining/ (25.9.2017)

Sažetak

U radu se bavimo pojmovima sigurnosti i privatnosti u kontekstu internetskog okruženja. Opisati ćemo stvaranje sigurne podloge u obliku hardvera i softvera – operacijskih sustava i pratećih aplikacija koje pokrećemo na njima, te sigurnosnih tehnologija koje nam omogućuju zaštićen pristup kako lokalnoj mreži tako i internetu.
Ukratko ćemo navesti najpoznatije internetske usluge te načine plaćanja koje primjenjujemo na internetu, a posebnu važnost pridodati ćemo sigurnosnim rizicima s kojima se susrećemo pri pristupu tim uslugama te načinima zaštite vezanima uz njih.
Spomenuti ćemo i regulative, u vidu internetskih kompanija i u vidu zakona europske unije, koje korisnike pomažu osigurati time što pružatelje usluga obvezuju na inteligentnu primjenu modernih tehnologija poput enkripcije i sličnih.
Rad će korisnike informirati o najvažnijim praksama pomoću kojih će oni biti u stanju osigurati se prije i tijekom korištenja interneta implementacijom aktualnih sigurnosnih tehnologija i svjesnošću u obliku stečenog znanja o rizicima koji vrebaju.

Ključne riječi: Privatnost, Sigurnost, Enkripcija, Mreže, Rizici