UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Gregor Firbas

Varovanje zasebnosti nekoč in danes

Diplomsko delo

Ljubljana, 2009

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Gregor Firbas
Mentor: doc. dr. Jaroslav Berce
Somentor: dr. Matej Kovačič

Varovanje zasebnosti nekoč in danes

Diplomsko delo

Ljubljana, 2009

Varovanje zasebnosti nekoč in danes

V diplomski nalogi je predstavljen časovni pregled načina in tehnik varovanja informacij vse od najbolj primitivnih oblik steganografije, do bolj sofisticiranih oblik šifriranja, ki so v uporabi danes (na primer.: »wpa2« - protokol za varovanje dostopa do brezžičnega omrežja). Opisane so tudi hekerske metode, tako čisto tehnične kot je napad z grobo silo, do naprednejših, ki vključujejo človeški faktor (npr.: socialni inženiring). Govora je tudi o pomanjkljivostih in težavah pri uporabi spletnih skupnosti ter mogočih nezaželenih posegih v zasebnost posameznika, ki nastanejo zaradi tega. Predstavljeni so tudi argumenti za in proti uporabi šifriranja za splošno javnost ter možni kompromisi za regulacijo. Na koncu je tudi pregled vladnih metod in njihovega načina sodobnega boja proti organiziranemu kriminalu. Ta obsega tako masovni nadzor nad komunikacijsko informacijskimi kanali (na primer: projekt »Echelon« - sistem za masovni nadzor implementiran s strani Ameriške nacionalno varnostne agencije), kot tudi razvoj orodij za pridobivanje podatkov iz računalnika osumljencev (na primer: »Bundestrojaner« - orodje, ki deluje na principu trojanskega konja).

Ključne besede: šifriranje, kriptologija, zasebnost, informacijska varnost, šifrirna metoda

Privacy protection in the past and present

This thesis looks at the evolution of the methods and techniques of providing information security, from the most primitive ones of steganography to the more sophisticated encryption techniques in use today (for example: »wpa2« - a protocol for protected wireless access). Various hacker methods are also described, such as the purely technical attack with brute force and the more advanced attack that involves the human factor (e.g. social engineering). The thesis also deals with the deficiencies and potential problems associated with taking part in online communities, especially the possible unwanted intrusions on the privacy of individuals that can arise from it. Arguments for and against the use of encryption for the general public are also looked at, as are the possible compromises that could be made in this area. There is also a review of the government's methods in fighting organized crime. This methods range from mass surveillance (for example: project »Echelon« - a system for mass surveillance implemented by the American national security agency) to the tools for collecting information from specific computers (for example: »Bundestrojner« - a tool working on the principle of a trojan horse).

Keywords: encryption, cryptology, privacy, information security, encryption method

Kazalo

Kazalo slik

1 Uvod

V Splošni deklaraciji človekovih pravic je zasebnost definirana kot pravica vsakega posameznika, da nadzira dostopnost informacij o samemu sebi. Pravica do zasebnosti tako pomeni, da ima vsak posameznik moč odločati, katere osebne informacije je pripravljen podati, komu jih bo zaupal ter v kateri namen bodo lahko uporabljene (United Nations General Assembly 1984).

Razvoj informacijsko komunikacijske tehnologije in njena množična uporaba je svetu prikrojila nov način življenja. Prvič v zgodovini se je začelo spreminjati splošno dojemanje dimenzij prostora in časa (Janssen in Kies 2001, 3). Takšno dojemanje je in bo prisotno s konverzijo različnih komponent te tehnologije ter zlitjem vseh naprav, ki nam omogočajo njeno uporabo.

Napredek in razvoj sredstev IKT prineseta s seboj dve skrajnosti. Prva je ta, da komunikacija omogoča lažji prenos informacij in njihovo lažjo pretočnost, kar spremeni tudi naš način delovanja in obstajanja ter nam olajša marsikatero delo. Tako lahko rečemo, da praktično že skoraj vsak izmed nas živi pravo »e-življenje«, kar se kaže tudi v velikem razcvetu elektronskega poslovanja; kot je na primer spletno bančništvo, spletno nakupovanje, e-uprava ipd. Druga skrajnost pa je ta, da smo skupaj z eksponentnim razvojem interneta in drugih informacijsko komunikacijske tehnologije tudi priča razvoju internetnega kriminala, ki ga je iz dneva v dan več. Zato se vedno večji pomen pripisuje t.i. informacijski varnosti, ki bo v prihodnjih letih igrala še pomembnejšo vlogo.

V diplomski nalogi bomo izpostavili in tako poskušali raziskati tri raziskovalna vprašanja:

- Kako je potekal razvoj kriptografije?
- Katere kriptografske metode so danes relevantne in v uporabi?
- Katere tehnike pridobivanja šifriranih podatkov poznamo?

Za raziskovanje te tematike, se je za najbolj primerno izkazala kvalitativna metoda raziskovanja s pomočjo analize tekstov.

V prvem delu diplomske naloge bodo opisane primitivne oblike varovanja informacij kot je steganografija, ki se je uporabljala že pred 4000 leti. V nadaljevanju bo sledila pot do razvoja prvih šifrirnih strojev, za katere se je izkazalo, da so v drugi svetovni vojni odigrali pomembno vlogo. V času začetkov razvoja informacijsko komunikacijske tehnologije se je potreba po varovanju informacij in zasebnosti iz vojaških krogov prenesla tudi v vsakdanjik posameznika. V današnji informacijski dobi si življenja brez šifriranja praktično več ne moremo predstavljati, zato bo sledil opis aktualnih metod za varovanje zasebnosti.

Ker pa metode za šifriranje postajajo vedno bolj sofisticirane in jih je težje razbiti, to predstavlja problem pri boju proti organiziranemu kriminalu. Vlade so kot odgovor na to dejstvo skupaj s svojimi represivnimi organi pripravile metode boja proti kriminalu, ki pa bodo opisane v nadaljevanju. Na koncu bomo opozorili tudi na težave in pasti uporabe spletnih socialnih omrežij, ki v zadnjem času postajajo vedno bolj priljubljene in združujejo ogromno število uporabnikov ter njihovih osebnih podatkov.

2 Šifriranje

2.1 Steganografija

Želja in potreba po tajnem komuniciranju in tajnih komunikacijah sega daleč v preteklost, že v obdobje pred našim štetjem. Ker pa takrat še niso poznali oziroma izumili tehnik, s pomočjo katerih bi lahko prikrili pomen besedila, ampak so bili prisiljeni, da so prikrili že sam obstoja sporočila. Takemu načinu tajne komunikacije, pri katerem skrijemo besedilo, se imenuje steganografija. Beseda izvira iz grškega jezika (*steganos* - prikrit, *graphein* - pisanje), njen dobesedni prevod pa je prikrito pisanje. Tako je iz zgodovine znanih že veliko oblik steganografije (Singh 2006, 20-21).

Naštetih je nekaj najbolj znanih primerov:

- Kitajci so svoja sporočila prikrili tako, da so koščke svile, na katere so napisali besedilo, pomočili v vroč vosek iz katerega so nato oblikovali majhne kroglice. Te kroglice je nato pogoltnil sel (Singh 2006, 20-21).

- Znan je tudi primer, ko so sužnja pobrili in mu na glavo vtetovirali ali vžgali sporočilo in nato počakali, da so mu ponovno zrastli lasje (Singh 2006, 20-21).

- Sporočila so skrivali tudi tako, da so na lupino kuhanega jajca pisali s pomočjo mešanice kisa in galuna. Tekočina je prodrla pod lupino jajca in tako je bilo besedilo vidno le znotraj na površini jajca (Singh 2006, 20-21).

- Eden izmed najbolj znanih načinov za skrivanje besedila pa je uporaba tako imenovanega skrivnega črnila, ki je pri normalni sobni temperaturi nevidno. Če list papirja segrejemo, se besedilo obarva rjavo. Kot nevidno črnilo so uporabljali mleko, kis, limonin sok ter tudi urin (Singh 2006, 20-21).

Glede na vse te primere je razvidno, da je steganografija res nudila določeno stopnjo varnosti in omogočila tajno komuniciranje. Takšne oblike steganografije bilo varno uporabljati samo dokler se za te steganografske trike ni razvedelo. Slabost je bila v tem, da ko so slej kot prej ugotovili za določen način skrivanja besedila in tako je bilo

tajnosti konec. Tako je bilo besedilo berljivo za vsakogar, ki ga je znal prebrati, za kar je bil predpogoj pismenost bralca, avtor skrivnega besedila pa za to velikokrat ni izvedel. Zaradi tega je bilo smotrno zraven skrivanja sporočil uporabiti tudi metodo skrivanja pomena samega sporočila in prav tukaj je začetek razvoja kriptografije oziroma šifriranja.

2.2 Začetki šifriranja

Prva dokumentirana uporaba kriptografije sega v leto 1900 pred našim štetjem, ko so Egipčani pri inskripciji uporabili ne-regularne hieroglife (Kahn v Dupuis 1996, 71) . Naslednji znan primer kriptografije zasledimo tudi pri Mezopotamcih okoli leta 1500 pred našim štetjem, ki so svoje postopke za izdelavo izdelkov iz gline šifrirali preden so jih zapisali na glinene plošče, v upanju da bi jih bili zmožni razumeti le oni sami (Kahn v Dupuis 1996, 75). Okoli leta 600-500 pred našim štetjem so temu sledili Hebrejci, ki so besedila šifrirali s pomočjo enostavne zamenjave črk, pri čemer so uporabljali obrnjeno abecedo (Kahn v Dupuis 1996, 77). Ta način šifriranja se imenuje Atbash in je prikazan na spodnji sliki (glej Sliko 2.1).

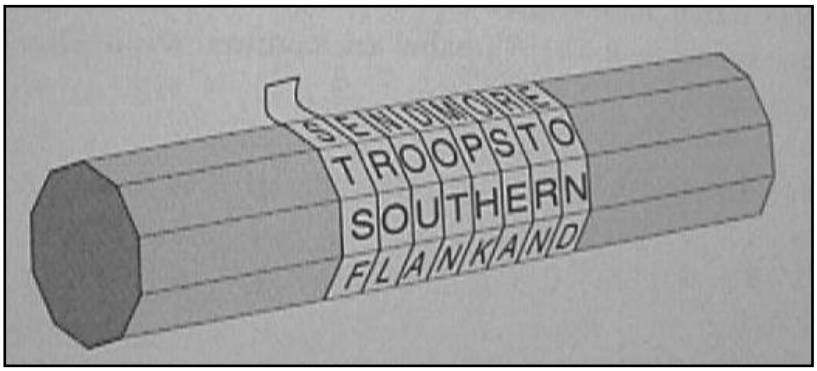
Slika 2.1 Prikaz načina uporabe Atbasha.

abeceda	A	B	C	…	V	Z	Ž
obrnjena abeceda	Ž	Z	V	…	C	B	A

Prva znana iznajdba naprave, s katero je bila mogoče mehansko šifriranje, je bila tako imenovan skital. Iznajdbo skitala pripisujemo Grkom, nastal bi naj leta 478 pred našim štetjem (Kahn v Dupuis 1996, 82). Skital ni bil nič drugega kot lesena palica, okoli katere so navili usnjen trak ter na njega napisali besedilo (glej Sliko 2.2). Sel je nato ta usnjeni trak uporabil kot pas. Ko je prispel do naslovnika, je ta trak spet ovil okoli lesene palice istega premera kot tiste, ki jo je uporabil avtor besedila, da je lahko pravilno prebral sporočilo. Tako sta avtor in naslovnik morala biti že v naprej

dogovorjena kakšno palico bosta uporabila. Uporaba te metode je zelo lep prikaz uporabe kombinirane tehnike kriptografije in steganografije za doseganje večje stopnje tajnosti. Skital predstavlja prvo dokumentirano uporabo kriptografije v državne oziroma v vojaške namene.

Slika 2.2: Prikaz načina delovanja skitala.



Vir: Beckwith (2008).

Kriptografijo je nato v državne namene uporabljal tudi Julij Cezar. Rimski imperij je namreč bil za takratne razmere izredno velik, zato je bilo komuniciranje z oddaljenimi deli imperija zelo oteženo in nevarno. Sli so namreč morali prepotovati ogromne razdalje, kar je povečalo možnost, da jih bodo zajeli nasprotniki. Cezarjevo kodiranje je potekalo s pomočjo ključa, ki nam pove za koliko mest je šifrirna abeceda pomaknjena v levo (glej Sliko 2.3).

Slika 2.3: Na sliki sta vidni abecedi šifrirani po Cezarjevem postopku s ključema 3 in 5 (Julij Cezar bi naj uporabljal ključ 3).

nešifrirana abeceda	A B C D E F G H I J K L M N O P R S Š T U V Z Ž
šifrirana abeceda(ključ:3)	D E F G H I J K L M N O P R S Š T U V Z Ž **A B C**
šifrirana abeceda(ključ:5)	F G H I J K L M N O P R S Š T U V Z Ž **A B C D E**

Problem pri uporabi vseh teh metod je ta, da se da njihovo zaščito dokaj hitro in enostavno razbiti s pomočjo analize frekvenc črk v abecedi. Na začetku postopka je potrebno opraviti analizo frekvenc črk pri dovolj dolgem standardnem besedilu oziroma še bolje pri daljših besedilih. S tem dobimo vpogled kolikokrat se bo pojavila katera izmed črka abecede. Naslednji korak je analiza frekvence ponavljanja znakov (lahko so črke ali kakršni koli drugi znaki) v šifriranem besedilu. Nato lahko s primerjavo obeh frekvenc ugotovimo kateri znak predstavlja katero črko in tako z malo vztrajnosti razbijemo šifrirano besedilo.
Naslednji pomemben koraki v zgodovini kriptologije je razvoj kompleksnejših mehaničnih strojev. S pomočjo teh lahko na eni strani avtor besedila z lahkoto zašifrira sporočilo, na drugi strani pa jo naslovnik s pomočjo iste naprave z lahkoto dešifrira, seveda pod pogojem, da pozna pravi ključ, po katerem je sporočilo šifrirano. Tako je s pomočjo šifrirnih strojev in uporabo naprednejših šifrirnih tehnik, šifriranje postalo veliko boljše in varnejše vendar težje razrešljivo za kriptoanalitike.

2.3 Šifriranje nekoč

2.3.1 Šifrirni valj (»cipher disk«)

Prva prava naprava za šifriranje (v bistvu je pred tem bil že skital, za katerega pa ne moremo trditi da je ravno naprava oziroma stroj), ki je omogočila nadaljnji razvoj šifrirnih strojev, je bila šifrirni valj. Deloval je na principu substitucije abecede. Na eni strani valja so bile črke abecede, na drugi strani pa njim pripadajoče črke nadomestne abecede uporabljane za šifriranje. Šifrirni valj je leta 1467 izumil Leon Battista Alberti, znan italijanski filozof in arhitekt (Singh 2006, 145-146).

2.3.2 Šifrirni koleščk (»cipher wheel«)

Šifrirni koleščk je naprava, za katero se domneva, da jo je v 18. stoletju izumil Thomas Jefferson. Naprava je bila sestavljena iz 36 lesenih obročkov vpetih na kovinski palici (glej Sliko 2.4). Na vsakem obročku je bila na eni strani označena

mešana abeceda, na drugi strani pa »prava« abeceda. Obročki so se na palici lahko prosto premikali in vrteli. Kriptograf je tako dolgo vrtel obročke, da je s pomočjo označene abecede sestavil sporočilo dolgo 36 znakov. Nato je pogledal kateri znaki šifrirane abecede pripadajo znakom »prave« abecede ter zapisal zašifrirano besedilo. Z naslovnikom se je moral ali v naprej dogovoriti kateri ključ bo uporabil ali pa mu ključ posredovati.

Lahko je namreč spreminjal vrstni red obročkov na palici, vsak obroček pa je bil označen s številko ter s tem spreminjal ključ šifriranja. Šifriranje s to napravo se je uporabljalo vse do konca prve svetovne vojne. Uporabljala pa se je predvsem za meddiplomatsko komunikacijo, ki je največkrat potekala v francoščini (National Security Agency 2009a).

Slika 2.4: Slika prikazuje napravo s vpetimi šifrirnimi obročki.

Vir: National Security Agency (2009c).

2.3.3 Enigma

Enigma je najbolj znana elektro-mehanska šifrirna naprava, ki jo je izumil in leta 1919 patentiral berlinski inženir Arthur Scherbius. Naprava je stopila v množično uporabo med drugo svetovno vojno. Enigma je na prvi pogled izgledala kot pisalni stroj. Delovala je s pomočjo med seboj povezanih rotorjev, ki so vsaki črki priredili

nek drug znak. Za varnost je bilo poskrbljeno tudi tako, da je naprava vsaki črki v besedilu, ki se je ponovila, priredila vedno drug znak. Tako so uspešno eliminirali možnost razbijanja šifre s pomočjo uporabe analize frekvenc. Da bi še dodatno izboljšala varnost so vsak dan zamenjali vrstni red rotorjev po vnaprej določenem ključu. Enigma je tako delovala kot brezpogojno varna naprava, katere šifrirana besedila je nemogoče razbiti, v kolikor ne poseduješ pravega ključa. Vendar pa je tudi Enigma imela svoje slabosti in pomanjkljivosti. Tako je poljskemu kripterju uspelo s pomočjo svojih kolegov matematikov leta 1923 najti način dešifriranja sporočil poslanih z Enigmo, brez tega da bi vedeli kakšen ključ je uporabljen. Svoje dosežke so nato posredovali Francozom in Britancem, ki so prav zaradi tega bili že pred izbruhom druge svetovne vojne, sposobni dešifrirati prestrežena nemška sporočila. Leta 1942 pa je Enigma doživela pomembno posodobitev, saj je bil napravi dodan še četrti rotor za vsako črko. Tako je bila komunikacija s pomočjo Enigme nekaj časa ponovno varna, a ne za dolgo. V boj proti njej so se vključile tudi Združene države Amerike in tako so vsi skupaj že naslednje leto izumili tako imenovan »Navy Bomber«, ki je znal učinkovito razbijati šifrirana besedila. Veliko se je govorilo tudi o tem, da je prav izum »Navy Bomber-ja« krivd, da so Združene države Amerike zmagale vojno v Evropi (Singh 2006, 148-181; National Security Agency 2009b).

2.4 Šifriranje danes

Dandanes, ko smo v tako imenovani informacijski dobi, so informacije postale ena izmed najdragocenejših stvari na svetu. Zaradi pomembnosti digitalnih informacij kot so na primer bančne transakcije, ki vsakodnevno pretakajo po svetovnem spletu, se je pojavila potreba po šifriranju tudi v vsakdanjem življenju.

Tako lahko ločimo dva različna načina šifriranja podatkov in sicer; simetrično šifriranje in asimetrično šifriranje (Kovačič 2006, 91-92).

Pri simetričnem načinu šifriranja se za šifriranje in dešifriranje uporablja isti ključ, pri asimetričnem pa gre za uporabo dveh različnih ključev (Kovačič 2003, 64).

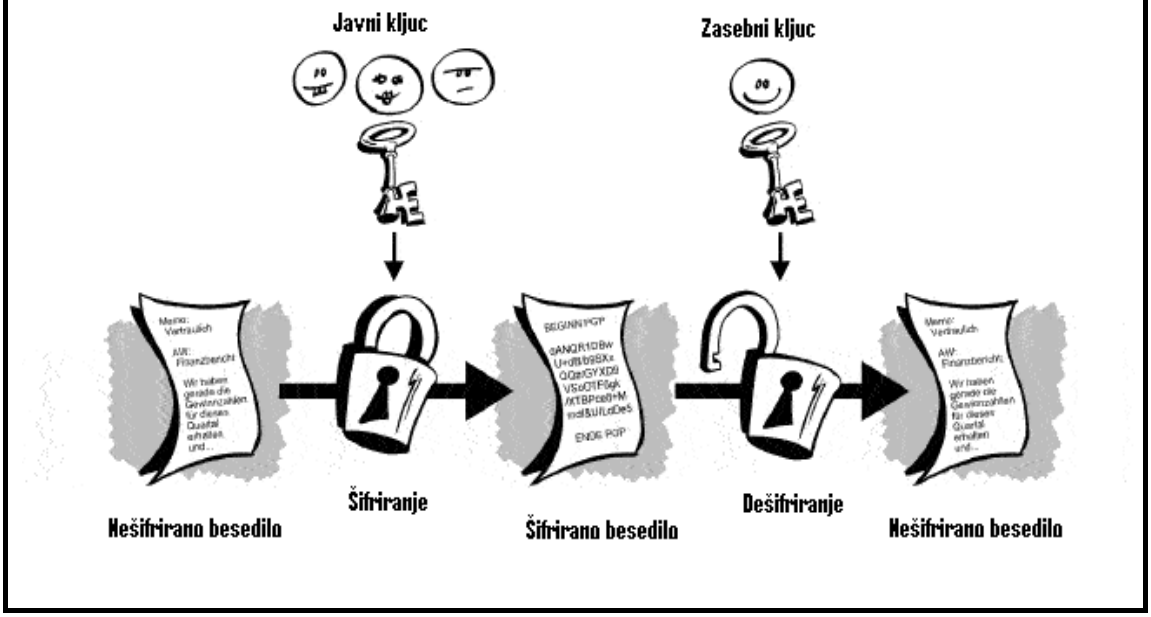
Prednost asimetričnega šifriranja je, da ni potrebno poskrbeti za varen prenos ključa (t.i. varen kanal). Asimetrično šifriranje namreč poteka po principu uporabe javnega in zasebnega ključa. Pošiljatelj sporočilo šifrira s pomočjo uporabe prejemnikovega javnega ključa (javni ključ je javno objavljen in prosto dostopen vsakomur), ta pa ga

lahko nato dešifrira s pomočjo svojega zasebnega ključa (zasebni ključ varno hrani vsak posameznik) (Tulloch 2003, 26).

2.4.1 RSA

RSA je šifrirni algoritem, ki so ga leta 1977 na MIT-ju (»Massachusetts Institute of Technology«) izumili Ron Rivest, Adi Shamir in Leonard Adleman. Algoritem deluje s pomočjo javnega in zasebnega ključa (Kovačič 2003, 65). Postopek je tak, da morata imeti tako avtor sporočila kot tudi naslovnik vsak po 2 ključa; javnega, ki ga morata javno objaviti in zasebnega, ki je tajen in ga poznata samo onadva. Pošiljatelj neko besedilo zakodira s pomočjo naslovnikovega javnega ključa in šifrirano besedilo pošlje, dešifrira pa ga lahko samo lastnik pripadajočega zasebnega ključa (v tem primeru naslovnik) (glej Sliko 2.5). To predstavlja povečano varnost in enostavnost, saj ključa ni več potrebno pošiljati z besedilom in zato ne potrebujemo »varnega kanala« po katerem bi ključ prenesli. RSA zaradi svoje dobre zaščite velja za praktično nezlomljivega in se zaradi tega množično uporablja pri internetnem bančništvu.

Slika 2.5 : Prikaz šifrirnega postopka RSA.



2.4.2 PGP (» Pretty Good Privacy«) in zgodba Phila Zimmermanna

Phil Zimmemann se je po izidu RSA algoritma odločil, da napiše uporabniku prijazen program, s katerim bi lahko vsak posameznik zavaroval svojo spletno zasebnost, saj je po njegovem mnenju to ena izmed temeljnih človekovih pravic. Kot izreden računalniški strokovnjak se je lotil dela z željo, da ustvari za uporabnika prijazen program, ki bi pa bil dovolj hiter in primeren za vsakodnevno uporabo, hkrati pa ne bi smel presegati tehničnih specifikacij povprečnega domačega računalnika. Tako je leta 1991 nastal program PGP, ki ga je Phil kot brezplačnega objavil na Usenetu. Na program je dobil izredno dober odziv pri uporabnikih, ki so se mu preko interneta zahvaljevali, da lahko končno svobodno komunicirajo in da je njihova zasebnost varovana pred totalitarnimi režimi.

Pri splavitvi svojega programa pa je naletel tudi na velike težave. Prva težava se je pojavila pri algoritmu in načinu kodiranja s pomočjo RSA patenta podjetja RSA Data Security. Ker pa jim s svojim programom ni želel konkurirati, saj je bil program namenjen le zasebni uporabi in ne v komercialne namene, je upal da mu bo RSA Data Security odobrila uporabo in mu podelila licenco za uporabo patenta. Pri tem se je uštel, saj se sprva to ni zgodilo.

Drugi problem, s katerim se je Zimmermann soočil, je bil še bolj pereč. To je bil osnutek zakona, ki jo je ameriški senat obravnaval že leta 1991 a je sprejem zakona zaradi pritiskov RSA Data Security predložil v kasnejšo obravnavo. Zloglasna klavzula zakona se je glasila: »Po mnenju kongresa je nujno, da ponudniki elektronskih komunikacijskih storitev in izdelovalci elektronskih komunikacijskih naprav zagotavljajo, da bodo svoje komunikacijske sisteme opremili tako, da bodo vsebine odprtih besedil pri telefonskih pogovorih, pri prenosu podatkov in pri drugih sporočilih lahko na voljo državnim službam, če bi imele te za to zakonito dovoljenje« (Ron Rivest v Singh 2006, 329).

Zimmermannu je zato za vrat začel dihati tudi FBI, ki ga je leta 1993 obtožil ilegalnega izvoza orožja, saj ameriška vlada med načine oboroževanja kot so na primer rakete, minometi, strojnice šteje tudi orodja in naprave za šifriranje kot tudi šifrirno programsko opremo. Za izvoz vsega tega iz države je po (takratnem) zakonu bilo potrebno pridobiti posebne odobritve s strani zunanjega ministrstva. Postopek proti njemu, zaradi ilegalnega trgovanja z orožjem je nato tekel naslednja 3 leta, leta

1996 pa je bil Zimmermann oproščen vseh obtožb. Prva obtožba zaradi uporabe patentirane programske opreme in algoritma RSA je bila ovržena potem, ko je RSA Data Security na koncu le popustila in mu podelila potrebno licenco in s tem umaknila tudi svojo tožbo. Drugo obtožba, obtožba FBI, da je Zimmermann iz države izvozil orožje, pa je padla zaradi večjih nerazrešenih pravnih vprašanj v zvezi s spletom kot tudi glede načina objave njegovega programa. Na oprostitev je vplivala tudi močna podpora vplivnih posameznikov in ustanov. Zadeva pa je šla celo tako daleč, da se je ustanovil tudi fond za denarno pomoč, s pomočjo katerega je Zimmermann plačeval svoje zagovornike. Dejstvo je bilo, da če bi bil program »izvožen« na nekem mediju kot disketa, bi se to brez težav lahko smatralo kot kriptografska naprava. Po drugi strani pa je Zimmermann objavi izvorno kodo programa, ki pa se ne more obravnavati kot popolno delujoč šifrirni sistem. S tem tako v bistvu ni izvozil šifrirne naprave ampak samo svoje znanje kar pa ni prepovedano. Tako je s pravnega stališča obstajalo preveč zakonskih pomanjkljivosti in nejasnosti ter premalo dokazov, da bi lahko Zimmermanna spravili za zapahe. Program PGP je v času sojenja postal že tako razširjen po celem svetu, da je bilo enostavno nemogoče omejiti njegovo uporabo. V vsem tem času je namreč s pomočjo Tehnološkega inštituta v Massachusettsu (MIT) izšla tudi knjiga z izvorno kodo programa PGP, kar je bil čisto legalen izvoz, zraven v tega pa patent RSA v Evropi ne velja (Lucas 2006, 2-4; Singh 2006, 320-331; Roblimo 2007).

2.4.3 Digitalni podpis

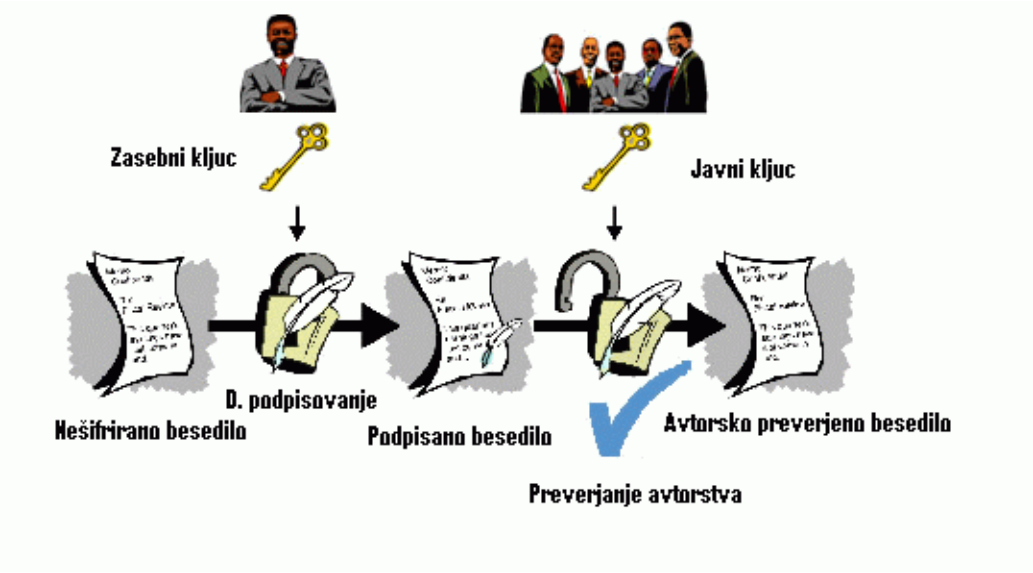
Še ena izmed zelo dobrih lastnosti PGP-ja je možnost kreiranja digitalnega podpisa. Ker v digitalnem svetu ne moremo spletne pošte in dokumentov podpisati lastnoročno in tako izkazati pristnost avtorstva, je digitalni podpis pomembno odkritje, ki omogoča uspeh naše informacijske dobe. Tako se digitalni podpis vedno bolj uporablja pri podpisovanju spletne pošte. Digitalni podpis, ki nam ga izda za to pristojna služba, nam celo omogoča oddajanje raznih dokumentov preko spleta, kot je na primer oddaja dohodnine.

Koncept digitalnega podpisa, ki sta ga razvila Whitfield Diffie in Martin Hellman, deluje na obratnem principu kot šifriranja z javnim in zasebnim ključem. V »klasičnem«« postopku šifriranja besedila se javni ključ uporablja za šifriranje,

zasebni ključ pa za dešifriranje. Pri digitalnem podpisu pa je ta postopek obrnjen tako, da je zasebni ključ tisti s pomočjo katerega se šifrira in javni ključ tisti s katerim se dešifrira (glej Slika 2.6). Res je, da ta sistem ne nudi varnosti, saj je javni ključ dostopen vsem in tako lahko vsak dešifrira sporočilo, vendar pa je to dokaz, da je sporočilo bilo šifrirano s pripadajočim zasebnim ključem, ki si ga lasti samo avtor besedila in s čimer dokazuje avtorstvo (Singh 2006, 327-328).

Torej, če želi nekdo poslati šifrirano sporočilo in dodati svoj digitalni podpis, mora uporabiti oba dva šifrirna postopka, najprej besedilo šifrira po postopku za dodajanje digitalnega podpisa in nato še po »klasičnem« postopku PGP. Ti dve združeni metodi tako predstavljata vzajemno varnost, saj avtor ve, da bo njegovo sporočilo ostalo tajno in ga bo zmožen prebrati le naslovnik. Na drugi strani pa je prejemniku zagotovljeno, da je domnevni avtor sporočila tudi dejanski avtor.

Slika 2.6: Prikaz šifrirnega postopka pri digitalnem podpisu.



2.4.4 WEP

WEP oziroma »Wired Equivalent Privacy" je prvi standardni šifrirni mehanizem uporabljen pri brezžičnem prenosu podatkov po standard IEEE 802.11. Wep šifriranje

deluje na tak način, da vse naprave ki dostopajo do brezžičnega omrežja, uporabljajo do štiri skrivne simetrične ključe. Ta ključe je potrebno pred tem namestiti na vsako izmed naprav. To je sicer prva pomanjkljivost tega načina šifriranja, ki je še posebej opazna pri večjih brezžičnih sistemih in pri brezžičnih omrežjih, kjer se uporabniki oziroma naprave hitro oziroma pogosto spreminjajo. Glavna pomanjkljivost WEP-a se je pokazala leta 2001, ko so uspeli šifrirni mehanizem popolnoma razbiti. Takratna metoda je omogočala obnovitev šifrirnega ključa v eni do dveh urah na povprečnem potrošniškem računalniku. Današnje metode to omogočajo že v manj kot 60 sekundah kljub uporabi 256 bitov dolgih šifrirnih ključev (Beck in Tews 2008, 1-2). Uporaba WEP šifriranja tako ni priporočljiva, saj praktično ne nudi varnosti in s tem povezane zasebnosti.

2.4.5 WPA

WPA oziroma »Wi-Fi Protected Access« predstavlja nadgradnjo šifrirnega mehanizma WEP. Implementira večino IEEE 802.11i standarda za brezžičen prenos podatkov. WPA za razliko od WEP-a nudi samodejno menjavo šifrirnega ključa. Uporabnikom brez naloženega ključa za dostop omogoča uporabo »pre-shared« ključev (ključ, ki se kreira za občasne uporabnike), za dostop do omrežja pa morajo uporabniki imeti geslo (Beck in Tews 2008). Kljub izboljšavi na področju šifrirnega algoritma, ki ga uporablja WPA, so ga razbili leta 2008. Postopek je na povprečnem računalniku trajal približno 15 minut. Izpopolnjena metoda za razbijanje WPA šifriranja je bila predstavljena 2009, kjer je raziskovalcema uspelo šifriranje razbiti v manj kot 60 sekundah (Ohigashi in Morii 2009).

2.4.6 WPA2

Po odkritju ranljivosti šifrirnega protokola WPA je tega nasledil standard WPA2, ki za šifriranje uporablja naprednejšo metodo AES (»Advanced Encryption Standard«). Pomanjkljivosti in ranljivosti te metode varovanja brezžičnega prenosa podatkov za enkrat še niso bile odkrite, tako da trenutno velja za najbolj varnega in edinega priporočljivega (McMillan 2009).

2.5 Dileme glede uporabe šifriranja za širšo javnost

Po objavi Zimmermannovega programa PGP se je o šifriranju namenjenemu širši javnosti vnela velika razprava. Na eni strani so zagovorniki šifriranja zavzeli stališče, da bi le-to moralo biti javno dostopno in dovoljeno vsem. Spet na drugi strani pa so se proti temu z različnimi argumenti borile vladne organizacije.

2.5.1 Argumenti proti uporabi šifriranja

Glavni problem pri vsem tem predstavlja bojazen, da v kolikor bo/je šifriranje javno dostopno, bodo dostop do naprednih kriptografskih tehnologij imeli tudi zločinci, kot so teroristi, prekupčevalci z orožjem in ostale organizirane kriminalne združbe. Z uporabo teh šifrirnih sredstev bi zato vladnim organizacijam bilo onemogočeno izvajanje uspešnega prisluškovanja oziroma prestrezanja in branja komunikacij, kar pa bi pomenilo velik udarec pri pregonu in zbiranju dokazov potrebnih za sojenje. Dober primer pri katerem je prisluškovanje odigralo ključno vlogo je iz 80ih letih, ko je policija imela ogromne težave pri lovljenju osumljencev, ker je mafija grozila vsem, ki so si drznili pričati proti njej. Poleg tega je veljal še vedno *ómerta, »*zakon molčečnosti« (Singh 2006, 332). Zaradi vsega tega je bila edina možnost za pridobitev ključnih dokazov prav prisluškovanje. Tako so sprejeli zakon, da je prisluškovanje dovoljeno, vendar samo v primeru, ko je to odobreno s strani sodišča. V prid prepovedi uporabe šifriranja navajajo tudi dejstva, da je že sedaj ogromno primerov, ko so člani organiziranih kriminalnih združb za komuniciranje uporabljali šifrirne postopke in jih zato niso mogli uspešno uloviti oziroma je delo policije bilo močno ovirano. Eden izmed takih primerov je primer, ko je ilegalni sindikat iger na srečo v Združenih državah Amerike uporabljal šifriranje za varovanje svojih dokumentov. Drug primer je uporaba šifriranja Ramzi Jusef-a, ki je na tak način uspešno prikrival svoje načrte za sodelovanje pri napadu na Svetovni trgovinski center »WTC« (Singh 2006, 332).

2.5.2 Argumenti za uporabo šifriranja

Eden izmed glavnih argumentov zagovornikov šifriranja je, da ima vsak človek pravico do zasebnosti, kar je določeno v ustavi pod temeljnimi človekovimi pravicami. Sicer ne nasprotujejo temu, da bi se prisluškovalo le takrat kadar gre za nek utemeljen sum kaznivega dejanja in je potrebno prisluškovati zaradi zbiranja dokazov. Skrbi jih predvsem dejstvo, da NSA (Ameriška nacionalna varnostna agencija) prisluškuje komunikacijam in jih nadzoruje masovno in ne le ciljno. Dokaz temu je sistem svetovnega omrežja prisluškovalnih naprav, ki ga ima NSA skupaj še z nekaj drugimi varnostno obveščevalnimi agencijami. Največja znana bazna postaja iz tega sistema je Menwith Hill Signals Intelligence Base v Yorkshiru, deluje pa po sistemu Echelon. Echelon je kompleksen sistem super računalnikov, ki je sposoben realno-časovno spremljati vse oblike telekomunikacij, kot so telefonski pogovori, internetna pošta in telefaksi. Informacije ki jih dobi nato primerja z že vnaprej pripravljenimi listami in na ta način izlušči informacije, ki bi bile koristne za nadaljnjo uporabo (Schneier 1999). Zagovorniki so tako mnenja, da je uporaba šifriranja nujno potrebna, za zaščito njihove digitalne zasebnosti, ki se na ta način krši, saj po 12. členu Splošne deklaracije o človekovih pravicah velja: »Nihče ne sme biti izpostavljen samovoljnim posegom v njegovo zasebno življenje, njegovo družino, njegov dom ali njegovo korespondenco, pa tudi ne napadom na njegovo čast in njegov ugled. Vsak človek ima pravico do zakonite zaščite proti takšnim posegom ali napadom« (United Nations General Assembly 1984).

Problem pri vsem tem je tudi, da je takšne sisteme moč tudi zlorabljati. Kot primer vzemimo, da se v neki državi približuje čas volitev. Ker je varnostna agencija državna, odgovarja vladi. Vlada tako zaukaže prisluškovanje vsem komunikacijam njihovih političnim nasprotnikov z razlogom, da izve vse njihove načrte in se na njih pripravi ter tako z lahkoto diskreditira svoje nasprotnike in tako brez težav in demokracije ponovno zmaga na naslednjih volitvah. Da tu ne gre za fiktivna dejstva, priča poročilo francoske nadzorne komisije Sécurité, da se samo v Franciji zgodi približno 100.000 ilegalnih prisluškovanj, ki niso bila potrjena s strani sodne oblasti (Privacy international 2003).

Z uporabo šifriranja se možnost za takšno množično prisluškovanje drastično zniža, saj morajo prisluškovanja biti ciljna za katere je potrebno uporabljati tudi druge

metode, ki so časovno in v praksi neizvedljive pri masovni populaciji. Projekt Echelon bi zaradi tega postal neuporaben.

2.5.3 Možni kompromisi

Eden izmed najbolj zanimivih komentarjev na temo omejevanja in preprečevanja kriptografije je vsekakor, komentar Rona Rivesta, enega izmed izumiteljev RSA:

> *Slaba politika je, če določeno tehniko brez razlik obsojamo samo zaradi tega, ker je nekaj kriminalcev morda sposobnih, da bi jo izrabili v svojo korist. Tako lahko vsak ameriški državljan kupi par rokavic, čeprav bi lahko vlomilec v njih oropal hišo, ne da bi za seboj pustil prstne odtise. Kriptografija je tehnika za zaščito podatkov, rokavice pa so tehnika za zaščito rok. Kriptografija varuje podatke pred hekerji, pred gospodarskim vohunjenjem in mojstrskimi sleparji, rokavice pa varujejo roke pred urezi, praskami, vročino, mrazom in okužbami. S kriptografijo se lahko zavarujemo pred prisluškovanjem FBI, z rokavicami pa lahko preprečimo analizo prstnih odtisov* (Singh 2003, 336).

Iz tega lahko razberemo, da ni smiselno obsojati kriptografije, ampak je potrebno delati na napredku novih policijskih metod za boj proti kriminalu. Ob branju vseh teh argumentov za prepoved in omejevanje šifriranja, se nisem mogel znebiti občutka, da za vsem tem stoji mnogo več kot se sprva kaže.

Kot vemo, je možno uporabiti mnogo drugih bolj naprednih metod za iskanje zločincev in dokazov, vendar le ti terjajo usmerjenost v specifičen cilj. Pri tem je potrebno omeniti, da šifriranje s pomočjo algoritma RSA na prvi pogled res deluje nezlomljivo, vendar če se zadeve lotimo iz drugega konca se nam ponuja veliko različnih možnosti. Eden izmed takih primerov je socialni inženiring, uporaba raznoraznih »keyloger-jev« in ne nazadnje tudi »temptest attack« (vsi ti izrazi so pojasnjeni v nadaljevanju), za pridobitev potrebnih ključev oziroma gesel, ki so potrebni za prisluškovanje oziroma nadzor.

Po mojem mnenju je eden izmed poglavitnih razlogov prizadevanja vlad za prepoved šifriranje v tem, da si s sistemi za masovno prisluškovanje kot je Echelon ustvarjajo iluzijo o nadzorovanju množic in vzpostavljanju neke prikrite orwellske države. Kot

je jasno razvidno je množičen nadzor dejansko samo iluzija, kar je nazorno vidno iz primera, ki se je zgodil 11. septembra v New Yorku. V tem primeru so varnostne agencije dejansko imele dovolj podatkov, da bi preprečile tragedijo ki se je zgodila ob napadu na WTC, a zaradi prevelike količine informacij teh niso uspeli pravi čas obdelati.

Naslednja brezpomenska stvar je tudi ta, da še vedno potek razprava omejevanju in prepovedi kriptologije. Nihče namreč ne pomisli, da je to že skoraj nemogoče v času, ko je od splavitve prvega programa, ki je vključeval RSA, preteklo že toliko časa in to v času ko se informacije brezkompromisno s skoraj svetlobno hitrostjo in brez omejitev pretakajo po svetu. Pri vsem tem pa nekateri še vedno živijo v utopiji, da bodo organizirane kriminalne združbe zaradi prepovedi prenehale z uporabo kriptografije.

Ena izmed možnih predlaganih rešitev je bil kompromis, da bi se angažirala neka neodvisna tretja stran (»Third party«), pri kateri bi zakonsko moral vsak posameznik deponirati svoje zasebne šifrirne ključe. Ti ključi bi bili na voljo le oblasti pregona in to samo v primeru, ko bi to odobrilo sodišče. Ta predlog je spodletel, kar je po mojem mnenju čisto pravilno, sploh če upoštevamo spodaj omenjeno zgodbo o Crypto AG.

3 Dešifriranje

Hkrati z razvojem šifriranja podatkov, so se začele pojavljati tudi metode za pridobivanje le teh. V preteklosti je šlo predvsem za same postopke dešifriranja podatkov in razvoja naprav, kot je zgoraj omenjeni »Navy bomber«.
Danes, ko se nahajamo v informacijski dobi in informacije igrajo ključno vlogo v svetu je želja po pridobivanju informacij močno v porastu. Vzporedno s tem smo lahko priča pojavu, kjer se velik del življenja in delovanja posameznika seli na splet, tako da so se tudi metode za dešifriranje temu prilagodile. V nadaljevanju bo tako opisanih nekaj najbolj znanih metod, s katerimi poskušajo napadalci bodisi pridobiti (naše) podatke bodisi nam jih uničiti.

3.1 Osnovne metode za pridobivanje zasebnih podatkov

3.1.2 Računalniški virus

Računalniški virus je zlonamerni program namenjen kontaminaciji informacijskih sistemov in računalniške opreme brez neke tendence avtorja, da bi od tega imel korist (Kovačič 2003, 57). Njegov cilj je okužiti računalnik in s tem povzročiti škodo, največkrat v smislu izgube podatkov in sistemskih napak (Tulloch 2003, 358).
Za svoje razmnoževanje potrebuje drug program oziroma izvršitveno datoteko na katero se namesti. Tako se skupaj s tem programom oziroma datoteko požene tudi virus, ki nato okuži druge programe oziroma datoteka (ti v nadaljevanju služijo kot nadaljnji okuževalci). Virusi so nevarni ravno zaradi dejstva, da lahko hitro pripeljejo do popolne okužitve celotnega sistema, saj njihovo razmnoževanje poteka eksponentno (Brain 2009).
V grobem lahko računalniške viruse ločimo na pet delov in sicer; Boot sector virusi, Datotečni virusi, Makro virusi, Večstranski virusi in Polimorfični virusi.
Boot sector virusi se namestijo na glavni pomnilnik trdega diska in se naložijo v pomnilnik sistema ob vsakem zagonu računalnika. Datotečni virusi se prilepijo na program ali izvršno datoteko. V pomnilnik sistema se naložijo vsakokrat, ko poženemo okužen program oziroma datoteko. Makro virusi so napisani v makro

programskih jezikih in za delovanje potrebujejo programsko opremo, ki uporablja ta jezik. Zaradi tega dejstva je njihova posebnost, da niso omejeni z informacijskim sistemom, saj je na vseh informacijskih sistemih moč najti programe, ki uporabljajo ta jezik. Makro virusi se zaradi svoje narave velikokrat prenašajo preko spletne pošte, saj jih je možno vstaviti v razne predstavitve, dokumente s tekstom, razpredelnice in ostalo. Večstranski virusi so kombinacija boot sector virusov in datotečnih virusov. Polimorfični virusi lahko pridejo v obliki kateregakoli zgoraj naštetega virusa, njihova posebnost je, da imajo zmožnost transformacije in spremembe svoje izvorne kode, tako da jih antivirusni programi težje zaslediji (Tulloch 2003, 358).

3.1.3 Računalniški črv

Računalniški črv je zlonamerna programska koda, ki se razmnožuje preko omrežja. Od računalniškega virusa se razlikuje po tem, da za svojo delovanje ne potrebuje gostitelja (program, izvršna datoteka), saj se lahko izvaja sam (Tech Faq 2009).
Računalniški črv je napisan tako, da izkorišča varnostne ranljivosti tako v operacijskih sistemih kot tudi različnih programih, ki se povezujejo na splet. Te varnostne ranljivosti nato izkoristi, se skozi njih prenaša na druge sistem in razmnožuje (Brain 2009). Računalniški črvi se uporabljajo predvsem za ustvarjanje omrežij bot-ov (»botnet«), s pomočjo katerih se nato izvajajo različne nelegalne operacije, kot so pošiljanje nezaželjene pošte, razpošiljanje virusov, motenje delovanja spletnih strani (»dDoS napad«) ipd.

3.1.4 Trojanski konj

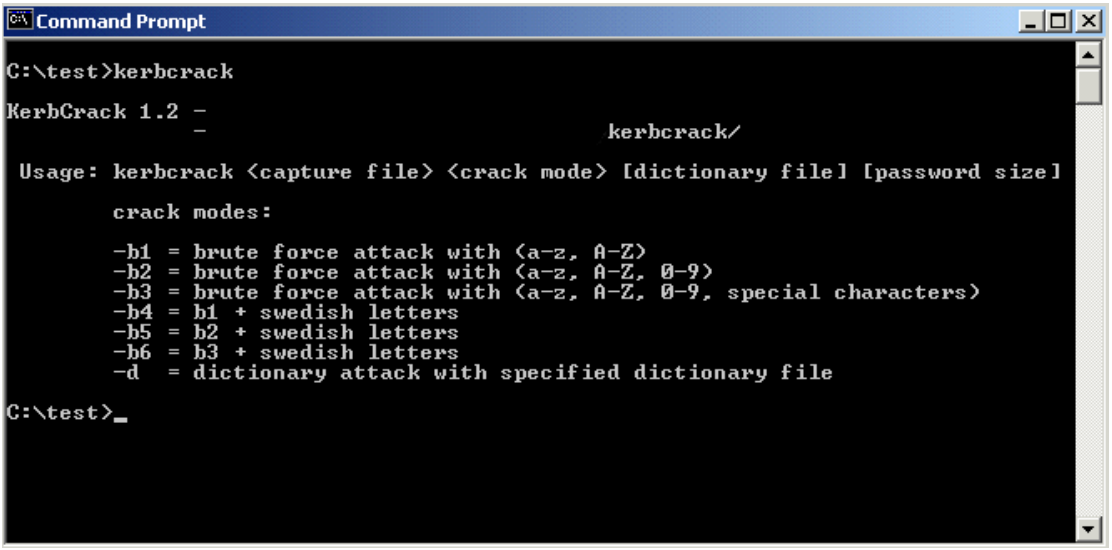
Trojanski konj je zlonamerni program, ki se od računalniških virusov in črvov razlikuje po dejstvu, da se ne more razmnoževati sam, brez posega uporabnika. Največkrat pride v obliki programa za katerega uporabnik ne ve, da ni to, kar predstavlja, tako da ga uporabnik sam zažene (Kovačič 2003, 56).
Splošno lahko po namembnosti ločimo štiri vrste trojanskih konjev. Prvi so namenjeni kraji gesel. Prihajajo lahko v dveh različicah; splošni in ciljni. Splošni se namestijo v operacijski sistem in zbirajo vsa gesla, ki jih vpiše uporabnik. Na drugi strani pa bolj ciljani delujejo na način, da ponaredijo vpisna mesta programov za katere napadalec

želi gesla (Tulloch 2003, 347-348). Prednost slednjih je, da napadalec dobi že prečiščene podatke, ki jih lahko takoj uporabi.

3.1.5 Napad z grobo silo

Napad z grobo silo je eden izmed najenostavnejših načinov dostopa do šifriranih podatkov oziroma vstopnih gesel. Napadalec napad izvede tako, da poskuša s programom karseda hitreje preizkusiti vse možne kombinacije in tako priti do gesla (glej Sliko 3.1). Realno gledano je ta napad mogoče izpeljati povsod in je vedno uspešen vendar je potrebno upoštevati tudi časovno komponento. Ob primerni dolžini gesla in uporabi različnih znakov, ki vključujejo tako števila, male in velike črke ter druge simbole (pika, podpičje, klicaj itd.) se čas za razbijanje takega gesla toliko poveča, da lahko govorimo o varnem geslu. Postopek razbijanja gesla z grobo silo s pomočjo preverjanja vseh možnih kombinacij namreč bi pri dolgem in kompleksnem geslu trajal tako dolgo, da šifrirane informacije ne bi več imele pomena.

Slika 3.1: Prikaz uporabe programa za napad z grobo silo.



vir: McAfee (2009).

3.2 Napredne metode za pridobivanje zasebnih podatkov

3.2.1 Socialni inženiring

Socialni inženiring je oblika napada, ki za razliko od drugih metod ne uporablja tehnologije ampak se naslanja na človeško naivnost oziroma nevednost. V tej obliki napada poskuša napadalec žrtev prepričati, da mu zaupa neke informacije s katerimi si lahko pridobi dostop do informacijskega sistema oziroma kakorkoli zaobide varnostne mehanizme (Kovačič 2003, 41-42).

Znani so primeri, ko so se napadalci na primer predstavljali kot delavci v podporni službi in so vskočili »na pomoč« frustriranim delavcem podjetja, ki so imeli težave s svojimi delovnimi postajami. Ali primer, ko so se napadalci pretvarjali, da so vzdrževalni delavci in so tako prepričali varnostnike ter si tako pridobili prost dostop do poslovnih prostorov.

Ena izmed komponent socialnega inženiringa je tudi opazovanje in preučevanje navad žrtev. Napadalec tako preži na napako žrtve, ko recimo ta zapusti delovno mizo brez da bi zaklenila svojo delovno postajo (Tulloch 2003, 321-322).

Kot smo iz tega lahko razbrali, človeški faktor igra zelo pomembno vlogo pri informacijski varnosti in varovanju podatkov, tako da je na takšne prevare potrebno biti še posebej pozoren.

3.2.2 Spletno ribarjenje

Spletno ribarjenje je eden izmed načinov pridobivanja osebnih podatkov s pomočjo ponarejanja obstoječih strani. Napadalec tako sname izvorno kodo obstoječe strani in jo namesti na svoj strežnik. Da prevara zgleda čim bolj resnično tudi URL naslov lažne strani navadno zamaskira, da je le-ta podoben originalnemu. Bratuša o tem piše tudi: »Z uvedbo mednarodnih domen (IDN - International Domain Names) se je situacija za uporabnike še dodatno poslabšala. Napadalec lahko namreč registrira domeno, ki bo imela v imenu http://mojabanka.com namesto običajnega znaka »a« podoben znak iz cirilice, ki je videti identičen. Ime domene se tako ujemajo s pričakovanji žrtve, čeprav bo šlo za popolnoma drugo domeno« (Bratuša 2006, 132).

Naslednji korak je pošiljanje spletne pošte žrtvi v kateri se napadalec pretvarja, da prihaja iz uradne strani, v njej pa prosi za obisk povezave (ki kaže na lažno stran) in vpiše določene osebne podatke, zamenja geslo ali celo napiše številko svoje kreditne kartice. Ko žrtev to stori, ga lažna stran preusmeri na originalno stran, tako da velika večina prevare sploh ne ugotovi.

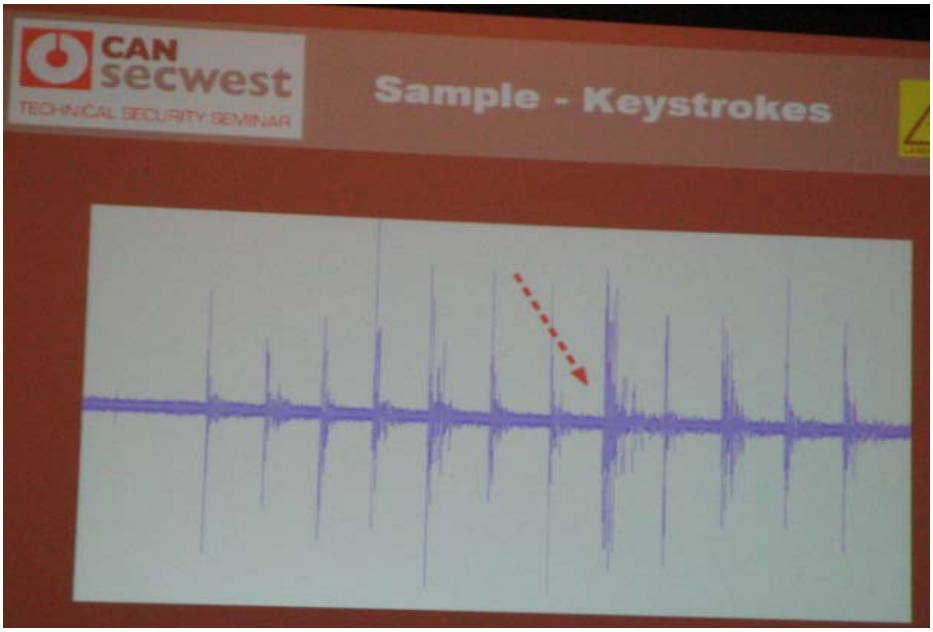
3.2.3 Tempest napad

Tempest napad pomeni prisluškovanje elektronskim signalom. Tako kot vsaka elektronska naprava, tudi računalniška oprema oddaja elektromagnetne signale, ki se jih da prestrezati. Prestrezanje poteka s pomočjo anten in širokopasovnih sprejemnikov. Najbolj ranljivi so katodni monitorji in televizije iz katerih se da z relativno zelo poceni opremo zajemati informacije (Kuhn 2004). Novejši LCD monitorji sicer naj ne bi bili tako ranljivi, vendar se je izkazalo, da je prestrezanje podatkov prav tako mogoče (Backes in drugi 2008).

Pri temu ni izjema niti druga računalniška oprema, kot je na primer tipkovnica. Raziskovalcem je namreč z opremo vredno manj kot 60 evrov uspelo izdelati napravo, ki prestreza elektromagnetne signale računalniške tipkovnice (glej Slika 3.2). Naprava deluje s pomočjo laserja, ki ga je potrebno usmeriti v tipkovnico ali prenosni računalnik in deluje tudi skozi steklo (okno) na razdalji med enim in tremi metri (Mills 2009).

Največja nevarnost tempest napada je, da se da podatke prestrezati na razdalji od nekaj metrov, z modernejšo opremo pa tudi do kilometra daleč, kljub temu da so vmes prepreke kot omare, zidovi in drevesa. Ta tehnika je relativno neznana, saj se o njej ni veliko pisalo, čeprav je prvi poskus bil predstavljen že leta 1985 (Kuhn 2004), NSA pa se te tehnike že dolgo poslužuje (Singel 2008).

Slika 3.2: Prikaz izpisa tempest napada na računalniško tipkovnico.



Vir: Mills (2009).

3.2.4 Cold boot napad

V javnosti velja splošno prepričanje, da se v delovnem pomnilniku računalnika podatki brišejo v trenutku, ko niso več v uporabi. V nasprotju s tem prepričanjem dokazi kažejo, da podatki v delovnem pomnilniku ostajajo od nekaj sekund pa tudi do nekaj minut po tem ko se računalnik izključi oziroma tudi takrat, ko se delovni pomnilnik odstrani iz matične plošče. S hlajenjem pa se lahko podatki v delovnem pomnilniku vzdržujejo tudi veliko dlje.

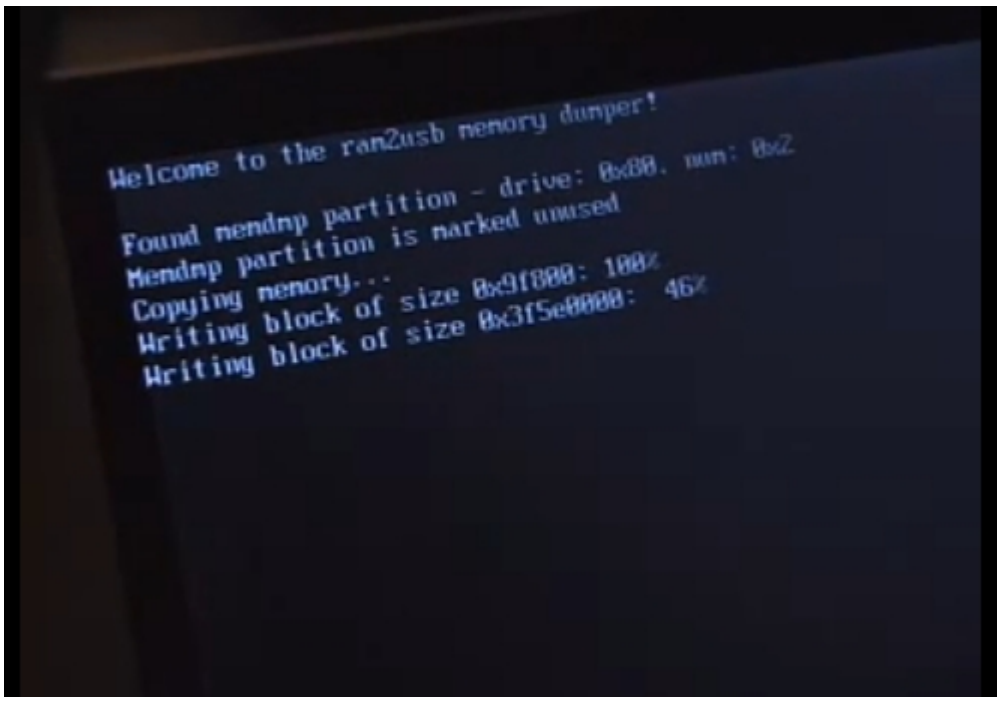
Za izvršitev cold boot napada mora napadalec imeti fizičen dostop do računalnika, ta pa mora biti prižgan. Napadalec nato računalnik (fizično) izklopi iz elektrike in ga nato hitro ponovno prižge. Iz USB ključka zažene prirejen operacijski sistem, s pomočjo katerega zajame podatke, ki so se nahajali v delovnem pomnilniku pred zagonom. Napad je mogoče izvesti tudi tako, da se iz računalnika fizično odstrani

delovni pomnilnik, ki ga napadalec vstavi v svoj računalnik z prednaloženim (prirejenim) operacijskim sistemom.

S to metodo se da pridobiti gesla praktično vseh šifrirnih programov vgrajenih v operacijskih sistemih kot tudi drugih programov namenjenih šifriranju (Halderman in drugi 2008).

Edina možna zaščita pred cold boot napadom je, da se računalnik vsakič, ko ga izpustimo iz vidnega polja in bi lahko nekdo nepooblaščeno dostopal do njega, izklopimo ter počakamo nekaj minut, saj se v tem času delovni pomnilnik izbriše. Razne metode zaklepanja računalnika oziroma hibernacija pri tem ni uspešna, saj se v računalniku kljub temu vzdržuje določen količina elektrike, ki zadostuje da se podatki ohranijo. Sicer obstaja še kakšna druga metoda, vendar bi ta potrebovala modifikacijo programske in strojne opreme (Center for information technology policy 2009).

Slika 3.3: Na sliki je prikaz postopka za zajem podatkov iz delovnega pomnilnika.



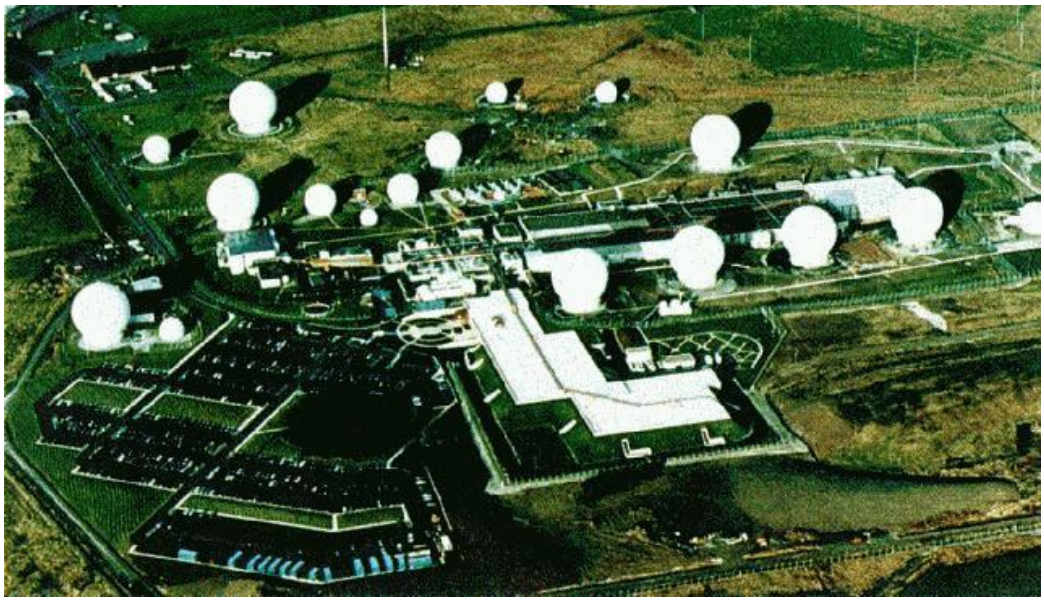
Vir: Center for information technology policy (2009).

3.3 Vladni projekti

3.3.1 Echelon

Echelon je eden izmed najbolj razvpitih in infrastrukturno najbolj zahtevnih vladnih projektov za globalno prestrezanje podatkov (glej Slika 3.4). Sistem je bil postavljen za realno-časovni zajem podatkov vseh telekomunikacijskih kanalov z namenom boja proti organiziranemu kriminalu. Zgrajen je bil pod vodstvom Ameriške nacionalne varnostne organizacije (NSA) s sodelovanjem z obveščevalno varnostnimi agencijami, Velike Britanije, Kanade, Avstralije in Nove Zelandije (Schneier 1999). Echelon je po nekaterih ocenah zmožen zajeti 3 milijarde komunikacij dnevno, ki jih s pomočjo podatkovnega rudarjenja prečisti ter jih tako naredi uporabne (Schneier 2005).

Slika 3.4: Prikaz domnevne infrastrukture projekta Echelon.



Vir: Dmitri (2007).

3.3.2 Crypto AG

Crypto AG je podjetje z dolgoletno tradicijo in izkušnjami na področju informacijske varnosti s sedežem v Švici. Začetki razvoja segajo v leto 1952, ko je podjetje ustanovil znan švedski kriptolog Boris Hagelin. Podjetje je postalo znano predvsem v času Druge svetovne vojne, saj so razvili svojo šifrirno napravo konkurenčno Enigmi. Podjetje je tako v času svojega delovanja razvila kar precejšni krog strank iz celega sveta.

Škandal okoli podjetja in njihovih šifrirnih strojev se je začel, ko so na dan prišle informacije, delno podprte tudi z dokumenti, da je podjetje sodelovalo tako z Nemško (BND) ko tudi Ameriško (NSA) obveščevalno agencijo. Podjetje bi naj tema dvema obveščevalnima agencijama posredovala šifrirne ključe in načrte šifrirnih naprav, tako da so brez težav prisluškovali komunikacijam njihovih strank. Crypto AG je vse te očitke odločno zavrnil, čeprav glede tega še danes ostaja veliko odprtih vprašanj (Spiegel 1996, 206).

3.3.3 Bundestrojaner

Bundestrojaner je projek, ki sta ga skupaj razvila nemška Državna obveščevalna služba (BND - »Bundesnachrichtendienst«) in Državni kriminalistični zavod (BKA - »Bundeskriminalamt«). Pri tem gre za trojanskega konja s pomočjo katerega lahko na računalnike s pomočjo oddaljenega dostopa namestijo drugo opremo za nadzor in opazovanje sistema in komunikacijskih kanalov ter s pomočjo »keyloggerjev« pridobijo potrebna gesla za dešifriranje dokumentacije potrebne za dokazovanje krivde. Sprva BKA razvoja Bundestrojaner-ja ni priznal, kasneje pa je pod pritiskom javnosti to le moral. To je dvignilo veliko polemik v nemški javnosti glede kršitev varovanja osebnih podatkov ter vdora v zasebnost. Kasneje so v parlamentu sprejeli zakon, da se sme to orodje uporabljati le z nalogom sodišča, tako kot tudi vsa druga preiskovalna sredstva, ki omogočajo poseg v zasebost (npr.: hišna preiskava) (Spiegel online 2008).

3.3.4 Carnivore

Projekt Carnivore oziroma DSC-1000 je program za nadzor nad spletno komunikacijo, ki ga je razvil Ameriški Zvezdni preiskovalni urad (FBI). Program se uporablja za prisluškovanje kakršnegakoli spletnega prometa, pri čemer ga je potrebno predhodno namestiti na uporabnikov računalnik. Pri tem projektu gre tako za ciljan in ne masovni nadzor, tarča pa naj bi bile skupine ljudi osumljene terorizma, otroške pornografije, špijonaže in informacijskih zločinov (Ventura in drugi 2005).

3.3.5 Magic Lantern

Magic Lantern je še eden izmed projektov FBI. Gre za tako imenovan »keylogger«, program, ki beleži vse vnose uporabnika (Mills Abreu 2001). Program se namešča s pomočjo trojanskega konja, tako da bi ga antivirusni programi morali zaznati, vendar je FBI glede tega sklenil dogovor z največjimi proizvajalci antiviusnih programov(Sposato 2001).

3.4 Nevarnosti spletnih socialnih omrežij

Zraven vseh zgoraj naštetih nevarnosti, ki prežijo na sodobne uporabnike spleta, je potrebno omeniti še trenutni fenomen, tako imenovan »social network site«-i oziroma spletne skupnosti. Ti že sami po sebi zaradi svojih značilnosti predstavljajo precejšnjo grožnjo za uporabnika, še posebej pa so nevarni saj posamezniki s tem dejstvom niso seznanjeni oziroma se tega ne zavedajo.

3.4.1 Primer Facebook-a

Facebook je trenutno najbolj priljubljen in posledično največji »social network site«, ki združuje kar 250 milijonov aktivnih uporabnikov iz vsega sveta (Facebook 2009). Zaradi svoje velikosti in ogromnega števila uporabnikov je priljubljena tarča tistih, ki želijo zbirati podatke o posameznikih. To se dogaja, saj Facebook ponuja mnogo osebnih informacij, česar se veliko uporabnikov tega spletnega servisa sploh ne

zaveda. Tako Facebook že sam po sebi predstavlja veliko grožnjo posameznikove zasebnosti, kar lahko pripelje k kršenju temeljnih človekovih pravic, ki so določene z Deklaracijo o človekovih pravicah.

Facebook je po mnenju avtorjev raziskave (Soltern in Jones 2005) glede zasebnosti, determiniran s tremi dejavniki. Prvi dejavnik, ki ga navajata raziskovalca je, da Facebook kot ponudnik storitve ne zagotavlja zadostnih ukrepov za varovanje zasebnosti in varstva osebnih podatkov uporabnikov. Drugi dejavnik je nepremišljenost uporabnikov, ki razkrivajo preveč osebnih informacij, čeprav se tega po navadi sploh ne zavedajo ter tako sami skrbijo za to, da so tudi informacije intimnega tipa na voljo tako rekoč vsakomur. Tretji dejavnik je ta, da je Facebook zaradi velikega števila aktivnih uporabnikov zelo priljubljeno orodje raznih podjetji in posameznikov, ki iščejo informacije o uporabnikih, saj jih lahko uporabijo v svoje namene (Soltern in Jones 2005, 1). Tukaj je potrebno omeniti, da lahko gre na eni strani tako za marketinška podjetja, ki zbirajo podatke za ciljno oglaševanje, kot na drugi strani tudi za posameznike, ki poskušajo izkoristiti varnostne ranljivosti sistema za pridobitev podatkov, ki jih potrebujejo v nelegalne namene (na primer: kraja identitete).

Pri vsem tem je potrebno upoštevati razlike v zakonu glede na različne države. V Sloveniji je potrebno kakršnokoli zbiranje podatkov predhodno prijaviti pri Informacijskem pooblaščencu, ki mora tako zbiranje podatkov potrditi. Da se zahtevek potrdi, mora biti namen zbiranja podatkov jasno določen in definiran (Informacijski pooblaščenec 2009). Nadaljnja uporaba pridobljenih podatkov v drug namen, kot je bil definiran ob prijavi je izrecno prepovedana. V nasprotju z našo zakonodajo, na primer v Združenih državah Amerike obstajajo celo podjetja, ki se čisto legalno ukvarjajo izključno samo s tem, da pridobivajo podatke, ki jih nato prodajajo marketinškim in drugim podjetjem.

V nadaljevanju bomo predstavili nekaj primerov, ki kažejo na kak način je lahko na »social network site-u« ogrožena naša zasebnost in naši osebni podatki.

3.4.2 Varnostne ranljivosti sistema

Varnostne ranljivosti v informacijskih sistemih predstavljajo veliko nevarnost in Facebook pri tem ni izjema. Varnostne ranljivosti, ki nastanejo pri programiranju in

jih namesto samih programerjev odkrijejo drugi posamezniki, predstavljajo velik problem, saj se lahko s pomočjo njih pride do nepooblaščenega vstopa v podatkovno zbirko. Facebook s svojim razvojem in širjenjem postaja vse večji in kompleksnejši ter tako težji za vzdrževanje. Premosorazmerno z rastjo je na eni strani tak sistem vedno težje vzdrževati in zagotavljati popolno varnost, po drugi strani pa raste tudi zanimanje hekerjev za vdor v njihove podatkovne zbirke (Soltern in Jones 2005, 25).
V zadnjem času predstavljajo vedno večji problem tudi »third party« vtičniki, ki jih uporabniki množično uporabljajo, za katere pa inženirji ne morejo zelo učinkovito jamčiti da so varni. V takem primeru vedno obstaja možnost, da je programer vgradil tudi stranska vrata. S pomočjo teh stranskih vrat si programer nato lahko omogoči neomejen dostop do podatkovnih zbirk.
Za enkrat poročil o odkritju večjih varnostnih lukenj na Facebooku še ni bilo, kar pa seveda ne pomeni, da le-te ne obstajajo. Prvi varnostni incident je bil zabeležen v začetku leta 2008, kjer je bil opažen prvi računalniški črv, ki bi se naj širil med uporabniki (The Facebook advice 2008) in ki je poskušal zbirati podatke bančnih kartic žrtev. Drug tak incident je bil opažen avgusta 2008 (Tech Crunch 2008). Kakorkoli pa glede na način širjenje in okužbe uporabnikov ne moremo trditi, da je šlo za varnostno luknjo v sistemu Facebooka, saj sta se oba črva širila s pomočjo uporabnika, ki je iz spleta prenesel bodisi okuženo aplikacijo v prvem primeru, bodisi okuženo domnevno posodobitev Flash player-ja v drugem primeru.

3.4.3 Podatkovno rudarjenje v komercialne namene

Kot sem že omenil prej v Združenih državah Amerike, kjer je to z zakonom dovoljeno, obstajajo podjetja, ki se ukvarjajo izključno s profiliranjem ter zbiranjem podatkov o posameznikih. Svoje podatkovne zbirke nato prodajajo drugim podjetjem, te pa jih uporabljajo za ciljno oglaševanje. Facebook in ostali »social network site-i«, so za taka podjetja zelo privlačni, saj so zaradi visoke stopnje aktivnih uporabnikov, podatki v večini primerov stoodstotno pravilni in tako uporabni. V primerjavi z drugimi viri za pridobivanje podatkov namreč aktivni uporabniki na »social network site-ih«, svoje profile vzdržujejo in jih redno osvežujejo(Soltern in Jones 2005 : 26).
Test, ki so ga izvedli v sklopu raziskave (Soltern in Jones 2005) je pokazal, kako je možno na lahek način v zelo kratkem času pridobiti veliko število podatkov. Test so

izvedli s pomočjo pripetega »crawlerja« oziroma pajka (tehnologija, ki jo uporabljajo spletni brskljalniki za indeksiranje spletnih strani). Ta je z malo vloženega časa v roku enega tedna nabral takšno veliko količino »uporabnih« podatkov, kot je avtorja sploh nista pričakovala. S tem sta dokazala, da je Facebook ne le (potencialna) tarča komercialnega podatkovnega rudarjenja, temveč tudi to, kako enostavno in hitro je moč na tak način zbirati podatke (Soltern in Jones 2005, 26).

3.4.4 Povratni inženiring podatkovnih baz

Facebook omogoča včlanitev v različne interesne skupine, znotraj katerih si lahko posamezniki ogledujejo profile drugih članov, ne glede na to ali jih imajo slednji dodane kot prijatelje ali ne. To funkcijo se sicer lahko onemogoči v nastavitvah, vendar se do določenih podatkov v profilu vseeno da dostopati s pomočjo funkcije naprednega iskanja, ki jo ponuja Facebook. Tako je uporabnikom nudena le navidezna zasebnost, saj vnosov v profil ni moč skriti. Kot primer je navedeno iskanje znotraj skupine neke fakultete, kjer je iskalni niz številke sob v kampusu v katerem prebivajo študenti te fakultete, pokazal na pravega uporabnika. To se je zgodilo zaradi tega, saj so se uporabniki preko storitve »write on my wall« pogovarjali o tem, v katerih sobah v kampusu stanujejo(Soltern in Jones 2005 : 27-28).

3.4.5 Pomanjkanje nadzora uporabnikov nad lastnimi informacijami

Facebook ponuja zanimivo storitev, na naloženih fotografijah označiš, kdo se vse na njih nahaja. Ta storitev je z vidika varovanja zasebnosti zelo sporna, saj lahko nekdo naloži fotografijo, na katerem označi drugega uporabnika kljub njegovi (ne)vednosti. To lahko pripelje do različnih posledic, saj te fotografije s povezavami, ki kažejo na uporabnika lahko vidijo vsi prijatelji, tako uporanika, ki je sliko naložil, kot tudi prijatelji tistega, ki je na fotografiji označen (Soltern in Jones 2005, 28-33).
Primer zgoraj opisanega problema je študentka, ki je bila degradirana s svoje funkcije v svetu fakultete, saj je nekdo naložil in označil sporne fotografije iz zabave, ki so jih nato videli tudi njeni nadrejeni. Tako je bila zaradi tega ne samo ob funkcijo ampak je doživela tudi javno razžalitev, čeprav uporabnik, ki je slike naložil na to sploh ni pomislil (Soltern in Jones 2005, 28-33).

3.4.6 Previdno pri izdajanju osebnih podatkov

Kot lahko vidimo iz vsega kar je napisano, lahko Facebook in tudi ostali »social network site-i« potencialno predstavljajo veliko grožnjo za uporabnikovo zasebnost. Zato velja, da je potrebno dobro razmisliti in paziti na to, katere osebne podatke smo pripravljeni razkriti. Vedno je tako potrebno v obzir vzeti dejstvo, da so ti podatki dostopni praktično vsakemu ter sprejeti riziko, da lahko močno vplivajo na naše življenje, čeprav smo se na Facebook prijavili zgolj iz radovednosti oziroma dolgega časa.

4 Sklepi raziskovanja

Skozi analizo predelanih tekstov smo tekom naloge v drugem poglavju (poglavje 2.1 do 2.4) odgovorili na raziskovalno vprašanje, kako je potekal razvoj kriptografije. Kot smo lahko ugotovili, se je razvoj varovanja podatkov razvil že davno v preteklosti s postopkom imenovanim steganografija oziroma uporabo metod, ki so zakrile obstoj samega sporočila (opisano v poglavju 2.1). Ko prikrivanje obstoja sporočila več ni bilo dovolj, so ljudje odkrili metode, kako informacije še dodatno zavarovati s pomočjo šifriranja. Začetki šifriranja segajo v dobo Egipčanov v leto 1900 pred našim štetjem, ki so pri inskripciji uporabljali ne-regularne hieroglife (opisano v poglavju 2.2). To so v letu 1500 pred našim štetjem nadaljevali Mezopotamci in leta 600 pred našim štetjem tudi Hebrejci (opisano v poglavju 2.2). Prva mehanska šifrirna naprava za katero so zaslužni Grki se imenuje skital in sega v leto 478 pred našim štetjem (opisano v poglavju 2.2). Razvoj šifriranja je nato potekal preko izuma šifrirnega valja (opisano v poglavju 2.3.1) leta 1467 do šifrirnega koleščka v 18 stoletju (opisano v poglavju 2.3.2). Vse to je botrovalo k razvoju šifrirne naprave Enigma leta 1919, ki je v drugi svetovni vojni odigrala zelo pomembno vlogo (opisano v poglavju 2.3.3).

Naslednje področje raziskave, ki smo jo analizirali, je katere kriptografske metode so danes relevantne in v uporabi (poglavje 2.5 do 3). Kot smo ugotovili se kriptografija danes razvija predvsem v smeri razvoja programske opreme in protokolov za zaščito in varovanja zasebnosti na spletu. Prvi velik korak na tem področju je predstavljal izum šifrirnega algoritma RSA (opisano v poglavju 2.4.1). Ta je botroval k razvoju PGP-ja Phil Zimmermann-a (opisano v poglavju 2.4.2), ki je s tem projektom želel šifriranje narediti dostopno vsakemu uporabniku spleta. S pomočjo delovanja algoritma RSA, vendar v obratni smeri, so uspeli rešiti tudi problem avtorstva digitalnih dokumentov, z uvedbo digitalnega podpisa (opisano v poglavju 2.4.3). Ker s(m)o ljudje vedno večji uporabniki brezžičnega omrežja so za varovanje tega protokola bili uvedeni standardi WEP oziroma Wired Equivalent Privacy (opisano v poglavju 2.4.4), ki ga je zaradi svojih pomanjkljivosti nasledil WPA oziroma Wi-Fi Protected Access (opisano v poglavju 2.4.5) in kasneje nadgrajena različica WPA2 (opisano v poglavju 2.4.6). Uporaba šifriranja v širši javnosti je sprožila veliko dilem, zato smo pogledali tudi argumenti za (opisano v poglavju 2.5.2) in proti (opisano v

poglavju 2.5.1) njeni prosti dostopnosti ter nekaj možnih kompromisov (opisano v poglavju 2.5.3).

Do sedaj smo tekom diplomske naloge razjasnili metode in postopke šifriranja podatkov, zato smo nadaljevali z raziskovanjem tehnik pridobivanja šifriranih podatkov (poglavje 4). Tehnike pridobivanja šifriranih podatkov se osredotočajo na različna področja pomanjkljivosti šifrirnih metod. Tako lahko ločimo napade na slabosti v algoritmu oziroma v njihovi implementaciji, kot so varnostne pomanjkljivosti standardov WEP in WPA (opisano v poglavju 2.4.4 in 2.4.5). Naslednja oblika pridobivanja šifrirnih podatkov so tako imenovani napadi na šifrirne ključe, kot je napad z grobo silo (opisano v poglavju 3.1.5). Najbolj smo se posvetili raziskovanju tretjega načina pridobivanja šifriranja podatkov, tako imenovanim »channel side« napadom, kjer se informacije pridobiva s fizičnim posegom v šifrirni sistem. Tukaj smo pod osnovnimi tehnikami opisali pojme računalniški virus (opisano v poglavju 3.1.2), računalniški črv (opisano v poglavju 3.1.3) in trojanski konj (opisano v poglavju 3.1.4). Napredne tehnike »channel side« napadov, ki smo jih raziskali so socialni inženiring (opisano v poglavju 3.2.1), spletno ribarjenje (opisano v poglavju 3.2.2), tempest napad (opisano v poglavju 3.2.3) in cold boot napad (opisano v poglavju 3.2.4). Z razvojem spleta se je pojavil tudi tako imenovan kiberkriminal. Na to so se države odzvale s svojimi projekti masovnega nadzora kot je Echelon (opisano v poglavju 3.3.1), kot tudi razvojem orodij za pridobivanje podatkov iz osumljenčevih računalnikov kot so; Bundestrojaner (opisano v poglavju 3.3.3), Carnivore (opisano v poglavju 3.3.4) in Magic Lantern (opisano v poglavju 3.3.5). Znane so tudi zgodbe o sumu povezav med obveščevalno varnostnimi agencijami in proizvajalci šifrirnih naprav, kot je bilo to v primeru Crypto AG (opisano v poglavju 3.3.2). Ker je za kršenje zasebnosti velikokrat kriv kar uporabnik sam, smo si na primeru Facebooka gledali tudi nevarnosti, ki pretijo na uporabnike trenutno zelo popularnih spletnih socialnih omrežij (opisano v poglavju 3.4.1).

5 Zaključek

Zgodovinski pregled razvoja kriptografije je sam po sebi zanimiv, saj nam razkrije, da skrb za varovanje informacij in zasebnosti ni le stvar sedanjosti, saj je prisotna že skoraj 4000 let. Pogled skozi različna zgodovinska obdobja nam tudi pokaže, kako so se tehnike šifriranja skozi različna časovna obdobja morala vedno bolj prilagajati razvoju tehnologije, če so hotela zagotavljati varnost.

Konvergenca oziroma zlitje obstoječih informacijsko komunikacijskih tehnologij, je s seboj prinesla centralizacijo, ki omogoča lažji nadzor tako nad posamezniki, določenimi skupinami kot tudi nad državami. V informacijski družbi katere del smo, informacije igrajo ključno vlogo in predstavljajo najvišjo dobrino, tako da ne poznajo cenovnih omejitev, saj prinašajo največ dobička.

Posameznik je danes zaradi tega dejstva tarča posegov v svojo zasebnost prav na vsakem koraku, pa naj gre za komercialni ali državni nadzor. Na ravni komercialnih ciljev je to lepo razvidno iz raznih spletnih strani, kjer se objavljajo personlizirani oglasi, razne »kvazi« akcijske kartice v trgovinah, monitoring obiskanosti spletnih strani in podobno. Pri tem je potrebno vzeti v obzir še hekerje, ki se poskušajo na različne načine okoristiti, bodisi zgolj s krajo identitete bodisi z dejansko krajo premoženja. Na ravni države je vse to sicer težje opazno in se poskuša delno prikriti, vendar to ne pomeni, da se nadzor ne krepi. Primer takega nadzora je postavitev nadzornih kamer v Londonu, kjer se zaradi njih kriminaliteta dokazano ni zmanjšala (BBC 2009) a jih kljub temu niso umaknili. Znan primer iz zgodovine so težave, na katere je naletel Phil Zimmermann ob splavitvi svojega šifrirnega algoritma PGP, i bi šifriranje približal splošni javnosti. Neposreden dokaz ne nazadnje kažejo tudi razni vladni projekti, kot so Echelon, Magic Lantern in Bundestrojaner, o katerih se bolj malo govori.

Kot lahko vidimo, informacijsko-komunikacijska tehnologija prinaša tako prednosti kot tudi slabosti. Trenutno življenje brez nje ne bi bilo mogoče vendar moramo, da bi jo izkoristili kot nekaj koristnega ter jo uporabili kot priročno orodje v svojem vsakdanu biti vseeno previdni in predvsem preudarni. Sam menim, da ta tehnologija prinese več prednosti kot slabosti, vendar jo je treba uporabljati premišljeno in upoštevati posledice, ki jih lahko pusti za seboj. Zato bi bilo dobro, da se vsak posameznik vpraša, katere osebne oziroma intimne informacije je na spletu

pripravljen razkriti in pazi na to, da je za svojo varnost poskrbel v zadostni meri. Takšna uporaba bo vsakomur v zadovoljstvo brez bojazni, da bo prišlo bodisi do posega v njegovo zasebnost bodisi da bi ostal brez premoženja zaradi ukradene kreditne kartice ali brez službe in/ali dostojanstva zaradi objavljenih fotografij na Facebooku.

6 Literatura

- Backes, Michael, Markus Dürmuth in Dominique Unruh. 2008. *Compromising reflections or how to read LCD monitors around the corner.* Dostopno prek: http://crypto.m2ci.org/unruh/publications/reflections.pdf (1. september 2009).

- BBC. 2009. *1,000 cameras »solve one crime«.* Dostopno prek: http://news. bbc.co.uk/2/hi/uk_news/england/london/8219022.stm (1. september 2009).

- Beck, Martin in Erik Tews. 2008. *Practical attacks against WEP and WPA.* Dostopno prek: http://dl.aircrack-ng.org/breakingwepandwpa.pdf (1. september 2009).

- Beckwith, Anthony. 2008. *Encryption and Cryptography.* Dostopno prek: http://mail.colonial.net/~abeckwith/images/scytale.gif (1. september 2009).

- Brain, Marshall. 2009. *How computer viruses work.* Dostopno prek: http://www. howstuffworks.com/virus.htm (1. september 2009).

- Bratuša, Tomaž. 2006. *Hekerski vdori in zaščita.* Ljubljana: Pasedana.

- Center for information technology policy. 2009. *Cold Boot: Frequently Asked Questions*. Dostopno prek: http://citp.princeton.edu/memory/faq (1. september 2009).

- Dupuis, Clement. 1999. *A short history of crypto*. Dostopno prek: http:// jproc.ca/crypto/crypto_hist.html (1. september 2009).

- Facebook. 2009. *About: Statistics*. Dostopno prek: http://www. facebook.com/press/info.php?statistics (1. september 2009).

- Halderman, J. Alex, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum in Edward W. Felten. 2008. *Lest we remember: Cold Boot attacks on encryption keys.* Princeton University: Electronic Frontier Foundation. Dostopno prek: http://citp.princeton.edu/pub/coldboot.pdf (1. september 2009).

- Informacijski pooblaščenec. 2009. *Zakon o varstvu osebnih podatkov: Dolžnosti upravljavcev osebnih podatkov*. Dostopno prek: http://www.ip-rs.si/pogosta-vprasanja/varstvo-osebnih-podatkov/#c293 (1. september 2009).

- Jones, Harvey in Jose H. Soltern. 2005. *Facebook: Threats to Privacy*. Dostopno prek: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf (1. september 2009).

- Janssen, Davy in Raphael Kies. 2004. *Online Forums and Deliberative Democracy: Hypotheses, Variables and Methodologies*. Dostopno prek: http://edc.unige.ch/edcadmin/images/onlineforums.pdf (1. september 2009).

- Kovačič, Matej. 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut. Dostopno prek: http://www2.mirovni-institut.si/slo_html/publikacije/pdf/MI_politike_zasebnost_na_internetu.pdf (1. september 2009).

- --- 2006. *Nadzor in zasebnost v informacijski družbi*. Ljubljana: Znanstvena knjižnica FDV. Dostopno prek: http://dk.fdv.uni-lj.si/eknjige/EK_Kovacic_2006_Nadzor.pdf (1. september 2009).

- Kuhn, Marcus G. 2004. *Electromagnetic eavesdropping risks of flat-panel displays*. Dostopno prek: http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf (1. september 2009).

- Lucas, W. Michael. 2006. *PGP and GPG: E-mail for the practical paranoid.* San Francisco: No starch press.

- McAfee. 2009. *PWCrack KerbCrack*. Dostopno prek: http://vil.nai.com/vil/content/v_100071.htm (1. september 2009).

- McMillan, Robert. 2009. *WPA wireless security cracked in 60 seconds: Users urged to switch to WPA2*. Dostopno prek: http://www.pcadvisor.co.uk/news/index.cfm?RSS&NewsID=3200541 (1. september 2009).

- Mills Abreau, Elinor. 2001. *FBI confirms 'Magic Lantern' project exists.* Dostopno prek: http://www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/ Magic_Lantern.pdf (1. september 2009).

- Mills, Elinor. 2009. *Sniffing keystrokes via laser and keyboard power.* Dostopno prek: http://news.zdnet.com/2100-9595_22-280184.html (1. september 2009).

- National Security Agency. 2009a. *18th Century Cipher Device Exhibit*. Dostopno prek: http://www.nsa.gov/about/cryptologic_heritage/museum/virtual_tour/museum_tour_text.shtml (1. september 2009).

- --- 2009b. *World War 2: 'Big' Machines Exhibit*. Dostopno prek: http://www.nsa.gov/about/cryptologic_heritage/museum/virtual_tour/museum_tour_text.shtml (1. september 2009).

- --- 2009c. *National Cryptologic Museum - Virtual Tour*. Dostopno prek: http://www.nsa.gov/about/cryptologic_heritage/museum/virtual_tour/index.shtml (1. september 2009).

- Ohigashi, Toshihiro in Masakatu Morii. 2009. *A Practical Message Falsication Attackon WPA*. Dostopno prek: http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf (1. september 2009).

- Privacy international. 2003. *Privacy and human rights: France 2003.* Dostopno prek: http://www.privacyinternational.org/survey/phr2003/countries/france.htm (1. september 2009).

- Roblimo. 2007. *Philip Zimmermann and »Guilt« Over PGP*. Dostopno prek: http://slashdot.org/interviews/01/09/24/162236.shtml (1. september 2009).

- Schneier, Bruce. 1999. *ECHELON Technology.* Dostopno prek: http://www.schneier.com/crypto-gram-9912.html (1. september 2009).

- --- 2005. *Uncle Sam is Listening.* Dostopno prek: http://www.schneier.com/essay-100.html (1. september 2009).

- Singel, Ryan. 2008. *Declassified NSA Document Reveals the Secret History of TEMPEST*. Dostopno prek: http://www.wired.com/threatlevel/2008/04/nsa-releases-se (1. september 2009).

- Singh, Simon. 2006. *Knjiga šifer: Umetnost šifriranja od starega Egipta do kvantne kriptografije*. Učila international, Tržič.

- Spiegel. 1996. *Wer ist der befugte Vierte?* Dostopno prek: http://wissen.spiegel.de/wissen/dokument/dokument.html?titel=%22Wer+ist+der+befugte+Vierte%3F%22&id=9088423&top=SPIEGEL&suchbegriff=wer+ist+der+befugte+vierte&quellen=&qcrubrik=natur (1. september 2009).

- Spiegel. 2008. *Bundestag stimmt Online-Durchsuchungen zu.* Dostopno prek: http://www.spiegel.de/politik/deutschland/0,1518,590044,00.html (1. september 2009).

- Sposato, Mike. 2001. *The FBI's Magic Lantern*. Dostopno prek: http://www.wnd.com/news/article.asp?ARTICLE_ID=25471 (1. september 2009).

- Tech Crunch. 2008. *Elaborate facebook worm virus spreading*. Dostopno prek: http://www.techcrunch.com/2008/08/07/elaborate-facebook-worm-virus-spreading/ (1. september 2009).

- Tech Faq. 2009. *What is a computer worm.* Dostopno prek: http://www.tech-faq.com/computer-worm-virus.shtml (1. september 2009).

- The Facebook advice (2008). *Are we seeing the first facebook worm?* Dostopno na: http://facebookadvice.com/2008/03/25/are-we-seeing-the-first-facebook-worm/ (1. september 2009).

- Tulloch, Mitch. 2003. *Microsoft encyclopedia of security*. Redmont: Microsoft Press.

- United Nations General Assembly. 1948. *The universal declaration of human rights*. Dostopno prek: http://www.un.org/Overview/rights.html (1. september 2009).

- Ventura, Holly E., Mitchell Miller in Marthieu Deflem. 2005. *Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power.* Dostopno prek: http://www.cas. sc.edu/socy/faculty/deflem/zgovernterror.pdf (1. september 2009).

- Vitaliev, Dmitri. 2007. *Digital security and privacy for human rights defenders.* Dostopno prek: http://www.frontlinedefenders.org/manual/en/esecman/chapter1_1.html (1. september 2009).