

UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

**OCENJEVANJE PRISTOPOV IN TEHNOLOGIJ ZA
VAROVANJE ZASEBNOSTI NA INTERNETU**

Ljubljana, junij 2007

TOMAŽ BREZNIK

IZJAVA

Študent Tomaž Breznik izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom prof. dr. Borka Jerman Blažič in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih straneh.

V Ljubljani, dne 5. 6. 2007

Podpis: _____

KAZALO

1 UVOD.....	1
1.1 Namen in cilji naloge	2
1.2 Metode dela.....	2
1.3 Struktura naloge	3
2 RAZUMEVANJE ZASEBNOSTI.....	3
2.1 Informacijska zasebnost.....	5
2.2 Zasebnost in uporabniki interneta	7
2.3 Inštrumenti varovanja zasebnosti.....	10
2.4 Zasebnost in varnost.....	12
3 GROŽNJE ZASEBNOSTI V INFORMACIJSKI DRUŽBI	14
3.1 Metode zbiranja podatkov	17
3.1.1 Pasivno zbiranje podatkov	17
3.1.2 Aktivno zbiranje podatkov.....	18
4 PRISTOPI IN TEHNOLOGIJE ZA VAROVANJE ZASEBNOSTI.....	27
4.1 Pristopi za varovanje zasebnosti v okolju oken	27
4.2 Tehnologije za varovanje zasebnosti	35
4.2.1 Razvrstitev	36
4.2.1.1 Tehnologije varovanja na osebni ravni	36
4.2.1.2 Tehnologije varovanja identitete.....	41
4.2.1.3 Tehnologije varovanja s privolitvijo	47
4.2.2 Primerjalna analiza na enotni osnovi	49
4.2.3 Ocena dosedanje uspešnosti.....	52
5 PRIPOROČILA IN USMERITVE ZA PRIHODNOST	56
5.1 Zagotavljanje trga.....	56
5.2 Inovativno snovanje	59
5.3 Izobraževanje javnosti.....	65
5.4 Standardizacija zasebnosti	66
6 RAZISKAVA O ZASEBNOSTI MED UPORABNIKI INTERNETA.....	68
6.1 Namen in cilji raziskave.....	68
6.2 Načrt raziskave.....	68
6.3 Rezultati raziskave in njihova interpretacija	70
6.3.1 Zavedanje uporabnikov o zasebnosti	71
6.3.2 Obnašanje uporabnikov na internetu.....	72
6.3.3 Uporaba pristopov in tehnologij za varovanje zasebnosti	73
6.4 Ugotovitve raziskave.....	74
7 SKLEP.....	75
8 LITERATURA IN VIRI.....	79
8.1 Literatura	79
8.2 Viri	81
PRILOGE	I

KAZALO SLIK

Slika 1: Domene informacijske zasebnosti	5
Slika 2: Cikel zasebnosti informacijskih tehnologij.....	7
Slika 3: Delež spletnih strani, ki zbirajo posamezne osebne informacije	7
Slika 4: Usmeritve uporabnikov interneta glede zasebnosti	8
Slika 5: Delež uporabnikov interneta, ki lagodno posredujejo posamezne osebne informacije	9
Slika 6: Razširjenost zakona o varovanju podatkov po svetu	10
Slika 7: Primerjava elementov informacijske varnosti in zasebnosti.....	13
Slika 8: Vodilne družbe nadzorovanja v EU in po svetu	16
Slika 9: Spletna datoteka dogodkov, zabeležena na strežniku	18
Slika 10: Spletni piškotek v glavi HTTP protokola	19
Slika 11: Komunikacija med odjemalcem in strežnikom pri namestitvi spletnega piškotka... ..	19
Slika 12: Spletni hrošč, odkrit na spletni strani New York Times-a.....	21
Slika 13: Registracijsko okno spletne strani	22
Slika 14: Različice nezaželene e-pošte (SPAM)	24
Slika 15: Nastavitve pomnilnika v spletnem brskalniku.....	30
Slika 16: Nastavitve spletnih piškotkov v spletnem brskalniku.....	30
Slika 17: Nastavitve samovpisovanja v spletnem brskalniku	31
Slika 18: Nastavitve varnosti v spletnem brskalniku	32
Slika 19: Nastavitve blokiranja in filtriranja v poštnem odjemalcu.....	33
Slika 20: Nastavitve varnosti v poštnem odjemalcu	34
Slika 21: Nastavitve varne povezave v poštnem odjemalcu	34
Slika 22: Princip delovanje programa PGP (šifriranje in dešifriranje)	37
Slika 23: Princip delovanja programa Bugnosis	39
Slika 24: Princip delovanja orodja Anonymizer	41
Slika 25: Princip delovanja sistema Onion Routing.....	44
Slika 26: Princip delovanja sistema Crowds	45
Slika 27: Princip delovanja P3P.....	47
Slika 28: Ikona zasebnosti pri IE6.....	48
Slika 29: Ikona zasebnosti pri AT&T Privacy Bird	49
Slika 30: Kategorizacija trenutno dostopnih rešitev zasebnosti.....	61
Slika 31: Proces zasebnosti	61
Slika 32: Izogibanje tveganjem zasebnosti z njeno vgraditvijo v sistem.....	65
Slika 33: Prepričanja uporabnikov interneta glede zasebnosti.....	71
Slika 34: Prepričanja uporabnikov interneta glede pridobivanja informacij.....	71
Slika 35: Upoštevanje dobrih praks med uporabniki interneta pri navigiranju.....	72
Slika 37: Uporaba pristopov v okolju oken pri uporabnikih interneta	73
Slika 38: Uporaba klasičnih PET programov pri uporabnikih interneta	73
Slika 39: Uporaba naprednih PET sistemov in programov pri uporabnikih interneta	74

KAZALO TABEL

Tabela 1: Značilnosti, povezane z zasebnostjo v različnih tehnoloških obdobjih	6
Tabela 2: Vrstni red faktorjev, ki vplivajo na zaupanje do praks zasebnosti spletnih strani ...	10
Tabela 3: Besedni zaklad spletnih piškotkov	20
Tabela 4: Primerjalna analiza mehanizmov zasebnosti in varnosti, orodij, protokolov in storitev	51
Tabela 5: Model zasebnosti.....	60
Tabela 6: Demografske značilnosti uporabnikov in neuporabnikov interneta v Sloveniji	70

1 UVOD

Z globalizacijo ter hitrim razvojem žičnih in brezžičnih omrežij je postala posameznikova zasebnost vse bolj ogrožena. Glavni problem je v tem, da prenos podatkov po globalnih omrežjih običajno prečka številne mednarodne meje, zaradi česar so lahko ti prestreženi ali nadzorovani na različnih koncih sveta. Tako se lahko odkrije, kdo je komuniciral s kom, kje, kdaj in koliko časa (Fischer Hübner, Lindskog, 8. 1. 2007). Grožnjo posameznikovi zasebnosti pa predstavlja tudi zbiranje in shranjevanje osebnih informacij ter vzorca obnašanja med uporabo interneta. Informacije lahko tako postanejo dragoceno blago, ki oskrbujejo poslovne organizacije s sredstvi za učinkovitejše določevanje in segmentiranje njihovega trga (Tuner C., Dasgupta, 2003, str. 8). To jim nenazadnje omogoči možnost povečanja dobička in zagotavljanja konkurenčne prednosti.

Trenutno živimo v družbi, ki ni niti zasebna niti nadzorovana, ampak mešanica obeh. Do zasebnosti imamo zelo velika kolektivna pričakovanja, medtem ko so ta pričakovanja pri posamezniku zelo majhna. To družbo lahko s tega vidika poimenujemo kot »družba hrupa«. Količina hrupa načeloma zagotavlja dobro kolektivno zasebnost, medtem ko je ta na nivoju posameznika skoraj povsem zabrisana (Lundblad, 2004, str. 2).

Sodoben koncept zasebnosti sloni na osnovni razdelitvi med okoljem in posameznikom, kjer na eni strani leži zasebno, na drugi strani javno. Osnovni namen varovanja zasebnosti je v postavitvi meje med zasebnim in javnim ter v dilemi, v kolikšni meri in pod kakšnimi pogoji je dostop do zasebnih podatkov možen. To neposredno pomeni, da je vdor v zasebnost vdor javnega na področje zasebnega brez posameznikove privolitve. Kontrola meje med zasebnim in javnim ter pravica do odločanja, katere informacije je posameznik pripravljen odkriti in pod kakšnimi pogoji, sta osnovna elementa zaščite in varovanja zasebnosti (Jerman Blažič, 2005, str. 123–124).

Desetletja je bil boj za varovanje zasebnosti usmerjen v razvoj ustrezne zakonodaje. V skladu s tem so bila leta 1981 s strani Organizacije za ekonomsko sodelovanje in razvoj (OECD) sprejeta primerna informacijska načela (FIP), ki so bila osnovni temelj za sprejemanje prihodnje zakonodaje v Evropi in Severni Ameriki. Primer sta direktiva Evropske unije o varovanju podatkov (95/46/EC) iz leta 1995 in Kanadska zakonodaja za varovanje zasebnosti (Bill C-6) iz leta 1999. V ZDA je zakonodaja ostala dokaj nespremenjena. Kljub znatnemu napredku na področju zakonodaj se je zbiranje in obdelovanje osebnih informacij nadaljevalo in zasebnost je postala vse bolj ogrožena (Stalder, 2002, str. 2). Med politiki se je kmalu pojavila tudi težnja po harmonizaciji mednarodne zakonodaje na področju varovanja podatkov, vendar je splošno znano, da je to zelo težko doseči predvsem zaradi kulturnih, zgodovinskih in političnih razlik med državami. Nazoren primer tega je lahko kompromisni sporazum »Varni pristan« (*Safe Harbour*) med Evropsko Unijo in ZDA, katerega glavni namen je izboljšati varovanje informacij v ZDA v skladu s strožjo zakonodajo Evropske unije ter tako pospešiti prost pretok informacij (Loring B., 2002, str. 451).

Kot odgovor na pomanjkljivo dodelano zakonodajo in na splošne spremembe v tehnološkem razvoju družbe se je v zadnjih letih pojavila povsem nova smernica za varovanje zasebnosti. Razvile so se tako imenovane tehnologije za varovanje zasebnosti (PET) z namenom, da se posamezniku omogoči nadzor nad količino osebnih informacij, ki jih odkrije v internetnih transakcijah. Cilj je vzpostaviti ponovno ravnotežje med posameznikom, ki želi obdržati svojo zasebnost, in številnimi drugimi igralci na internetu, ki želijo zbirati osebne informacije. Končni namen teh iniciativ pa je narediti informacijsko samoodločanje kot vsakdanjo realnost ter implementirati zakonodajo in samoregulacije, ki imajo za cilj zmanjšanje priložnosti za kršenje zasebnosti z omejevanjem določenih praks (Seničar, Jerman Blažič, Klobučar, 2003, str. 151).

Na drugi strani je zelo zanimiva tudi uporaba pristopov za varovanje zasebnosti, ki jih lahko posameznik nemudoma implementira in so ponavadi dokaj enostavni in razumljivi (Garfinkel, 2002, str. 230). Predvsem s pravilnim nastavljanjem internetnih aplikacij v okolju oken, se lahko bistveno pripomore k večji zasebnosti, vendar pa se ti pristopi po pomenu in učinkovitosti ne morejo primerjati s tehnologijami za varovanje zasebnosti.

1.1 Namen in cilji naloge

Namen magistrskega dela je izdelati študijo o varovanju zasebnosti med uporabo internetnih storitev, kot sta svetovni splet in elektronska pošta ter pripraviti ustrezna priporočila.

Cilji magistrskega dela so: predstaviti pojem zasebnosti v informacijski družbi, izdelati podroben pregled internetnih tehnologij, ki ogrožajo zasebnost, pripraviti podroben pregled in analizo pristopov ter tehnologij za varovanje zasebnosti ter predstaviti priporočila in usmeritve za prihodnost. V zadnjem delu pa prikazati rezultate opravljene empirične študije med uporabniki interneta.

V magistrskem delu želim preveriti naslednji hipotezi:

- *Tehnologije za varovanje zasebnosti na internetu niso popolnoma dodelane in učinkovite.*
- *Uporabniki interneta se zavedajo zasebnosti, vendar so na internetu neprevidni ter se ne poslužujejo pristopov in tehnologij za varovanje zasebnosti.*

1.2 Metode dela

V magistrskem delu bom uporabil znanje, pridobljeno na podiplomskem študiju na Ekonomski fakulteti v Ljubljani. Pri izdelavi bom uporabil deskriptivno metodo ter analizo primarnih in sekundarnih virov. Skliceval se bom predvsem na tujo strokovno literaturo ter na gradiva, ki sem jih našel na internetu, saj je obravnavano področje dokaj novo v znanstvenih

krogih. Kot praktični prispevek k magistrskemu delu bo opravljena empirična raziskava med uporabniki interneta, s katero želim preveriti njihovo zavedanje o zasebnosti, njihovo obnašanje na internetu ter uporabo pristopov in tehnologij za varovanje zasebnosti.

1.3 Struktura naloge

Magistrsko delo sem razdelil v štiri teoretične sklope in en empirični sklop.

V prvem vsebinskem sklopu se bom osredinil na obrazložitev pojma zasebnosti in njegovo sodobno različico, to je informacijska zasebnost v povezavi s tehnologijami. Podrobneje bodo predstavljene tudi usmeritve uporabnikov interneta glede zasebnosti. V nadaljevanju bosta sledila še pregled inštrumentov, ki so na voljo za varovanje zasebnosti, ter koncept povezave med varnostjo in zasebnostjo.

Trenutno najpogosteje uporabljene tehnologije, ki ogrožajo posameznikovo zasebnost na internetu, bom predstavil v drugem vsebinskem sklopu. Pregledane bodo oboje – tiste, ki omogočajo aktivno kot pasivno zbiranje podatkov med uporabo internetnih storitev, kot sta svetovni splet in elektronska pošta.

Glede na predhodni vsebinski sklop bom nato v tretjem sklopu analiziral učinkovitost in pomanjkljivost pristopov za varovanje zasebnosti v okolju oken pri internetnih aplikacijah (spletni brskalnik in poštni odjemalec) ter pri najpogosteje uporabljenih tehnologijah za varovanje zasebnosti (programi in sistemi).

V četrtem vsebinskem sklopu bom predstavil največkrat omenjena priporočila in usmeritve, ki sem jih zasledil v strokovni literaturi in so se nanašala tako na boljše sprejetje kot tudi razvoj bolj dodelanih, učinkovitih in do uporabnikov prijaznejših tehnologij za varovanje zasebnosti.

Empirični sklop bo predstavljala opravljena raziskava o zasebnosti med uporabniki interneta, kjer bom na podlagi analize odgovorov iz vprašalnikov prikazal njihovo trenutno zavedanje o zasebnosti, njihovo obnašanje na internetu, ter katere pristope in tehnologije za varovanje zasebnosti uporabljajo.

2 RAZUMEVANJE ZASEBNOSTI

Zasebnost ima veliko definicij in dimenzij, saj obstajajo različni pogledi nanjo. Nekatere izmed že uveljavljenih definicij so (Ponnurangam, 24. 1. 2006):

... pravica posameznika, skupin ali institucij, da se odločijo, kdaj, kako in do katere mere bodo informacije o njih posredovane drugim ... prostovoljni in začasni umik osebe iz družbe preko fizičnih ali psiholoških načinov ... anonimnost ali zadržanost ...

zasebnost ni nikoli absolutna ... posameznik uravnava željo po zasebnosti z željo po odkrivanju in komuniciranju.

... zasebnost ni absolutna. Je vsebinska in subjektivna ... ocenjevanje bo močno odvisno od tega kdo ga izvaja ... niti vrednost niti stroški zasebnosti niso absolutni.

.... pravica da si sam.

.... želja vsakega od nas po fizičnem prostoru, kjer smo lahko svobodni pred motnjami, vdori, zadregami ali odgovornostjo ter poskusi kontroliranja časa in načinov odkrivanja naših osebnih informacij.

Treba se je zavedati, da se definicija zasebnosti razlikuje od posameznika do posameznika ali od organizacije do organizacije, in da je ta vsebinsko specifična. Zaradi tega ni nujno, da se sprejme samo en univerzalni pogled na zasebnost, ki velja za vse situacije.

Opredelimo lahko naslednje dimenzije zasebnosti (Clark, 1. 4. 2007):

- **Zasebnost osebe.** Obravnava celovitost posameznikovega telesa in s tem povezanimi vprašanji, kot so na primer transfuzija krvi brez privolitve, prisilna sterilizacija itd.
- **Zasebnost osebnega obnašanja.** Nanaša se na vse vidike obnašanja, še posebej do občutljivih stvari kot, so navade, politične aktivnosti, verska prepričanja itd., tako na zasebnih kot javnih krajih.
- **Zasebnost osebnega komuniciranja.** Posamezniki izražajo interese po medsebojnem komuniciranju, uporabljajo različne medije, vendar brez rutinskega nadzorovanja s strani drugih oseb ali organizacij.
- **Zasebnost osebnih podatkov.** Posamezniki izražajo, da njihovi podatki ne smejo biti samodejno dostopni drugim posameznikom ter organizacijam. Tudi tam, kjer so podatki v lasti drugih oseb, bi morali imeti možnost določenega nadzora nad njimi in njihovo uporabo.

Po izjavah ljudi so glavni razlogi, s katerimi argumentirajo, zakaj je zasebnost pomembna naslednji:

- **Psihološki.** Ljudje morajo imeti zasebni prostor. To velja tako v javnosti kot za zaprtimi vrati. Sposobni moramo biti razgledati se po okolici, presojati, ali predstavljajo ljudje v bližini nevarnost, skakati od veselja itd.
- **Sociološki.** Ljudje morajo biti svobodni pri obnašanju in medsebojnem druženju, upoštevajoč pri tem moralne vrednote, vendar brez neprestane grožnje po nadzorovanju.
- **Ekonomski.** Ljudje morajo biti svobodni pri inoviranju, saj je mednarodna konkurenca vse močnejša. Razvite države z visokimi stroški dela morajo biti vse pametnejše, če želijo obdržati svoj standard življenja.

- **Politični.** Ljudje morajo biti svobodni pri razmišljanju, razpravljanju itd., saj nadzorovanje ovira obnašanje in govor ter ogroža demokracijo.

2.1 Informacijska zasebnost

Zasebnost je bila kot družbeno in pravno vprašanje dolgo časa skrb sociologov, filozofov in odvetnikov. Vendar se je s širšo uporabo modernih IT sistemov in komunikacijskih omrežij v smislu nekajkratnih dnevnih aktivnosti (npr. bančna opravila, nakupovanje, komuniciranje s prijatelji, sodelovanje z državnimi oblastmi itd.) postavila dodatna zahteva, to je varovanje elektronske zasebnosti posameznika. Združevanje področij računalništva in komunikacij, še posebej od leta 1980 dalje, je zasebnost osebnih podatkov in zasebnost osebnega komuniciranja tesno povezala, zaradi česar lahko kombinaciji obeh pravimo kar **informacijska zasebnost**.

Po poročilu Mednarodne skupnosti za telekomunikacijo obstajajo tri domene informacijske zasebnosti: **tehnična**, **regulatorna** in **sociološka**. Vsaka je svojevrstna vendar hkrati povezana z ostalimi (Privacy and Ubiquitous Network Societis, 2005, str. 9). Znotraj tehnične domene je zasebnost obravnavana kot snovalsko vprašanje, vezano na področja, kot sta mrežna varnost in snovanje uporabniških vmesnikov. Regulatorna domena obravnava zasebnost kot vprašanje varovanja podatkov ter s tem povezanimi zakoni in regulacijami. Sociološka domena pa zasebnost razume kot družbeno vprašanje, vezano na kulturne običaje, etiko in institucije (Slika 1).

Slika 1: Domene informacijske zasebnosti



Vir: Privacy and Ubiquitous Network Societis, 2005, str. 10

Zasebne informacije so lahko definirane kot »tista dejstva, komunikacije ali mnenja, ki se nanašajo na posameznika, in katere bi ta običajno imel za intimne ter zaupne, zaradi česar jih želi obdržati oziroma omejiti njihov pretok«. Ta izjava predstavlja glavno vprašanje informacijske zasebnosti: to je **nadzor** (Watt et al., 2001, str. 119).

Razpolaganje z zasebnimi informacijami je trenutno zelo vroča tema na internetu, saj je potreba po povečanju uporabnikove zasebnosti povsem v nasprotju s potrebami poslovnega sveta po zmanjšanju prevar. Osnovni cilj prvega je povečanje anonimnosti uporabnikov, medtem ko je osnovni cilj drugega neizbežna identifikacija in preverjanje uporabnikov. Tu je treba doseči določen kompromis, ki pa do danes žal še ni bil dosežen (Oppliger, 2005, str. 1796). Na drugi strani predstavlja dodatni izziv še potreba uporabnika po prilagojenih

elektronskih storitvah, ki se ponujajo preko poslovnih ali vladnih e-transakcij. Te storitve namreč delujejo povsem v nasprotju s splošnimi načeli zmanjševanja zbiranja informacij in njihovega shranjevanja, takoj ko odslužijo svojemu namenu.

Ključni element v zasebnosti je zmožnost združevanja in povezovanja informacij iz različnih virov, kar lahko privede do kršitve posameznikove zasebnosti, tudi če informacija iz vsakega vira velja za povsem neškodljivo. Podatki, ki se vtipkajo v spletne obrazce ali so vsebovani v obstoječi podatkovni bazi, se lahko skoraj neomejeno kombinirajo s transakcijskimi zapisi ter z zapisi o klikih posameznikov na internetu. Vprašanja povezana z zasebnostjo, so se s pojavom in dostopnostjo orodij ter storitev za podatkovno rudarjenje samo še stopnjevala.

Informacijska zasebnost in tehnologija

Na splošno je znano, da lahko uporaba tehnologij povzroči težave pri varovanju zasebnosti, saj imajo elektronski mediji drugačno skupino atributov kot dokumenti v tradicionalnem papirnatem svetu. Informacija ni več vezana na samo eno fizično mesto, lahko se kopira, premika ali celo spreminja brez vsakršnega sledu. Kljub temu pa varovanje elektronskih informacij pred njihovo izpostavljenostjo, spreminjanjem ali izgubo ni bil glavni kriterij pri snovanju omrežij ter programske/strojne opreme, ki trenutno vsebuje in procesira osebne podatke. Že od samega začetka interneta so bile sicer dodane nekatere lastnosti za izboljšanje varovanja podatkov, vendar ima osnovna zasnova omrežij še vedno resne pomanjkljivosti, ki se lahko izkoristijo za zbiranje zasebnih informacij ter izvajanje številnih prevar (Privacy Enhancing Technologies, 2005, str. 11).

Glavne značilnosti, povezane z zasebnostjo v različnih tehnoloških obdobjih, ki so predstavila nove informacijske tehnologije, so prikazane v Tabeli 1.

Tabela 1: Značilnosti, povezane z zasebnostjo v različnih tehnoloških obdobjih

Tehnološko obdobje	Značilnosti	Zmožnosti
Informacijsko	Centralizirano računalništvo / shranjevanje	Zbiranje, manipulacija
Mrežno	PC delovne postaje, LAN / WAN distribuirano računalništvo / shranjevanje	Zbiranje, manipulacija, komuniciranje
Internetno	PC brskalniki, neodvisne platforme, mrežno računalništvo / shranjevanje, Web storitve	Zbiranje, manipulacija, komuniciranje, delovni tok
Mobilno	Prenosniki, GSM telefoni, brezžične, mobilne storitve	Omejeno zbiranje in manipulacija, globalno komuniciranje in pozicioniranje

Vir: Turner, Dasgupta, 2003, str. 10

Zgodovinsko gledano je bila hitra predstavitev novih informacijskih tehnologij z razvijajočimi se zmožnostmi za nadzorovanje, shranjevanje, komuniciranje in pridobivanje osebnih informacij povod za sprožitev verižnega cikla dogodkov, poznanega kot cikel zasebnosti informacijskih tehnologij (Slika 2). Ta se začne s predstavitvijo nove informacijske tehnologije, ki poveča zmožnost posameznika ali organizacije, da zbira informacije o ljudeh in njihovih navadah. Z večanjem števila organizacij, ki sprejemajo, vpeljujejo in izkoriščajo tehnologijo, se večja tudi zaskrbljenost v javnosti, zaradi česar se jo začne obravnavati kot

grožnjo posameznikovi zasebnosti. Stopnjevanje pritiska na vlado povzroči pripravo/sprejetje nove zakonodaje in regulativ zasebnosti. Neizogibno se razvijejo nove tehnologije, ki začenjajo nov cikel zasebnosti informacijskih tehnologij (Tuner C., Dasgupta, 2003, str. 10).

Slika 2: Cikel zasebnosti informacijskih tehnologij

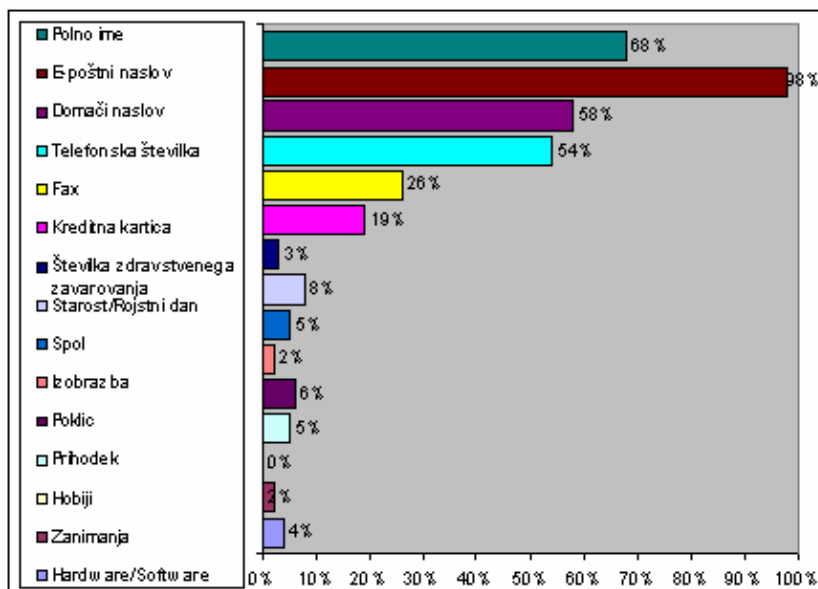


Vir: Turner C., Dasgupta, 2003, str. 10

2.2 Zasebnost in uporabniki interneta

Internet omogoča učinkovito in nedrugo zbiranje informacij, običajno brez dovoljenja uporabnikov interneta in z edinstvenimi načini. Raziskava FTC-ja iz leta 1998 je pokazala, da kar 92 % spletnih strani zbira vsaj eno izmed osebnih informacij (Slika 3). Med drugim so te sposobne ustvariti tudi osebne profile svojih potrošnikov in sicer s povezovanjem osebno identifikacijskih informacij (npr. ime, e-poštni naslov, domači naslov itd.) ter demografskih informacij (npr. spol, preference itd.) (Privacy Online, 1998, str. 23–25). Denarna vrednost teh informacij je eden izmed glavnih razlogov za njihovo tako množično zbiranje.

Slika 3: Delež spletnih strani, ki zbirajo posamezne osebne informacije



Vir: Privacy Online, 1998, str. 25

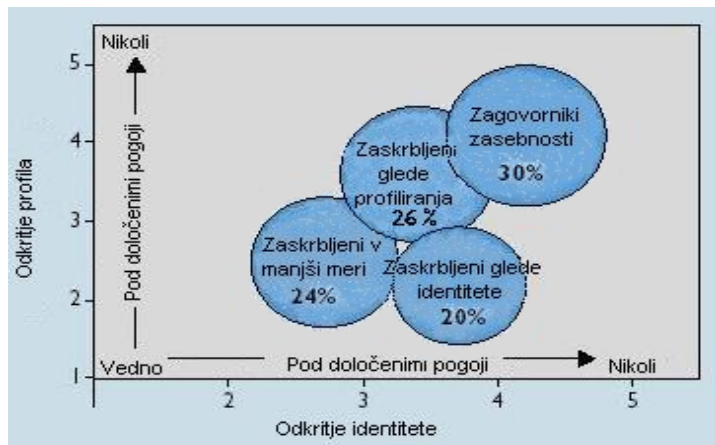
Vse to pri uporabnikih interneta povzroča splošno zaskrbljenost glede njihovih zasebnih pravic. Predvsem jih skrbi varnost njihovih osebnih informacij, strah pred njihovimi možnimi zlorabami, in kako se z njimi trenutno ravna oziroma se bo ravnalo v prihodnosti. Bolj natančno so opredelili naslednje vrste groženj zasebnosti, nad katerimi so zaskrbljeni (Chung, Paynter, 25. 3. 2007):

- obiski spletnih strani bodo naskrivaj nadzirani,
- naslovi e-pošte in druge osebne informacije se bodo shranjevale brez dovoljenja in bodo uporabljene za marketinške in druge namene,
- osebne informacije se bodo prodale tretjim osebam brez dovoljenja,
- kraja kreditnih kartic.

Raziskava o preferencah uporabnikov interneta do zasebnosti je pokazala, da jih lahko glede na njihovo usmeritve razdelimo v tri skupine (Ackerman S., Cranor Faith, Reagle, 1999, str. 3):

- **Zagovorniki zasebnosti** so zelo zaskrbljeni glede kakršne koli uporabe njihovih podatkov in na splošno neradi posredujejo svoje podatke spletnim stranem tudi v primerih, ko so mehanizmi varovanja nameščeni.
- **Pragmatiki** so prav tako zaskrbljeni nad uporabo podatkov, vendar manj kot zagovorniki zasebnosti. Pogosto imajo specifične skrbi in posebne načine za njihovo reševanje. S prisotnostjo ukrepov varovanja, kot so zakonodaja zasebnosti ali objavljena politika zasebnosti na spletnih straneh, se je njihova zaskrbljenost bistveno zmanjšala. Znotraj te skupine je mogoče identificirati tiste, ki so bolj zaskrbljeni glede *identitete*, in tiste, ki so bolj zaskrbljeni glede *profiliranja* (Slika 4) (Berendt, Günther, Spiekermann, 2005, str. 104).
- **Zaskrbljeni v manjši meri** so na splošno pripravljeni posredovati podatke spletnim stranem skoraj pod vsakim pogojem, čeprav pogosto izražajo milejšo obliko zaskrbljenosti glede zasebnosti.

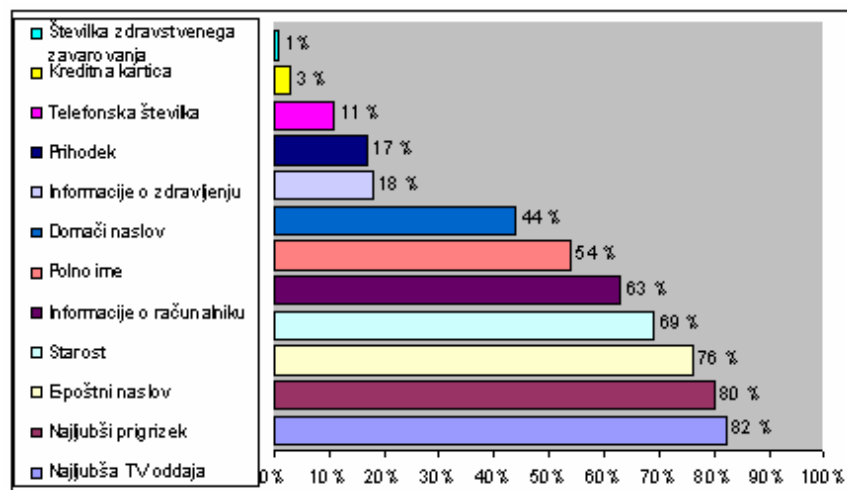
Slika 4: Usmeritve uporabnikov interneta glede zasebnosti



Vir: Berendt, Günther, Spiekermann, 2005, str. 103

Med drugim je bilo tudi ugotovljeno, da ti posredujejo osebne informacije spletnim stranem z različno lagodnostjo, odvisno od tega, za kako občutljive jih imajo (Slika 5). Veliko informacij se ima že po naravi za zasebne, med temi so najbolj občutljive tiste o zdravju, financah, verski ali politični pripadnosti. Toda glede na vsebino se ima lahko tudi nepomembne informacije, kot so nakupovalni vzorci, informacije o telefonskem pogovoru ali geografski lokaciji, za občutljive.

Slika 5: Delež uporabnikov interneta, ki lagodno posredujejo posamezne osebne informacije



Vir: Cranor Faith, Ackerman S., Reagle, 1999, str. 3

Ostale podobne raziskave so še pokazale, da uporabniki interneta raje podajo osebne informacije v primerih, ko niso identificirani, ter da ne marajo nezaželene komunikacije ali katere koli druge oblike samodejnega prenosa podatkov. Večina jih želi biti informirana o tem, katere informacije o njih se zbirajo, kako bodo podatki uporabljeni, in ali se bodo informacije uporabile samo v agregatni obliki. Poslovno prakso vidijo kot manj vsiljivo do zasebnosti, kadar so seznanjeni, da se informacije zbirajo v okviru obstoječega sodelovanja, če je to pomembno za izvedbo transakcije, za vzpostavitev zanesljivih in veljavnih vmesnikov, in če imajo nadzor nad njihovo prihodnjo uporabo. Nenazadnje je spremljanje potrošnikov, ki so bili pripravljeni trgovati za ugodnosti v zameno za odstop od svojih interesov glede zasebnosti, pokazalo, da se njihova percepcija o tem kaj sestavlja primerna informacijska načela, spreminja med uporabo interneta in da je praksa zbiranja informacij nekje sprejemljiva drugje pa povsem nesprejemljiva. Drugače povedano, to je percepcija o tem, ali so osebne informacije, ki so bile zbrane za potrebe zavarovanja, zaposlovanja, direktnega trženja itd., predstavljale korist oziroma grožnjo zasebnosti, kar se spreminja v odvisnosti od namena. Pri tem uporabniki interneta večkrat ravnaajo v nasprotju z njihovimi splošnimi preferencami glede zasebnosti, saj so pogosto pripravljeni podati več informacij, kot bi jih sicer. Ta protislovnost je dokaz, da so usmeritve in obnašanja pri varovanju osebnih informacij stvar pogajanj, odvisno od situacije, vrste zahtevanih informacij, pogojev uporabe informacij, ponujenih ugodnosti v zameno za informacije in obsega do katerega se bodo te delile (Tuner C., Dasgupta, 2003, str. 11). Prav tako se je izkazalo, da je pomembnost posameznih faktorjev, ki vplivajo na njihovo zaupanje do zasebnih praks spletnih strani, različna (Tabela 2) (Earp B., Baumer, 2003, str. 83).

Tabela 2: Vrstni red faktorjev, ki vplivajo na zaupanje do praks zasebnosti spletnih strani

Vrstni red najbolj vplivnih faktorjev	Faktor
1	Ime podjetja
2	Možnost izstopa »opt-out«
3	Prisotnost politike zasebnosti
4	Prisotnost pečata zasebnosti
5	Oblika spletne strani

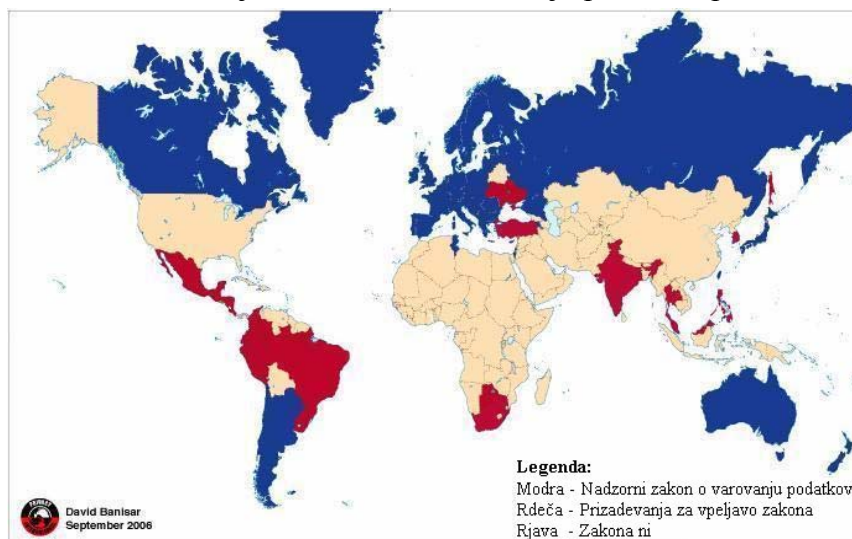
Vir: Earp B., Baumer, 2003, str. 83

Berend, Günther in Spiekermann so prišli do spoznanja, da ima mnogo uporabnikov interneta sicer močna prepričanja glede zasebnosti in da izražajo tudi svoje preference, vendar niso sposobni primerno ukrepati. Ko se enkrat znajdejo v spletni transakciji, namreč pogosto ne nadzorujejo dovolj svojih dejanj. Preveč se zanašajo na varovanje s strani zakonodaje, čeprav je znano, da imajo zakoni in regulative težave pri odzivanju na hitre spremembe v internetni komunikaciji (Berendt, Günther, Spiekermann, 2005, str. 105–106).

2.3 Inštrumenti varovanja zasebnosti

Internet je mednarodni in večinoma nereguliran, kar pomeni, da se zakoni katere koli države običajno ne uporabljajo za internetne aktivnosti, ki izhajajo iz drugih držav. Vse države danes ne implementirajo zakonov vezanih na internetno zasebnost (Slika 6), zato je zelo pomembno, da se razpravlja o tem, kako bi se doseglo varovanje zasebnosti na globalen konsistenten način. Trenutno prevladuje prepričanje, da se lahko to doseže z uporabo kombiniranih rešitev. Kombinacija zakonodajnih, samoregulacijskih in tehnoloških rešitev lahko zagotovi sinergijo, ki je veliko bolj učinkovita kot posamezne rešitve. Medtem, ko so samoregulacije in tehnologije za varovanje zasebnosti dobrodošle pri razvoju ustreznega varovanja zasebnosti, pa mogoče same po sebi niso zadostne, zato jih lahko spremlja še zakonodaja (Chung, Paynter, 25. 3. 2007).

Slika 6: Razširjenost zakona o varovanju podatkov po svetu



Vir: [URL:<http://www.privacyinternational.org/survey/dmap.jpg>], 16. 1. 2007

Trenutno obstajajo štiri glavni modeli varovanja zasebnosti. Glede na uporabo, so lahko komplementarni ali kontradiktorni. V državah, kjer najbolj učinkovito varujejo zasebnost, so uporabljeni vsi štiri modeli (PHR–2004 Overview of Privacy, 13. 11. 2004):

- ***Nadzorni zakoni***

V številnih državah po svetu obstaja splošni zakon, ki opredeljuje zbiranje, uporabo in širjenje osebnih informacij tako v javnem kot v zasebnem sektorju. To je preferenčni model za večino držav, ki uporabljajo zakone za varovanje podatkov in je bil uporabljen tudi s strani Evropske unije za zagotovitev skladnosti s svojim lastnim režimom varovanja podatkov.

- ***Sektorski zakoni***

Nekatere države, kot so ZDA, so se izognile uzakonitvi splošnih pravil za varovanje podatkov in so bolj naklonjene sektorskim zakonom, ki urejajo specifično področje, na primer izposajo video kaset, finance itd. Glavni problem tega pristopa je, da zahteva sprejetje nove zakonodaje za vsako novonastalo tehnologijo, zaradi česar varovanje pogosto zaostaja. Pomanjkanje pravnega varovanja posameznikove zasebnosti na internetu v ZDA je zgovoren primer njihovih omejitev. Med drugim obstaja še problem pomanjkanja splošne krovne nadzorne agencije. V številnih državah so sektorski zakoni uporabljeni kot dopolnilo nadzornim zakonom za zagotavljanje bolj podrobnega varovanja za posamezno kategorijo informacij, kot so telekomunikacije, policijske kartoteke ali kreditni zapiski potrošnikov.

- ***Samoregulacije***

Varovanje podatkov se lahko teoretično doseže s številnimi oblikami samoregulacij, v katerih podjetja/industrije vzpostavijo pravila in načela glede zbiranja podatkov in tako nadzorujejo sama sebe. V mnogih državah, še posebej pa v ZDA, je ta način prinesel popolno razočaranje in malo oprijemljivih dokazov, da se vzpostavljena pravila in načela glede zbiranja podatkov tudi dejansko izvajajo. Ustrezna pravila in nadzor sta glavna problema tega pristopa. Industrijska pravila so tako v mnogih državah zagotovila zelo skromno varovanje in slab nadzor.

- ***Tehnologije zasebnosti***

Z razvojem komercialno dostopnih tehnološko zasnovanih sistemov se je zasebnost preselila tudi v roke posameznih uporabnikov. Ti lahko uporabijo številne programe in sisteme, ki zagotavljajo različne stopnje zasebnosti in varnosti komuniciranja (npr. šifriranje, vmesni strežniki itd.). Nenazadnje se morajo zavedati dejstva, da vsa orodja ne varujejo zasebnosti učinkovito, saj so lahko nekatera slabo zasnovana, medtem ko so lahko druga zasnovana za lažje zakonsko dostopanje.

Trenutne raziskave, ki potekajo na področju zasebnosti uporabnikov, opredeljujejo pot za varovanje zasebnosti v smislu štirih zahtev in sicer (Kavakli, Kalloniatis, Gritzalis, 12. 12. 2006):

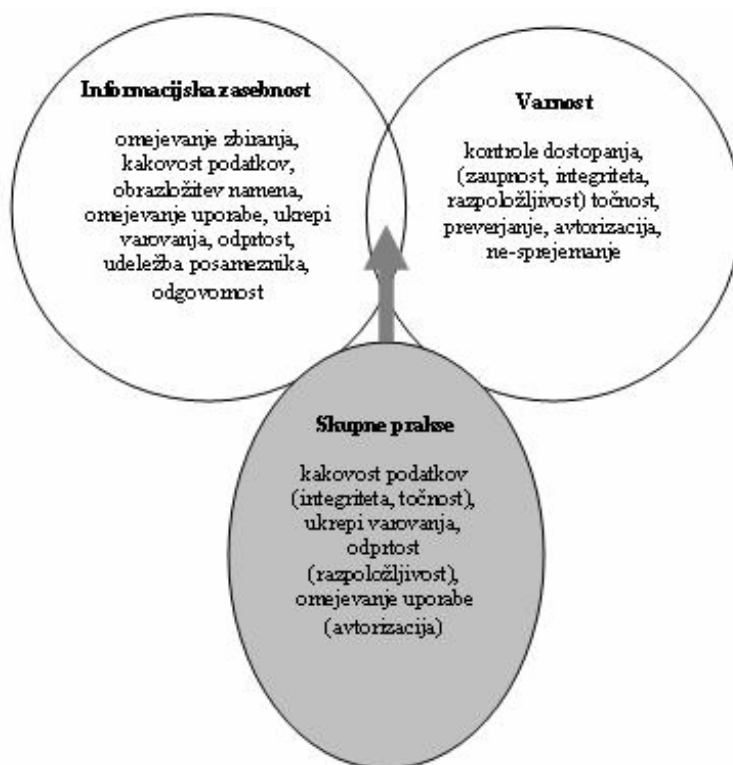
- **Anonimnost** je stanje, ko je uporabnik anonimen ali virtualno neviden; ima možnost delovati na spletu, ne da bi bil pri tem zasledovan oziroma lahko uporabi vir ali storitev brez odkritja svoje identitete. Anonimnost služi glavnemu namenu, to je skrivanju osebno identifikacijskih informacij, kadar ni potrebe po njihovem odkritju. Navigiranje po internetu samo z namenom pridobivanja informacij je eno izmed vprašanj, pri katerem igra anonimnost pomembno vlogo.
- **Psevdonimnost** je možnost uporabnika, da uporablja vir ali storitev pod enim ali več psevdonimi (vzdevki) ter tako skrije svojo pravo identiteto. V nekaterih situacijah (npr. kršenje zakonov) je kljub temu še vedno mogoče prevesti psevdonim v pravo identiteto. Psevdonimnost ima podobne značilnosti kot anonimnost in sicer v tem, da uporabnika ni mogoče identificirati, vendar ga je mogoče izslediti preko uporabljenih vzdevkov. Uporablja se za varovanje uporabnikove identitete v primerih, ko anonimnost ne more biti zagotovljena (npr. ko mora biti uporabnik odgovoren za svoja dejanja).
- **Nepovezljivost** izraža nezmožnost povezovanja sorodnih informacij. Ta je še posebej uspešno dosežena, kadar napadalec ni zmožen povezati specifične informacije z uporabnikom, ki te informacije procesira. Med drugim je lahko nepovezljivost uspešno dosežena tudi med pošiljateljem in prejemnikom. V tem primeru nepovezljivost pomeni to, da pošiljatelj in prejemnik ne moreta biti identificirana, da sodelujeta v medsebojni komunikaciji. Zmožnost povezovanja transakcij bi lahko dala opazovalcu tudi namig o vsakdanjih navadah posameznika ali pa zavarovalnici idejo, koliko alkohola porabi družina v mesecu. Zagotavljanje nepovezljivosti je ključna za varovanje uporabnikove zasebnosti.
- **Neopazovanost** varuje uporabnika pred opazovanjem ali sledenjem med navigiranjem po internetu ali dostopanju do storitev. Neopazovanost je podobna nepovezljivosti v smislu, da namerava napadalec odkriti uporabnikove identifikacijske informacije rajši s opazovanjem kot pa s povezovanjem informacij, ki jih je ta odkril.

2.4 Zasebnost in varnost

Literatura prikazuje primere različnih konceptov povezav med zasebnostjo in varnostjo. Primerjava skupno sprejetih elementov varnosti in zasebnosti je pokazala, da lahko nekatere

komponente varovanja zasebnosti naslovimo z mehanizmi varnosti, nekaterih pa ne (Slika 7). Nekatere varnostne funkcije lahko ovirajo ali celo ogrozijo potrebno varovanje zasebnosti, na drugi strani pa lahko tudi ukrepi zasebnosti oslabijo ali ogrozijo upravičene varnostne ukrepe, kar predstavlja svojevrsten varnostno – zasebnostni paradoks (The Security – Privacy Paradox, 2003, str. 3). Tehnično prekrivanje zasebnosti in varnosti bi lahko deloma pojasnili z dejstvom, da oba služita enakim moralnim načelom, to je zadovoljitev psiholoških potreb posameznika, da se počutiti varnega pred zunanjimi vmesniki. Sta del tako imenovanega »varovalnega plašča«, ki pospešuje gradnjo identitete, obenem pa sta tudi nujna pri gradnji zaupanja (Stahl Carsten, 20. 3. 2007).

Slika 7: Primerjava elementov informacijske varnosti in zasebnosti



Vir: The Security – Privacy Paradox, 2003, str. 4

Kadar se v tehnološki družbi govori o varnosti, se na splošno misli na varovanje podatkov pred naključnim odkritjem, napačno uporabo ali zlorabo, uničenjem podatkov in sicer osebno identifikacijskih ali katerih koli drugih. Varnost lahko vključuje shranjevanje, prenašanje, varnostne kopije in druge transakcije, ki vključujejo podatke. Varnostne rešitve, produkti in storitve poskušajo preprečiti aktiviranje virusov, odpraviti ranljivost omrežij, omejiti dostop neavtoriziranim uporabnikom ter preveriti podatke, sporočila ali uporabnike. To so kritična orodja za varovanje shranjenih ali prenesenih osebnih informacij. Brez varnostnih tehnologij bi bilo zelo težko ali celo nemogoče varovati podatke in ponuditi orodja zasebnosti posameznikom, korporacijam in drugim organizacijam. Zmožnost nudenja izbire potrošnikom glede zbiranja in varovanja zbranih ali shranjenih podatkov, temelji na široko dostopnih in močnih varnostnih tehnologijah. Poleg potrebe, da so osebni podatki varovani z ustreznimi mehanizmi varnosti, vključuje varovanje zasebnosti omejitev pravno dovoljene narave zbiranja, ravnanja ali prenosa osebno identifikacijskih in agregatnih informacij, ki so bile

zbrane od posameznih uporabnikov. Ali se osebna informacija zbira, kako je uporabljena ali deljena, kakšne možnosti ima uporabnik, ali lahko uporabnik dostopa do informacij in kdo je dostopal do zbranih informacij, pa so vsa vprašanja zasebnosti (Privacy Online: OECD Guidance on Policy and Practise, 2003, str. 257).

Tako tesna povezava med konceptoma zasebnosti in varnosti je pogosto razlog za zmedenost pri številnih ljudeh. Trenutno še ni povsem jasno, kaj točno sestavlja zasebnost kot tudi ni splošnega dogovora glede definicije varnosti. Na zasebnost se prepogosto gleda kot na politično, na varnost pa kot na tehnološko vprašanje. Prav tako še ni dogovora o tem, kako naj bodo ti koncepti varovani (z etiko, zakoni, trgom ali drugimi mehanizmi), ali kdo naj bi bil zanje odgovoren (država, posameznik, organizacije itd.).

3 GROŽNJE ZASEBNOSTI V INFORMACIJSKI DRUŽBI

Grožnje zasebnosti prihajajo iz različnih virov. Na splošno jih lahko razdelimo v tri skupine (Rotenberg, 6. 1. 2007):

- ***Tehnološke grožnje***

V moderni dobi se na tehnologijo pogosto gleda kot na vir številnih groženj zasebnosti. Vzrok lahko najdemo v dejstvu, da tehnologija skozi čas prevzema določene oblike, kar lahko pripelje do sprejetja novih, izpopolnjenih sistemov za nadzorovanje. Med ključnimi značilnostmi tehnologij v nadzorovanem okolju so pojačanje, rutinizacija in pomanjšanje.

Pojačanje se nanaša na zmožnost tehnologije, da razširi možnosti zbiranja informacij in da vdre v zasebna življenja. Tehnike pojačanja zajemajo tudi druge informacije izven tistih, ki so bile upravičeno odobrene (npr. potrebne zaradi boja proti kriminalu). Reguliranje teh tehnik namesto aktivnosti, neizbežno povečuje nevarnost kriminalnega obnašanja, saj bi lahko slednje veljale za dopustne. Zato je ena prvih nalog zakonodaje zasebnosti osredinjavanje na spremljajoče aktivnosti, in ne na samo tehnologijo.

Rutinizacija je proces, ki naredi vdiranje v zasebna življenja za nepretrgan proces. Tehnologija je tu uporabljena z namenom, da se zgradi vzorec ali prakso nadzorovanja. Tehnike rutinizacije so običajno združene z metodami za zapisovanje. Trenutno smo še vedno na začetni stopnji vključevanja novih tehnik v svet rutiniziranega nadzorovanja, vendar lahko pričakujemo, da bo naslednja stopnja v teh sistemih sprejetje metod za procesiranje informacij.

Pomanjšanje je način, s katerim je tehnike za vdiranje v zasebnost veliko težje odkriti. Majhne naprave za zbiranje podatkov so še posebej problematične, saj imajo posamezniki tu le malo možnosti, da se izognejo zaznavanju. Nenazadnje obstaja tudi v svetu politike le malo priložnosti za spoprijemanje z željami po takih tehnikah.

- ***Vladne grožnje***

Veliko najresnejših groženj zasebnosti prihaja s strani vlad, ki lahko zmanjšajo zasebnost z različnimi programi (npr. za zbiranje identifikacij, profiliranje na podlagi podatkovnih baz itd.). Te grožnje so še posebej problematične, saj z vzpostavitvijo omenjenih programov državljan nima druge izbire, kot da se podredi. Aktivnosti vlad, ki so povzročile največ neodobravanja, so pogosto vključevale tudi predloge vezane na reguliranje uporabe tehnologij za varovanje zasebnosti (npr. šifriranje).

- ***Korporacijske grožnje***

Korporacije ogrožajo zasebnost na številne načine. Eden izmed teh je izvajanje nadzora zaposlenimi z nadzorovalnimi in opazovalnimi praksami (uporaba računalnikov, video nadzor itd.). Če na zasebnost gledamo širše, je ta na trgu ogrožena predvsem zaradi pridobivanja komercialnih vrednosti iz osebno identifikacijskih transakcij potrošnikov. Pri strankah sedaj ne zadostuje več samo plačilo za dobrine in storitve, ampak morajo podati tudi svoje osebne podatke, ki jih lahko podjetja kasneje uporabijo za povsem druge namene. Napor za odpravo teh procesov so osredinjeni bodisi na reguliranje omejitev zbiranja informacij ali na tehnična sredstva, ki pri komercialnih transakcijah ne zahtevajo odkritja osebno identifikacijskih informacij.

Raziskava o globalni zasebnosti, ki je bila opravljena s strani Združenja za človekove pravice (PI) in Informacijskega centra za elektronsko zasebnost (EPIC), in v kateri se je ocenjevalo stanje na področju tehnologij, nadzorovanja in varovanja zasebnosti po posameznih državah, je pokazala, da je zasebnost po svetu različno ogrožena (Slika 8) (2006 International Privacy Survey: Ranking by Countries, 13. 3. 2007).

Slika 8. Vodilne družbe nadzorovanja v EU in po svetu



Vir: [URL:[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-545269&als\[theme\]=Privacy%20and%20Human%20Rights](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-545269&als[theme]=Privacy%20and%20Human%20Rights)], 28. 1. 2007

3.1 Metode zbiranja podatkov

Zbiranje podatkov je možno na več načinov in ni dvoma, da se bodo z napredkom v tehnologiji pojavile nove tehnike, ki bodo to še olajšale. V nadaljevanju bom predstavil trenutno najbolj razširjene oblike.

Komercialne spletne strani zbirajo podatke s prostovoljnimi in pasivnimi načini. Prostovoljni načini vključujejo spletne strani za registracijo, spletne ankete in druge spletne obrazce. Pri tem se ponavadi zahteva določena aktivnost uporabnika interneta, zaradi česar se ta zaveda posredovanja oziroma zbiranja določenih podatkov. Pasivni načini pa tipično vključujejo agregatno zbiranje podatkov in uporabo spletnih strani, pri čemer se uporabnik mogoče ne zaveda, da se zbirajo večinoma neosebne informacije (Privacy Online: OECD Guidance on Policy and Practise, 2003, str. 249).

3.1.1 Pasivno zbiranje podatkov

Neosebni podatki, ki se odkrijejo z navigiranjem po spletnih straneh, povedo veliko o internetnih aktivnostih. Spletni strežniki lahko zbirajo informacije o spletnih straneh, ki jih je uporabnik pogledal, koliko časa je bila določena stran posredovana na zaslonu, URL naslov nedavno obiskane spletne strani in URL naslov naslednje zahtevane spletne strani.

Nobena od teh informacij ni neposredno osebno identifikacijska, večinoma so agregatne in se uporabljajo za analizo trga ter spletnih strani. Na primer, za spletnega operaterja je lahko zelo pomemben podatek, da je njihovo osnovno stran obiskalo 100.000 ljudi v enem mesecu, medtem ko je stran z utripajočo naslovnico »vroča ponudba« obiskalo le 2.000 ljudi. Večina teh informacij se zbira tudi z namenom, da se administratorjem omogoči opravljanje potrebnega systemskega vzdrževanja, kontroliranja, optimiziranje zmogljivosti do posameznikovega računalnika, povečanje hitrosti ter ostala dela na sistemskih funkcijah, s čimer se zagotovi pravilno delovanje spletne strani in pravočasni dostop obiskovalcem.

Datoteka dogodkov

Vsakič, ko spletni brskalnik naloži stran, se zapis tega dogodka samodejno zabeleži na oddaljenem strežniku v spletni datoteki dogodkov (*Web Logs*) (Slika 9). Če je spletna stran prikazana z uporabo podatkovnega strežnika, lahko le ta ustvari svojo spletno datoteko dogodkov. Navsezadnje se spletne datoteke dogodkov samodejno ohranjajo tudi na mrežnih požarnih zidovih, vmesnih strežnikih (*Proxy*) in spletnih pomnilnikih. Posledica enostavne spletne navigacije so tako lahko številni shranjeni zapisi na napravah in to na lokacijah, ki so pod nadzorom različnih organizacij, kar lahko predstavlja tudi določeno grožnjo. Spletne datoteke dogodkov se pogosto zahtevajo in uporabljajo v pravnih postopkih ali kriminalnih raziskavah, pri nadzoru aktivnosti zaposlenih, s strani sistemskih administratorjev pa med drugim tudi za vohunjenje. Vendar v večini primerov teh informacij nihče ne pregleda (Garfinkel, Spafford, 2002, str. 211).

Informacije, ki so shranjene v spletnih datotekah dogodkov oziroma se lahko iz njih hitro razberejo, so naslednje:

- ime in IP naslov računalnika, ki je naložil spletno stran,
- čas zahtevka,
- zahtevani URL naslov,
- potrebni čas nalaganja datoteke,
- v primeru HTTP preverjanja uporabniško ime osebe, ki je naložila datoteko,
- kakršne koli napake,
- predhodno naložena spletna stran s strani spletnega brskalnika,
- vrsta uporabljenega spletnega brskalnika.

Slika 9: Spletna datoteka dogodkov, zabeležena na strežniku

```
Prosti-klic-77.freeport.mwci.net - - [09/Mar/1997:00:04:11 -500]
' DOBI /awa/issue2/Woodstock.gif HTTP/1.0' 200 26385
' http://www.vineyard.net/awa/issue2/Wood.html '
' Mozilla/2.0 (kompatibilno; MSIE 3.01; Windows 95) '
```

Vir: Garfinkel, Spafford, 2002, str. 213

Tudi za poslano, prejeto ali preneseno e-sporočilo preko strežnika obstaja velika verjetnost da je nekje program, ki zapisuje te podatke v poštno datoteko dogodkov (*Mail Logs*). Ta ponavadi vsebuje "od: " in " za: " naslove, čas, ko je bilo sporočilo poslano, in oznako sporočila. Naslovna vrstica in vsebina ponavadi nista zabeleženi, čeprav bi zagotovo lahko bili.

3.1.2 Aktivno zbiranje podatkov

Veliko spletnih strani aktivno zbira transakcijske ali osebne informacije in sicer z uporabo specifičnih tehnologij ali poslovnih procesov na njihovih straneh. Nekateri izmed teh pristopov so dokaj jasni in pri zbiranju podatkov zahtevajo sodelovanje uporabnika interneta (npr. spletni obrazci in uporabniški računi itd.), drugi pa so obiskovalcu spletne strani manj očitni (npr. spletni piškotki in hrošči itd.).

Spletni piškotki

Spletni piškotek je tekstovna datoteka ponavadi manjša od 4 KB, ki jo namesti spletni strežnik na posameznikov računalnik (trdi disk) z dodatno vrstico v glavi HTTP protokola (Slika 10) (Debussere, 2005, str. 74). Pokazali so se kot najbolj zanesljiv, robusten in omrežju prijazen način za zagotavljanje funkcionalnega stanja na spletu (Slika 11). Spletne piškotke lahko glede na čas trajanja razdelimo v dve skupini: sejne in stalno prisotne. Sejni shranijo informacije v začasni pomnilnik in trajajo tako dolgo kot seja spletnega brskalnika s spletnim strežnikom, vse do zaprtja spletnega brskalnika. Stalno prisotni pa jih shranijo na trdi disk računalnika in trajajo tako dolgo, dokler jim ne poteče datum oziroma so izbrisani. Druga

delitev poteka glede na to, katera spletna stran je namestila spletni piškotek, in sicer: prva – stran ali tretja – stran. V prvem primeru gre za osnovno spletno stran, ki jo obiskuje uporabnik, v drugem primeru pa za spletno stran, ki nudi storitve osnovni spletni strani.

Slika 10: Spletni piškotek v glavi HTTP protokola

```

Http/1.1 200 OK
Vsebina-dolžina: 22592
Strežnik: Microsoft-IIS/5.0
Datum: Sat, 21 Apr 2001 12:05:56 GMT
Namesti-piškotek: lubid=018AE17403512; poteče=Mon, 18-Jan-2038 08:00 GMT; domena=.lycos.com; pot=/
Vsebina-tip: tekst/html
Pomnilnik-kontrola: zasebna

```

Vir: Garfinkel, Spafford, 2002, str. 217

Slika 11: Komunikacija med odjemalcem in strežnikom pri namestitvi spletnega piškotka



Vir: [URL:<http://www.oreilly.com/catalog/learnphp5/chapter/ch08.pdf>], 20. 12. 2006

V spletnih piškotkih sta lahko shranjeni dve vrsti informacij: osebno identifikacijske in osebno neidentifikacijske. Prve so sestavljene iz podatkov, ki se uporabljajo za identifikacijo posameznika in ki jih spletnim stranem ponavadi posreduje že posameznik sam (npr. pri e-trgovini). Druge pa niso povezane z nobeno posamezno osebno informacijo in jih tipično sestavljajo tako imenovani podatki o klikih (npr. kolikokrat je posameznik kliknil na spletno oglasno vrstico). Potencialna grožnja spletnih piškotov ni v informacijah, ki so shranjene na uporabnikovem računalniku, ampak v tem, kaj lahko podjetja z njimi naredijo. Že od samega začetka so bili uporabljeni tudi za zlonamerna dejanja, kar ji je uvrstilo na seznam številnih vprašanj zasebnosti, kot so napadi na zasebnost in kršitev zavestne privolitve. V letu 2002 sta bili tako proti oglaševalskemu podjetju DoubleClick, Inc. vloženi dve tožbi, ki sta utemeljevali, da je omenjeno podjetje uporabljalo spletne piškotke za sledenje aktivnostim uporabnikov interneta brez njihovega pravega dovoljenja ter da je zbrane informacije uporabljalo za ustvarjanje njihovih obsežnih profilov (Ha et al., 12. 10. 2005).

Prav tako predstavljajo za uporabnika različno vrednost (Tabela 3), odvisno od tega, ali so nastavljeni zato, da mu olajšajo delo (npr. pomnjenje gesel in omogočanje preferenc itd.), ali pa so nastavljeni zato, da omogočajo spletni strani slediti njegovemu obnašanju

(nadzorovanje) (Market View: A New Cookie Cutter for Classifying Web Cookies, 27. 8. 2005).

Tabela 3: Besedni zaklad spletnih piškotkov

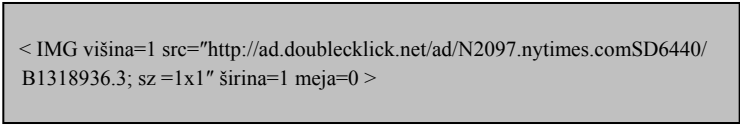
Vrednost za uporabnika	Zbiranje	Namen procesiranja	Strežnikov vir	Primer	Opis
Visoka 	Ena-stran (piškotek sledi obnašanju ene strani)	Omogočanje (zmanjšuje delo uporabniku)	Prva-stran	Amazon.com	Amazon shranjuje informacije o obiskovalcu in preference, da mu omogoči personalizacijo na spletni strani in priporočila
			Tretja-stran	Clickability, uporabljen na Nascar.com	Nascar.com uporablja Clickability za ustvarjanje »shrani«, »natisni« in drugih gumbov na svoji strani (Clickability prav tako nadzoruje uporabo teh gumbov za Nascar.com)
Minimalna 	Ena-stran	Nadzorovanje (gleda obnašanje; ni takojšne koristi za uporabnika)	Prva-stran	American Express.com	American Express uporablja spletno analitične programe (Sane) za nadzorovanje uporabnikovega obnašanja
			Tretja-stran	Omniture, uporabljen na Classmates.com	Classmates.com uporablja spletno analitične storitve tretjih oseb (Omniture) za nadzorovanje uporabnikovega obnašanja
Grožnja 	Več-strani (piškotek sledi obnašanju na več straneh)	Nadzorovanje	Tretja-stran	ValueClick, Claria uporabljen na Classmates.com	Ta oglaševalska omrežja zbirajo obnašanja pri navigiranju kot način za ponujanje relevantnih oglasov

Vir: Market View: A New Cookie Cutter for Classifying Web Cookies, 27. 8. 2005, str. 3

Spletni hrošči

Spletni hrošči (*Web bugs*) so naslednji široko uporabljeni inštrument, ki predstavlja grožnjo zasebnosti, uporabljajoč pri tem spletne tehnologije zasledovanja (Slika 12). So nevidne grafične slike, znane tudi kot GIF slike velikosti 1x1 pik (*pixel*) in so lahko naskrivaj dodane kateri koli spletni strani, e-pošti in pisarniškim datotekam z namenom zbiranja informacij o obnašanju internetnega uporabnika. Spletni hrošči pošiljajo pridobljene informacije nazaj k spletnim strežnikom in sicer za potrebe oglaševanja ali internetnega trga. Sporni niso samo zaradi dejstva, da se pogosto uporabljajo za zbiranje informacij o uporabniku brez njegove privolitve, ampak tudi zato, ker preliščijo spletni brskalnik, da pri tem nadzorovanju sodeluje z utemeljitvijo, da je slika sestavni del spletne strani.

Slika 12: Spletni hrošč, odkrit na spletni strani New York Times-a



```
< IMG višina=1 src="http://ad.doubleclick.net/ad/N2097.nytimes.comSD6440/B1318936.3; sz=1x1" širina=1 meja=0 >
```

Vir: Cranor Faith, Garfinkel, 2005, str. 478

Spletni hrošči se lahko uporabljajo tudi z namenom (Martin, Wu, Alsaid, 2003, str. 260):

- štetja, kolikokrat je bila določena spletna stran ogledana;
- prenosa demografskih podatkov o obiskovalcih spletnih strani k marketinškem podjetjem. Te informacije se tipično uporabljajo za namene spletnega profiliranja;
- prenosa osebno identifikacijskih informacij o obiskovalcih spletnih strani k marketinškem podjetjem. Te informacije se tipično uporablja za namene spletnega profiliranja. Lahko se kombinirajo tudi z demografskimi podatki;
- profiliranja posameznikov preko spremljanja strani, ki so jih obiskali znotraj številnih spletnih strani;
- posredovanja iskalnih besed iz vnosne vrstice spletnega iskalnika k marketinškem podjetjem;
- povezave nakupa uporabnika s predhodno ogledanim oglasom;
- štetja, kolikokrat se je določeni oglas pojavil;
- poročanja spletni strani o vrsti in nastavitvi spletnega brskalnika, ki ga uporablja obiskovalec. Te informacije se uporabljajo v agregatni obliki za potrebe določanja vsebine na spletni strani, da si jo bo lahko ogledala večina obiskovalcev;
- omogočanje tretjim osebam, da nudijo strežniško logiranje spletnim stranem, ki tega ne morejo opraviti samostojno.

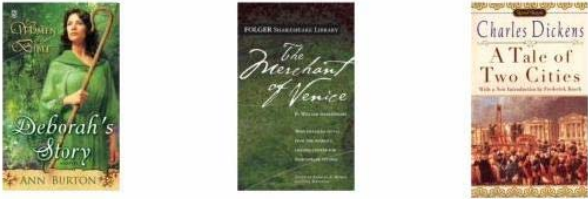
Vse zgoraj našteje oblike uporabljanja ne predstavljajo neposredne grožnje zasebnosti, so pa vse neka oblika nadziranja uporabnikov interneta. Bolj vsiljiv način uporabe spletnih hroščev vključuje zajem IP naslova spletnega obiskovalca ali namestitve škodljivih datotek na trdi disk njegovega osebne računalnika. Nevarnost je predvsem ta, da lahko postane s spletnim hroščem računalnik obiskovalca povsem izpostavljen zlonamernim spletnim stranem, ki lahko vzamejo katero koli datoteko ali informacijo iz programov na njegovem trdem disku, in to brez vednosti ali privolitve. Neko poročilo navaja, da kar 16 od 51 milijonov pregledanih spletnih strani vsebuje najmanj enega spletnega hrošča, ki je bil pripet s strani tretjih oseb, kot so oglaševalske mreže. Kadar so spletni hrošči uporabljeni zlonamerno, se lahko na uporabnikovem računalniku ukrade tudi celotni seznam e-naslovov in to že samo s klikanjem po spletni strani, ki vsebuje spletne hrošče (Chung, Paynter, 25. 3. 2007). Poleg tega so ti še posebej problematični v primerih, ko so nameščeni v pisarniških datotekah, ki omogočajo neposredno pripojitev slik s spletnih strani. Ob vsakem odprtju posamezne datoteke se pri tem ponovno naloži tudi slika, kar omogoča spletnemu hrošču sledenje njene uporabe in gibanja. Enako velja za e-pošto, saj pošiljatelji nezaželene pošte (SPAM) z njimi preverjajo veljavnost obstoječega naslova za kasnejše pošiljanje, lahko pa se uporabljajo tudi za ugotavljanje, ali je posameznik prebral sporočilo.

Uporabniški računi in spletni obrazci

Enega izmed najbolj podrobnih in škodljivih virov osebnih informacij na internetu predstavljajo uporabniki sami, saj ti posredujejo ogromne količine informacij ob ustvarjanju uporabniškega računa ali ob izpolnjevanju spletnih obrazcev v zameno za brezplačne storitve oziroma ugodnosti (npr. pridobitev e-poštnega naslova, popusta, nagrade itd.).

Nekatere spletne strani omogočajo ustvarjanje uporabniškega računa. Ta se pogosto uporablja, kadar mora uporabnik dostopiti do preteklih informacij ali zbranih podatkov (npr. na spletnih straneh e-trgovine). Pri ustvarjanju uporabniškega računa mora uporabnik običajno podati svoje osnovne kontaktne informacije, preference, včasih pa tudi informacije o kreditni kartici (Slika 13). Veliko spletnih strani pogosto zbira in vzdržuje zgodovino uporabe, naročanja, podatke o klikih in osebne informacije, kar je običajno potrebno za dokončanje uporabnikove transakcije ali zahtevka. Med drugim informacije o preferencah uporabnikov prav tako pomagajo spletnim stranem pri določanju, katere ponudbe so za njih zanimive in uporabne, in katere niso (Privacy Online: OECD Guidance on Policy and Practise, 2003, str. 250).

Slika 13: Registracijsko okno spletne strani



DOMOV/Registracijska stran

Registracijska stran

Ime	
Preimek	
Naslov 1	
Naslov 2	
Mesto	
Država	State
Poštna številka	
Telefonska	
Fax	
E-pošta	
Geslo	
	Pošlji

Vir: [URL:<http://www.kevacorp.com/NewCustomer.asp>], 23. 2. 2007

Spletni obrazci so druga običajna metoda zbiranja osebnih informacij. Ti se lahko uporabijo na nešteto načinov – od zbiranja podatkov o uporabniku, ki je zahteval dodatne informacije o produktu ali storitvi podjetja, do sodelovanja pri spletnih anketah. V veliko primerih registracija ni zahtevana za uporabo spletne strani ali za spletno naročilo, vendar pa dodatne storitve neregistriranim uporabnikom ponavadi niso na voljo (npr. spremljanje statusa pošiljke, shranitev domačega naslova za prihodnjo uporabo itd.). Najverjetneje bodo morali ti tudi večkrat vtipkati najpomembnejše informacije, ne bodo mogli pregledovati iskalnih in

nakupovalnih navad ali spremeniti svojih spletnih preferenc. Izbira je povsem odvisna od njih samih.

Trenutno obstaja v ZDA zelo malo omejitev pri tem, kaj lahko spletne strani naredijo z osebnimi informacijami, ko so te enkrat zbrane. Medtem, ko so nekateri trgovci objavili politiko zasebnosti na svojih spletnih straneh (opredelila naj bi zbiranje in uporabo informacij), je objava le te še vedno prostovoljna. Številne druge države imajo sicer sprejeta strožja pravila kaj, se lahko naredi z osebnimi informacijami in česar ne, vendar so bile te na drugi strani zelo počasne pri širitvi pravnega reda na področje interneta (Garfinkel, Spafford, 2002, str. 209).

Nezaželena e-pošta

E-pošta kot nujno in cenjeno orodje poslovanja podjetij/organizacij ter posameznikov postaja vse bolj ogrožena zaradi invazije nezaželene e-pošte (SPAM) v uporabnikov poštni nabiralnik in škodovanju IT sistemom. SPAM je poznan pod različnimi imeni, kot sta nenaročena masovna e-pošta (UBE) ali nenaročena komercialna e-pošta (UCE). Na splošno je sprejeto, da mora SPAM doseči tri glavne kriterije: mora biti »nezaželen«, mora biti »komercialen« po naravi in mora biti poslan »masovno«. Skrb zbujajoči so podatki, ki govorijo da kar 80 % vseh e-sporočil predstavlja SPAM in da se ta delež še povečuje. Dnevna količina poslane »junk« e-pošte po vsem svetu je v letu 2004 znašala okoli 58 milijonov, kar je za poslovanje predstavljalo okoli 198 milijard dolarjev stroškov na letni ravni zaradi nakupov programske opreme za varovanje ter izgubljene produktivnosti. Nenazadnje zaradi SPAM-a kar 63 % uporabnikov e-pošte v ZDA vse manj zaupa temu orodju.

Poročilo Gartner navaja štiri različice nezaželene e-pošte (SPAM), ki so prikazane v nadaljevanju (Slika 14) (Thorson, Sedore, 2. 3. 2007):

- Čiste spam smeti (*fraudulent schemes*),
- Verižna pisma (*chain letters*),
- Ljudje, ki prodajajo za zaslužek (*junk mail*),
- Spam s strani kolegov (*occupational SPAM*).

Slika 14: Različice nezaželene e-pošte (SPAM)

Čiste spam smeti

Spoštovani,

Sem Maryam Spammer, vdova nekdanjega generala v Nigeriji, ki je umrl takoj po aretaciji 8. junija 1998. Država Nigerija nam je po revoluciji zasegla vse premoženje, razen 30.000.000 \$ katere je pokojni pred smrtjo položil na skrivni zasebni račun.

Naša družina nujno potrebuje omerjeni denar, da bo lahko začela novo življenje, vendar smo še vedno pod stalnim državnim nadzorom.

Zato potrebujemo nekoga, kateremu bi lahko zaupali certifikat depozita in (PIN) in kateri bi nam pomagal prenesti sredstva iz zasebnega podjetja izven naše države.

Če je ta ponudba za vas sprejemljiva, vam bo naša družina po prenosu sredstev na vaš tekoči račun odstopila 30 % od skupne vrednosti, kot zahvala za vašo pomoč.

Zaradi občutljivosti, vas prosim za strogo zaupnost. Lahko me kontaktirate po e-pošti ali pokličete na spodnji telefon. Nadaljnje informacije bodo sledile kmalu.

Hvala, čakam na vaš odgovor.

Maryam Spammer TEL: xxx - x - 7763xxx

Verižna pisma

Pozdravljeni, zahvaljujem se vam za vaše zanimanje za testno verzijo aplikacije, ki je namenjena sledenju e-pošte. Moje ime je Bill Gates. Na Microsoftu smo izpopolnili program, kateri bo sledil vsem, ki bodo prejeli to sporočilo.

Trenutno preizkušamo delovanje tega programa in zato potrebujemo tudi vašo pomoč. Prosim, da posredujete to sporočilo vsem, ki jih poznate in če boste poslali 1000 ljudem ali več, boste prejeli 1000 \$ in kopijo operacijskega sistema Windows 98.

Uživajte.

Vаш prijatelj, Bill Gates & Razvojni oddelek Microsoft.

Ljudje, ki prodajajo za zaslužek

Ponujamo BREZPLAČNO odobritev kredita na hipoteko ali za stanovanjske obnove.

Obresti so sedaj najnižje v zadnjih nekaj letih, zato kliknite nemudoma na spodnjo povezavo za BREZPLAČNO odobritev.

<http://www.ACA-Agency.com>

Spam s strani kolegov

(Zelo bi bil hvaležen, če bi posredovali to informacijo vsem članom znotraj Maxwell šole in pridruženim fakultetam --- Hvala.)

Sem mladi raziskovalec na področju Shakespeare literature in antične Grčije ter avtor številnih knjig na omenjeno temo.

V nadaljevanju sledi krajši opis štirih mojih knjig o antični Grčiji, ki so nekoliko drugačne in vam bodo mogoče tudi izredno zanimive.

.....

Vir: Thorson, Sedore, 2. 3. 2007

Na vprašanje, ali SPAM ogroža posameznikovo zasebnost, obstaja kar nekaj pritrdilnih argumentov. Prvi pravi, da SPAM krati ustavno pravico prejemnika do zadovoljstva in zasebnosti. Drugi argument ga razume kot neko obliko napada na zasebnost, saj vdira na zasebno področje. Tretji pa zbiranje in uporabo e-poštnih naslovov za pošiljanje SPAM-a razume ne samo kot kršenje zasebnosti na internetu, ampak tudi kot kršenje lastninskih pravic (Chul Huh, 6. 2. 2007).

Najbolj običajni načini pridobivanja e-poštnih naslovov uporabnikov interneta, ki se jih poslužujejo pošiljatelji SPAM-a so (Spam: What to Do about Junk E-Mail, 17. 5. 2005):

- nakup seznama elektronskih naslovov,
- uporaba programov za zbiranje elektronski naslovov s spletnih strani, novičarskih skupin, govorilnic itd.,
- pridobitev s soglasjem uporabnika ali brez ob obisku njihove spletne strani,
- kopiranje s spletnih »belih strani« imenikov,
- naključno ustvarjanje (uporaba zmogljivih računalnikov za ugibanje vseh možnosti za določeno domeno, na primer @snc.edu ali @aol.com).

Poleg problemov, ki jih povzroča uporabnikom e-pošte, predstavlja SPAM tudi resno grožnjo računalniški varnosti kot prenašalec virusov, črvov in vir za številne prevare. Veliko pošiljateljev SPAM-a uporablja metodi, kot sta lažno predstavljanje (*phishing*) in pridobivanje podatkov (*spoofing*) s ciljem kraje osebnih informacij in finančnega premoženja prejemniku e-pošte. Ti ustvarijo e-pošto, ki izgleda tako, kot da je prišla iz legitimnega in zaupanja vrednega vira (npr. prejemnikova banka ali e-trgovec). Pošiljateljev elektronski naslov je pri tem prirejen, SPAM sporočilo pa pogosto vsebuje povezavo na podobno spletno stran z namenom prevarati prejemnika, da poda številko kreditne kartice, uporabniško geslo, številko zavarovanja in podobne osebne informacije, ki se lahko kasneje uporabijo za krajo identitete ter vključitev v druge nelegalne aktivnosti (SPAM 2005, 2005, str. 15).

Spyware

Spyware je skupno ime za razred programov, ki se samodejno namestijo na uporabnikov računalnik, spremljajo njegove aktivnosti in o tem poročajo tretjim osebam za komercialne ali osebne namene. Spyware je dejansko program, ki prevzame nadzor nad uporabnikovim računalnikom brez njegove vednosti.

Spyware vključuje naslednje oblike (Stafford F., Urbaczewski, 2004, str. 292):

- oglaševanje (*Adware*),
- beleženje udarcev na tipkovnici (*Key Loggers*),
- trojanske konje (*Trojan Horses*).

Te aplikacije v najboljši možni meri izkoristijo računalniške vire, pasovno širino in lahko v najslabšem primeru pripeljejo do resnih varnostnih problemov v uporabnikovem računalniku. Čeprav so nekateri mnenja, da so spyware aplikacije še vedno dokaj nedolžne, lahko pričakujemo, da bodo kmalu postale glavno orodje za krajo identitete in kreditnih kartic ter pridobivanje gesel.

Oglaševanje

Aplikacije, ki so kategorizirane kot oglaševalske, opravljajo veliko različnih funkcij:

- Spremljajo uporabnikove spletne aktivnosti in glede na to pošiljajo ciljno oglaševanje na njegov zaslon.
- Spremenijo lahko delovanje uporabnikovega spletnega brskalnika z namestitvijo »brskalnikovih predmetov«.
- Spremenijo lahko osnovne nastavitve spletnega brskalnika, da prikazuje različne spletne strani in sezname ter preusmerijo iskanja na različne iskalne sisteme.

Veliko teh oddaljenih aplikacij za nadzorovanje je s strani njihovih lastnikov opredeljenih kot legitimno sredstvo za poslovno rabo, namenjeno potrebam neposrednega pop-up oglaševanja končnim uporabnikom glede na njihove spletne in iskalne aktivnosti.

Beleženje udarcev na tipkovnici

Programi za nadzorovanje uporabnikov so obstajali v številnih oblikah že pred dobo osebnega računalništva in so omogočali zajem informacij, kot so identitete in gesla. Nekateri sistemi za beleženje so označeni kot legitimno orodje za sledenje zaposlenih ali družinskih članov, vendar poleg teh obstajajo še druge zelo pogoste in ogrožajoče oblike. Razlogi za spremljanje aktivnosti izhajajo iz upravičenih skrbi staršev in delodajalcev glede primerne uporabe interneta pa do visoko nelegalnih dejanj, kot so kraje identitet ali namensko vohunjenje.

Beleženje udarcev na tipkovnici prav tako uporabljajo hekerji za zajem gesel in pretihotapljenje v ciljna omrežja. Pogosto je to sestavni del napada trojanskega konja. Beleženje udarcev lahko nenazadnje prevzamejo tudi mehanične naprave, ki so nameščene na računalniško tipkovnico.

Oddaljeni administrativni trojani

Napad trojanskega konja tipično vključuje namestitev programa (ponavadi z brezplačnimi igricami ali »peer-to-peer« programi), ki je lahko kontaktiran s strani zunanjega računalnika in kateri omogoča nadzor nad gostiteljevim računalnikom. Oznaka za ta razred spywara je RAT. Njihove grožnje segajo od klicnega programa, ki

zaposli uporabnikov modem, da kliče drago zunanjo številko (090), pa do bolj prefinjene modifikacije mrežnih administrativnih orodij, ki izkoristijo varnostne luknje v operacijskem sistemu in tako omogočijo zunanjim uporabnikom zajem slike na zaslonu in vtipkanih podatkov, ali pa dejansko prevzamejo nadzor nad oddaljenim računalnikom.

Te oddaljene administrativne oblike spywara so nedvoumno zlonamerne, čeprav je oddaljeno administriranje ena izmed mnogih tehnik, ki jih uporabljajo administratorji za spremljanje in kontroliranje omrežja, za katerega so odgovorni. Tipičen primer RAT-a so škodljive nevronske vsebine, ki pridejo kot priloga e-pošte ali ob namestitvi programov. RAT napadajo z izkoriščanjem pomanjkljivosti spletnega brskalnika ali operacijskega sistema za svojo namestitvev in kasnejšo sprožitev namestitve orodij, ki nadzorujejo ciljni računalnik za zlonamerne namene. Ti segajo od milejših oblik, kot je preusmeritev na druge spletne strani, pa do hujših oblik, kot je ustvarjanje in prenašanje SPAM pošte.

4 PRISTOPI IN TEHNOLOGIJE ZA VAROVANJE ZASEBNOSTI

Tudi če so osebne informacije fizično nadzirane s strani posameznika ali prepuščene tretjim osebam, ki jim zaupamo (npr. zaupni centri, poslovni partnerji in institucije itd.), bo varovanje pogosto zahtevalo elektronska orodja, ki nadzirajo dostop do informacij in njihovo uporabo glede na posameznikove odločitve. Razvita je bila široka paleta orodij in tehnologij za podprtje zasebnosti v elektronskih rešitvah, od katerih se jih večina nanaša na internetno zasnovane komunikacije in transakcije. Namen teh tehnologij za varovanje zasebnosti (PET) je varovati zasebnost posameznikov, pri čemer jim še vedno omogočajo interakcijo z drugimi udeleženci v sodobni družbi, uporabljajoč elektronske komunikacije (Privacy Enhancing Technologies, 2005, str. 8). Kljub dejstvu, da nekatera podjetja na široko uporabljajo tehnologijo za izvajanje invazijskih praks na zasebnost, lahko ta odigra pomembno vlogo pri varovanju zasebnosti, še posebej zaradi možnosti prečkanja mednarodnih, političnih, regulativnih in poslovnih pregrad, podobno, kot to velja za internet (Tuner C., Dasgupta, 2003, str. 13). Nenazadnje lahko posamezniki varujejo svojo zasebnost tudi z uporabo že uveljavljenih pristopov v internetnih aplikacijah v okolju oken, s katerimi lahko odpravijo določene slabosti v njihovi zasnovi in tako izboljšajo zasebnost.

4.1 Pristopi za varovanje zasebnosti v okolju oken

Spletni brskalnik Internet Explorer vsebuje mnogo vstavljenih funkcionalnosti, kar ga naredi zelo kompleksnega in s tem nagnjenega k implementacijskim napakam. V zadnjih nekaj letih so tako v tem produktu skoraj vsak mesec odkrili številne varnostne pomanjkljivosti, od katerih jih je bilo veliko izkoriščenih s strani zlonamernih spletnih strani, e-sporočil ali avtomatskih črvov. Poštni odjemalec Outlook Express in nekateri drugi programi uporabljajo komponente Internet Explorer-ja za procesiranje HTML e-sporočil, zaradi česar se veliko

njegovih pomanjkljivosti neposredno odraža tudi pri njih (Internet Explorer Safety, 3. 4. 2007). Kadar se izkoristi določeno pomanjkljivost produkta, se pri tem pogosto zaobide notranjo kontrolo varnosti. V takih primerih uporabnik postane žrtev, ne da bi bil posebno aktiven, saj zadostuje že samo branje škodljive e-pošte, klik na zlonamerno spletno povezavo ali obisk zlonamerne spletne strani, da se nadzor nad računalnikom in vseh njegovih podatkov prenese na virus ali tretjo osebo (torej ni treba klikniti nobene priloge ali prenesti nobene datoteke s spletne strani).

Spletni brskalnik (Microsoft Internet Explorer 6.0)

Tako kot vsi drugi široko uporabljeni programski produkti je tudi spletni brskalnik postal običajna tarča za ljudi, ki želijo zmotiti poslovne ali druge vrste procesov. Najbolj so v uporabi naslednje vrste napadov (Desktop Application Security Tehnical Implementation Guide, 2006, str. 19):

- Podatki, spletne strani in datoteke, poslane spletnemu brskalniku, lahko vsebujejo mobilne kode, ki lahko poškodujejo tako uporabnikove kot tudi systemske datoteke na osebem računalniku. Obseg škode lahko sega od enostavnih motenj do spremembe in stalne izgube podatkov.
- Podatki, spletne strani in datoteke, poslane spletnemu brskalniku lahko vsebujejo mobilne kode, ki lahko povzročijo odkritje shranjenih podatkov na uporabnikovem računalniku ali oslabijo varnost tako, da so lahko drugi poskusi za pridobitev podatkov uspešni. Škodljive mobilne kode lahko zbirajo podatke, gesla in druge občutljive informacije ter jih pošiljajo oddaljenemu strežniku.
- Podatki, spletne strani in datoteke, poslane spletnemu brskalniku, lahko vsebujejo mobilne kode, ki lahko sprožijo neko vrsto napada na druge uporabnike in strežnike s propagiranjem škodljivih kod ali ustvarjanjem pogojev, katerih rezultat je zavrnitev storitve (DoS).

Pravilno nastavljanje in uporaba preverjenih programov lahko naredi Internet Explorer prav tako varen kot kateri koli drugi spletni brskalnik na trgu. Pri njegovem nastavljanju je poudarek na ravno pravšnji nastavitvi, ki ustreza potrebam uporabnika po varnosti in zasebnosti, in uravnovešenosti z enostavnostjo uporabe glede na dosedanje navade. Sam uporabnik se mora tudi odločiti, kolikšno tveganje je pripravljen sprejeti, da bi si lahko ogledoval številne spletne vsebine. Povedano drugače, prisiljen je izbrati med povečanjem varnosti in zasebnosti na spletu ali zmanjšanjem dostopa do določenih vsebin (Configuring Internet Explorer for Practical Security and Privacy – Part 1, 12. 2. 2007).

Spodaj predstavljeni načini bodo bistveno zmanjšali tveganja, vendar ne bodo odpravili vseh groženj.

Vsakokrat ko poskuša spletni brskalnik zajeti URL naslov na internetu, najprej pogleda v svoj pomnilnik, če ima kopijo informacije, ki naj bi se prenesla. S tem se lahko bistveno poveča hitrost spletnega brskanja, saj v primeru klikanja na spletni strani z veliko gumbi zadostuje že enkratno nalaganje posameznega gumba kljub možnosti, da se gumbi pojavijo na več straneh. Vendar je pri tem treba opozoriti, da če pridobi dostop do računalnika tretja oseba, ji bo ta omogočil kopije vseh spletnih strani, ki jih je obiskala predhodna oseba. Obstajajo številni načini za zmanjšanja vpliva na zasebnost v brskalnikovem pomnilniku (Garfinkel, Spafford, 2002, str. 242):

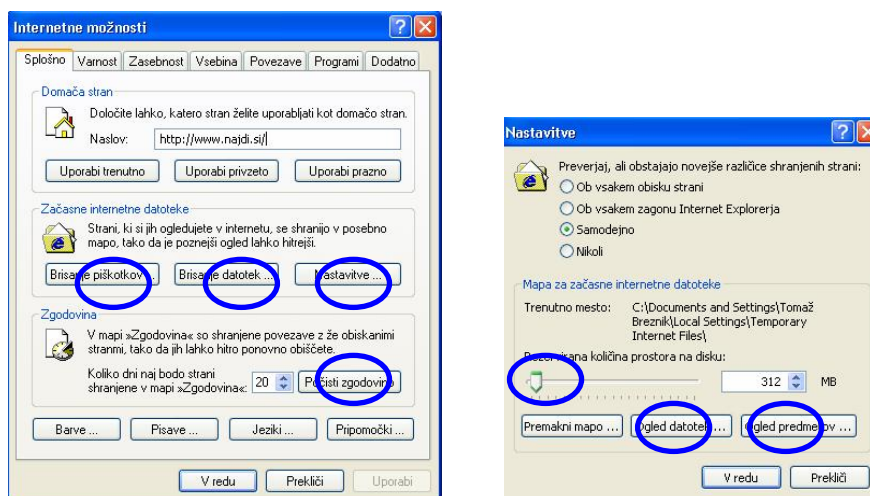
- Običajno lahko brskalnik nastavimo tako, da se spletne strani in slike, naložene s protokolom SSL, ne zabeležijo na trdem disku. Na ta način se zaupne informacije kot so izjave bankam in številke kreditnih kartic ne shranjujejo lokalno. To je upoštevano že v privzetih nastavitvah pri večini spletnih brskalnikov.
- Brskalnik lahko nastavimo tako, da se tudi ostale spletne strani in slike ne zabeležijo na trdem disku. Ta pristop daje sicer največjo možno stopnjo varovanja, vendar na drugi strani znatno zmanjša zmogljivost brskalnika.
- Ročno izbrišemo informacije v brskalnikovem pomnilniku, potem ko zapustimo še posebej občutljivo spletno stran. Alternativno lahko pregledamo brskalnikov pomnilnik in od tam izbrišemo občutljiv material.

Uporabnik lahko upravlja s pomnilnikom Internet Explorer-ja s pomočjo menija »Orodja«, kjer izbere »Internetne možnosti« in nato zavihek »Splošno« (Slika 15). S klikom na gumb »Brisanje datotek« se bo sprožilo brisanje vseh shranjenih datotek, s klikom na gumb »Brisanje piškotkov« pa brisanje vseh shranjenih spletnih piškotkov znotraj mape za začasne datoteke. Uporabnik lahko alternativno klikne tudi na gumb »Nastavitve« in nato gumb »Ogled datotek«, da se odpre mapa za začasne datoteke, in od tam izbriše datoteke. Poleg teh datotek lahko naloži Internet Explorer od spletnih strani tudi izvršilne kode v obliki ActiveX komponent. Uporabnik si jih lahko ogleda s klikom na gumb »Ogled predmetov« in jih od tu tudi izbriše, če ne želi imeti teh pripomočkov na svojem računalniku. Ob morebitnem obisku spletne strani, ki bi te kode zahtevala, jih lahko ta vedno znova namesti. Nenazadnje lahko uporabnik z drsnikom spreminja tudi količino prostora na trdem disku računalnika, ki je dodeljen za shranjevanje začasnih datotek.

Poleg pomnjenja naloženih spletnih strani in slik si večina spletnih brskalnikov zapomni vsak URL naslov, ki so ga uporabniki obiskali v zadnjih nekaj dneh. Brskalnik si zapomni te informacije z namenom, da lahko nudi uporabnikom podporo ob ponovnem vtipkavanju URL naslovov in sicer tako, da jim ta ob delnem URL naslovu ponudi seznam nedavno obiskanih. Ti lahko predstavljajo potencialno občutljive informacije še posebej v primerih, ko URL naslovi vsebujejo iskalne nize in imena uporabniških

računov. Uporabnik jih lahko vedno izbriše v zavihku »Splošno« s klikom na gumb »Počisti zgodovino«.

Slika 15: Nastavitve pomnilnika v spletnem brskalniku

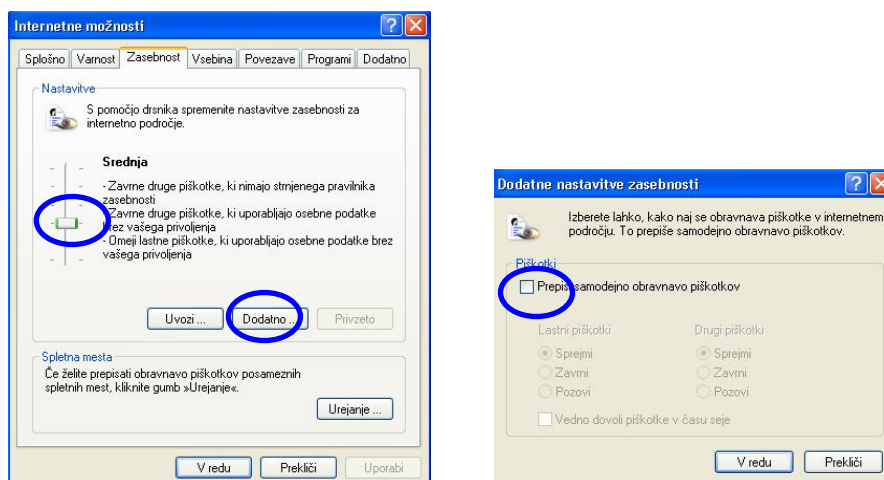


Vir: Internet Explorer 6.0

Zasebnost

Kot je bilo že predstavljeno, se lahko spletni piškotki uporabijo za številne namene, kot so podpora pri nudenju personaliziranih storitev, uporabi nakupovalnih kartic in sledenju aktivnostim uporabnika interneta. Spletni piškotki so zaradi tega tako močno orodje, da v kolikor bi imel nekdo dostop do njih, bi bilo mogoče ukrasti identiteto uporabnika ali pa vsaj izvedeti določene informacije o njem. Z vidika upravljanja s spletnimi piškotki lahko uporabnik s pomočjo zavihka »Zasebnost« z drsnikom spreminja stopnjo varovanja zasebnosti (na višjo ali nižjo), ki je v osnovi nastavljena na srednjo stopnjo. Alternativno lahko uporabnik klikne tudi na gumb »Dodatno«, kjer lahko prepíše samodejno upravljanje s spletnimi piškotki in si nato določi kriterije (Slika 16).

Slika 16: Nastavitve spletnih piškotkov v spletnem brskalniku

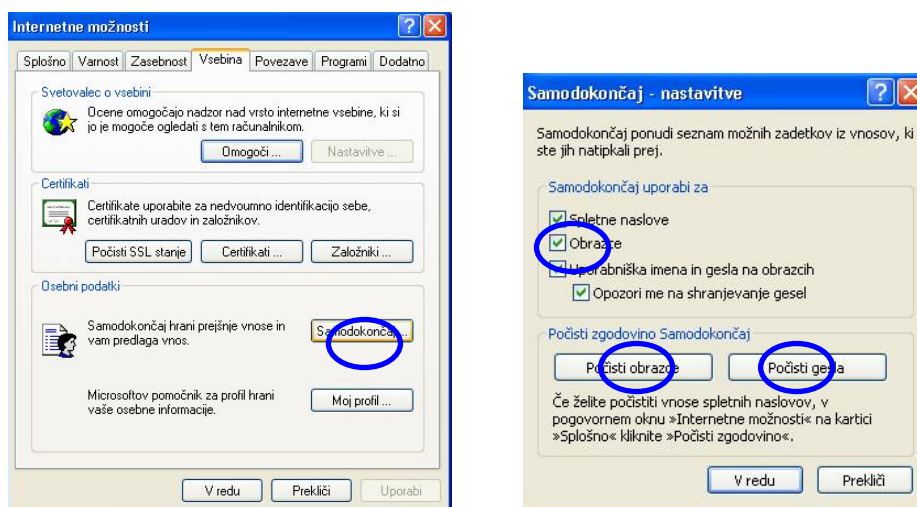


Vir: Internet Explorer 6.0

Gesla, izpolnjevanje obrazcev

Internet Explorer ima možnost pomnjenja vsega, kar uporabnik vtipka v spletne obrazce, med drugim tudi uporabniška imena in gesla, ki jih ta posreduje spletnim stranem. Program v svoji osnovi uporabniku že sam predlaga samovpisovanje, da mu s tem prihrani čas pred ponovnim vtipkavanjem. Čeprav je to zelo uporabno, se lahko tretjim osebam, ki uporabljajo isti računalnik, odkrijejo določene informacije o navadah predhodnega uporabnika. Uporabnik lahko to prepreči z nadziranjem pomnjenja in sicer s klikom na zavihek »Vsebina« ter na gumb »Samodokončaj«, kjer si nato znotraj novega okna določi, kaj naj si program zapomni oziroma ima možnost, da počisti zgodovino s pomočjo gumbov »Počisti obrazce« in »Počisti gesla« (Slika 17).

Slika 17: Nastavitve samovpisovanja v spletnem brskalniku

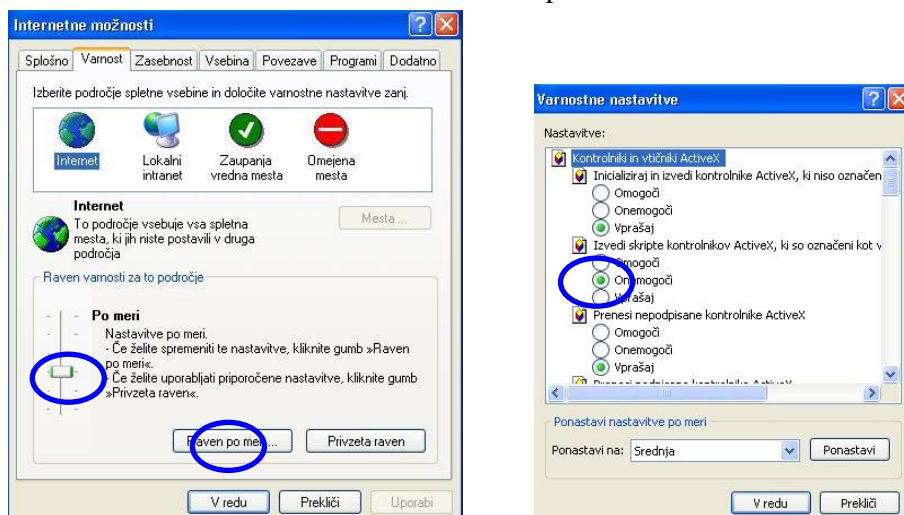


Vir: Internet Explorer 6.0

Varnost

Internet Explorer razvršča spletne strani v posamezne skupine zaradi svoje varnostne politike. Ko uporabnik obišče določeno spletno stran, se zanjo določi ustrezna cona iz parametrov Internet Explorer-ja (vsaka cona ima svoje varnostne nastavitve). Na splošno zagotavljajo te nastavitve nadzor nad funkcijami, ki so podprte v spletni vsebini (ActiveX kontrole, plug-ini, Java pripomočki, skripte, spletni piškotki itd.). Ker lahko ta vsebina vključuje tudi potencialno škodljive mobilne kode, so nastavitveni parametri zelo pomembni za varnost (Desktop Application Security Technical Implementation Guide, 2006, str. 73). V osnovi so varnostne nastavitve za internetno področje nastavljene na srednjo stopnjo, vendar jo lahko uporabnik v zavihku »Varnost« z drsnikom spreminja (na višjo ali nižjo). Alternativno lahko ta klikne tudi na gumb »Raven po meri«, kjer si nato določi varnostne kriterije (Slika 18).

Slika 18: Nastavitve varnosti v spletnem brskalniku



Vir: Internet Explorer 6.0

Poštni odjemalec (Outlook Express 6.0)

Outlook Express je s svojimi privzetimi nastavitvami prav tako (ne) varen kot Internet Explorer. Čeprav gre za dve povsem ločeni aplikaciji, sta ti zasnovani na enakih osnovnih komponentah (Securing your E-mail client – Outlook Express Part 1, 1. 2. 2007).

Zaradi pomembnosti e-pošte za poslovne ali druge vrste procesov so se pojavile številne oblike napadov (Desktop Application Security Tehnical Implementation Guide, 2006, str. 27):

- Podatki e-sporočila so lahko razviti tako, da povzročijo zmanjšano funkcionalnost uporabnikove programske opreme.
- Podatki e-sporočila lahko vsebujejo mobilne kode, ki lahko izbrišejo uporabnikove ali sistemske datoteke, jih spremenijo ali posredujejo podatke ter občutljive informacije oddaljenim strežnikom.
- Podatki e-sporočila lahko vsebujejo mobilno kodo, ki namerava sprožiti neko vrsto napada na druge uporabnike ali strežnike s propagiranjem škodljivih kod ali z ustvarjanjem pogojev, katerih rezultat je zavrnitev storitve (DoS).

Danes je najobičajnejša oblika napada s prilogami e-sporočilom. Te lahko vsebujejo samostojne programe ali skriptne ukaze, vendar škoda ponavadi ne nastane, dokler se teh prilog ne odpre, s čimer se sproži zlonamerna koda.

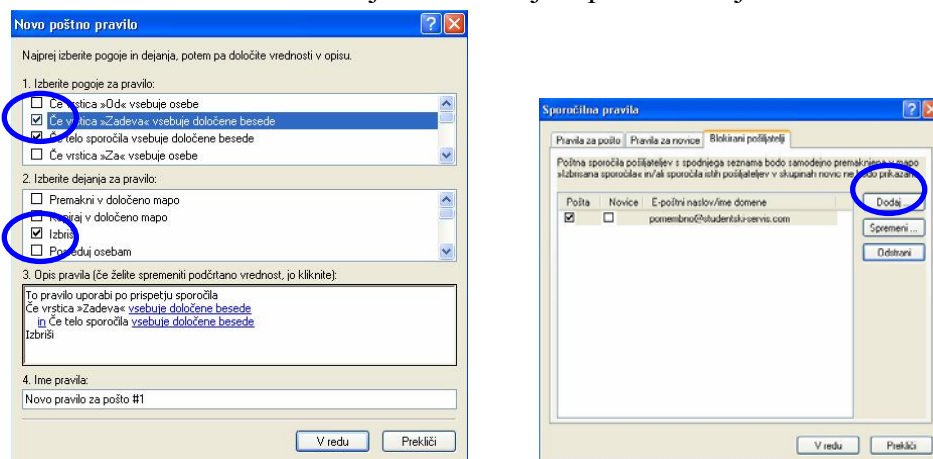
Spodaj predstavljeni načini bodo bistveno zmanjšali tveganja, vendar ne bodo odpravili vseh groženj.

Filtriranje in blokiranje

Outlook Express vključuje nekatere načine za obvladovanje nezaželene e-pošte (SPAM) (Outlook Express 6, 10. 8. 2004). Prva možnost so poštna pravila, ki opravljajo različne aktivnosti, kot so premikanje ali brisanje e-sporočil glede na nastavljene kriterije.

Uporaba poštnih pravil za nadziranje je težavno, saj pošiljatelji SPAM-a zelo pogosto spreminjajo vsebino sporočil, zato je lahko to le začasna rešitev. Uporabnik lahko nastavi poštna pravila s pomočjo menija »Orodja«, kjer izbere »Sporočilna pravila« in nato »Pošta« (Slika 19). Druga možnost je blokiranje e-sporočil določenega pošiljatelja ali spletnega naslova. Uporabnik lahko to stori s klikom na »Seznam blokiranih pošiljateljev«, kjer nato vpiše e-naslove, vendar tudi ta način ni posebej učinkovit, saj lahko SPAM prihaja iz istega vira, medtem ko se e-naslovi neprestano spreminjajo.

Slika 19: Nastavitve blokiranja in filtriranja v poštnem odjemalcu

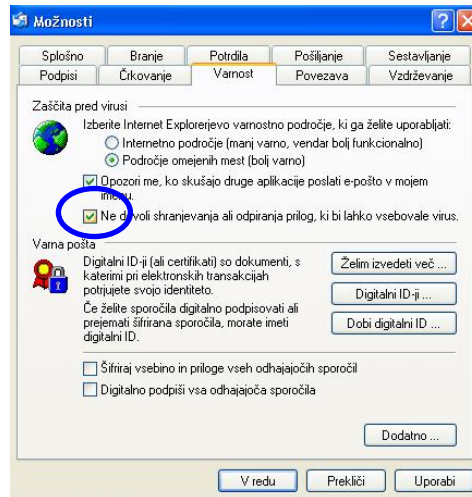


Vir: Outlook Express 6.0

Varnost

Outlook Express uporablja prednosti Internet Explorer varnostne cone za zavarovanje pred škodljivimi kodami (npr. ActiveX kontrole, Java, skripte itd.), ki so lahko vstavljene v telo besedila e-sporočila. V svoji osnovi je že nastavljen na področje omejenih mest, ki je bolj varno od internetnega področja, vendar so ta na drugi strani zelo konzervativna. Obstaja tudi možnost, ki ne dovoli odpiranja ali shranjevanja prilog, ki bi lahko vsebovale viruse, vendar ta v osnovi ni izbrana. Uporabnik lahko to spremeni s pomočjo Outlook Express menija »Orodja«, kjer izbere možnost »Možnosti« in nato zavihek »Varnost«, v katerem to aktivira (Slika 20). Pri tem se je treba zavedati, da se s tem prepove dostop do veliko drugih datotek, med njimi tudi do tistih, ki so definirane znotraj nastavitve »potrdi odprtje po prenosu«, kar pa ni vedno povsem zaželeno (Pitsenbarger, Bartock, 2004, str. 14–17).

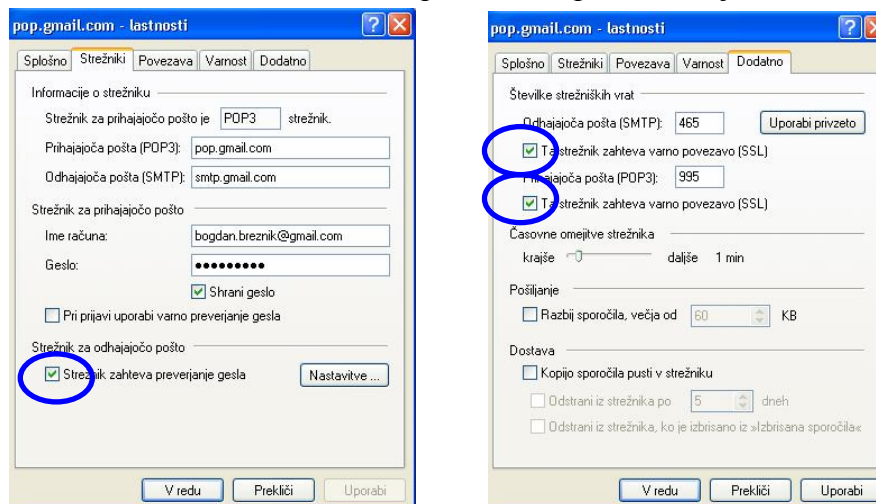
Slika 20: Nastavitve varnosti v poštnem odjemalcu



Vir: Outlook Express 6.0

Varna poveza v osnovni nastavitvi Outlook Express-a prav tako ni omogočena, kar danes predstavlja zelo veliko grožnjo zaradi vse bolj dostopnih tehnologij za nadzorovanje. Uporabnik lahko spremeni obstoječo komunikacijo s poštnim strežnikom tako, da ta poteka šifrirano (SSL), s čimer zavaruje vsebino e-sporočila in gesla. To stori s pomočjo menija »Orodja«, kjer izbere »Računi« in nato »Lastnosti« ter zavihka »Strežniki« in »Dodatno«, v katerih aktivira zahtevo za preverjanje gesla in varno povezavo (Slika 21).

Slika 21: Nastavitve varne povezave v poštnem odjemalcu



Vir: Outlook Express 6.0

Podjetje Microsoft, ki je lastnik programa Internet Explorer, je zaradi njegove široke uporabe ter zgodovine številnih varnostnih incidentov uvedlo svojo vzdrževalno politiko, ki vključuje storitvene pakete in dodatne programe. Storitveni paketi ponavadi vključujejo vzdrževanje, ki rešuje vprašanja varnosti, medtem ko so programi posredovani po potrebi za individualno popravilo problemov. Varnostne lastnosti in inovacije z naprednimi tehnologijami v storitvenem paketu za okna XP (XP SP2) pomagajo uporabnikom, da s pro-aktivnim pristopom izboljšajo varovanje računalnika, informacij ter zasebnosti. Te varnostne izboljšave

so razširjene tako na program Internet Explorer 6.0 kot tudi Outlook Express 6.0 in dajejo uporabnikom povsem nov, enostaven način za boljše varovanje računalnika, medtem ko navigirajo po spletu ali uporabljajo e-pošto (Windows XP Service Pack 2: Technologies Overview, 4. 8. 2004). Uporabnik lahko opravi spletno posodobitev omenjenih internetnih aplikacij v okolju oken s pomočjo menija »Zaženi«, kjer izbere možnost »Posodobi okna« oziroma s pomočjo uradne spletne strani podjetja Microsoft.

Izboljšave za Internet Explorer 6.0 v XP SP2 lahko pomagajo, da:

- naredijo brskanje bolj prijetno z bistvenim zmanjšanjem pop-up oglasov,
- nudijo boljše varovanje pred potencialno škodljivimi prenosi,
- ustavijo skripte, ki spremenijo velikost ali prestavijo okna brez uporabnikovega dovoljenja,
- nudijo močnejšo varnost za uporabnikov računalnik in sicer z vgrajenimi varnostnimi rešitvami.

Izboljšave za Outlook Express 6.0 v XP SP2 lahko pomagajo, da:

- zatrejo nevarne priloge v e-pošti, ki bi lahko potencialno širile viruse,
- blokirajo nekatere slike, ki bi lahko pošiljateljem SPAM-a potrdile uporabnikov e-poštni naslov,
- berejo e-sporočila samo v tekstovnem formatu.

4.2 Tehnologije za varovanje zasebnosti

Izraz tehnologije za varovanje zasebnosti (PET) predstavlja spekter tako novih kot že uveljavljenih tehnik za zmanjševanje izpostavljenosti osebnih podatkov, in so namenjene uporabnikom e-storitev v informacijski družbi. Vendar ta izraz še nima široko sprejete definicije, glavni cilj teh tehnologij pa je pogosto odvisen od namena uporabe (Privacy Enhancing Technologies, 2005, str. 5). Nekatera izmed orodij so aktivno udeležena pri shranjevanju in prenosu informacij, medtem ko druga podpirajo administracijo zasebnosti.

Lorrie Cranor navaja, da opravljajo tehnologije za varovanje zasebnosti mnogo funkcij med katerimi so (Cranor Faith, 2003, str. 80):

- preprečevanje neavtoriziranega dostopa do komunikacij in shranjenih datotek;
- samodejno pridobivanje informacij o praksah zasebnosti zbiralcev podatkov ter samodejno odločanje v imenu uporabnika na podlagi teh praks;
- samodejno nadziranje praks zasebnosti zbiralcev podatkov;
- filtriranje nezaželenih e-sporočil;
- preprečevanje samodejnega zajema podatkov s pomočjo spletnih piškotkov, http glav, spletnih hroščov, spywera itd.;
- preprečevanje povezovanja komunikacije z določenim posameznikom in;
- pospeševanje transakcij, ki v najmanjši možni meri odkrivajo osebne informacije.

4.2.1 Razvrstitev

Razvrstitve tehnologij za varovanje zasebnosti na internetu so različne in se razlikujejo glede na vir in namembnost gradiva. Številne tehnologije in principi za varovanje zasebnosti se med seboj prepletajo, zaradi česar je zelo težko kategorizirati prav določeno skupino tehnologij. Borka Blažič jih je zato razdelila v skupine glede na njihovo funkcionalnost in uporabnost (Jerman Blažič, 2005a, str. 228–229):

- ***Tehnologije varovanja na osebni ravni;*** varovanje zasebnosti uporabnika sloni na uporabi rešitev za varovanje zasebnosti, ki so pod nadzorom uporabnika in so ponavadi prisotne na njegovem osebem računalniku. Kdaj, kako in v kakšni meri bo uporabnik uporabil določeno rešitev, pa je odvisno od njegove osebne odločitve. V to skupino lahko uvrstimo programe za šifriranje, kot je PGP, in programe za upravljanje s spletnimi piškotki, hrošči, spywarom itd.
- ***Tehnologije varovanja identitete;*** sistem varovanja identitete zahteva tudi uporabnikovo sodelovanje, vendar pa izvedba varovanja zasebnosti ni odvisna samo od njegove lastne vpletenosti v sistem. Varovanje je odvisno od celotnega sistema in od vseh vpletenih (npr. ponudniki internetnih storitev, administratorji, izdelovalci spletnih strani itd.). Te tehnologije lahko razvrstimo kot tehnologije varovanja na sistemski ravni, med katere uvrščamo orodje Anonymizer, sistem LPWA, itd. Posebna vrsta teh sistemov so tehnologije varovanja z neizsledljivostjo, katerih namen je skrivanje akcij enega v akcijah mnogih. Te zagotavljajo, da so aktivnosti uporabnika nepovezljive z njegovo identiteto, zaradi česar je njegova identiteta neizsledljiva. V to skupino lahko uvrstimo sisteme, kot so Crowds, GUNet itd.
- ***Tehnologije varovanja s privolitvijo;*** tehnologija, ki jo lahko uvrstimo v to skupino, je P3P. Njena posebnost je v tem, da je odvisna od izdelovalcev oziroma lastnikov (npr. podjetij, organizacij itd.) spletnih strani in sistemov. Imenujemo jo lahko tudi tehnologija obveščanja o varovanju zasebnosti, saj ponuja uporabniku zgolj informacije (če spletni brskalnik podpira P3P) ali dodatne programe za branje dokumentov P3P XML, ne pa tudi anonimnih ter psevdonimnih storitev.

4.2.1.1 Tehnologije varovanja na osebni ravni

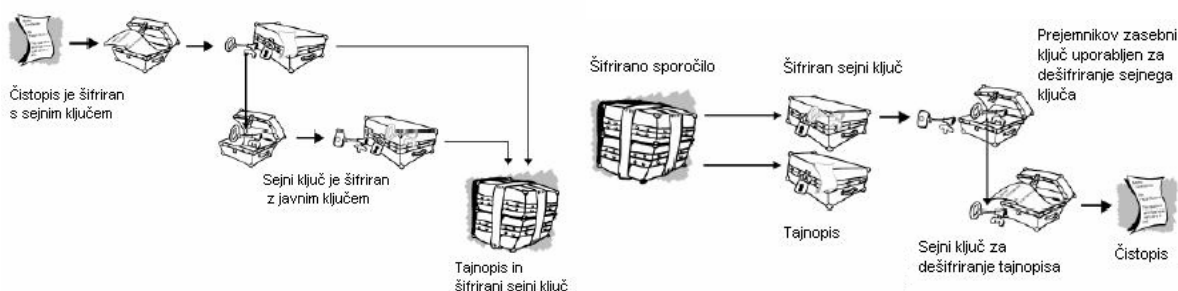
Kriptografija (PGP)

Kriptografija je znanost uporabljanja matematike za potrebe šifriranja in dešifriranja podatkov. Omogoča shranjevanje občutljivih informacij ali njihovo prenašanje preko nevarovanega omrežja, kot je internet, in sicer tako, da jih ne more prebrati nihče razen naslovljeni upravičenec. Kriptografski algoritem deluje v kombinaciji s ključem – beseda, številka ali fraza – da šifrira navadno besedilo. Varnost šifriranih podatkov je popolnoma odvisna od naslednjih dveh elementov: moči kriptografskega algoritma in tajnosti ključa.

Kriptografski algoritem in vsi možni ključki in protokoli sestavljajo kriptosistem (An Introduction to Cryptography, 2001, str. 12).

PGP je program za varovanje e-pošte (Slika 22), ki ga je napisal Phil Zimmermann in je zasnovan na osnovi IDEA algoritma za šifriranje navadnega besedila, za šifriranje zasebnega ključa pa uporablja RSA algoritem javnega ključa (Anand, 10. 1. 2007). Ta ima tudi določene omejitve in to je, da ne more rešiti vseh težav povezanih z računalniško varnostjo in zasebnostjo. Tako lahko zasledimo v njegovem priročniku kar nekaj groženj, ki se jih morajo uporabniki zavedati (Otterloo, 2001, str. 15).

Slika 22: Princip delovanje programa PGP (šifriranje in dešifriranje)



Vir: An Introduction to Cryptography, 2001, str.17–18

Čeprav napadalec ne more prebrati vsebine šifriranega e-sporočila, lahko z opazovanjem pridobi nekatere uporabne informacije in sicer, od kod je bilo sporočilo poslano, kam je bilo namenjeno, njegovo velikost ter kdaj je bilo poslano. Rešitev tega problema bo zahtevala snovanje posebnega komunikacijskega protokola za zmanjšanje izpostavljenosti analizi prometa, najverjetneje s pomočjo kriptografije. Druga oblika napada je oddaljeno odkrivanje elektromagnetnih signalov od uporabnikovega računalnika, s katerim se lahko zabeleži vse udarce na tipkovnici ali sporočila prikazana na zaslonu. Nekatere novejšje verzije PGP (6.0 ali kasnejša) že nudijo določeno rešitev tako, da prikažejo šifrirano besedilo s posebno oblikovanim stilom pisave, ki lahko zmanjšajo količino emisij radijskih frekvenc. Najhujše, kar se lahko zgodi, pa je razbitje PGP šifrirnega ključa s strani vladnih ali obveščevalnih služb, kar bi imelo nepredstavljive posledice.

Naslednji varnostni problem lahko izhaja iz načina delovanja operacijskega sistema. Ko uporabnik določeno datoteko šifrira in zatem izbriše originalno besedilo, njegov operacijski sistem fizično ne izbriše podatkov, ampak samo označi bloke trdega diska kot izbrisane, kar omogoča kasnejšo ponovno uporabo trdega diska. Morebitni napadalec bi lahko obnovil te datoteke z uporabo orodij za obnovitev stanja ali sistemskimi orodji. Edini način, da se prepreči obnovitev osnovnega besedila, je prepis izbrisanih datotek, kar je v novejših verzijah PGP (6.0 ali kasnejša) že omogočeno s pomočjo različnih dodatkov.

PGP prav tako nima nobene obrambe proti virusom, saj predvideva, da računalniško okolje deluje normalno. Virusi bi lahko bili razviti tako, da zajamejo geslo za dostopanje ali zasebni ključ, dešifrirajo sporočilo ter zapišejo te informacije v datoteko, ki jo nato pošljejo preko omrežja lastniku virusa. Obramba, ki je trenutno na voljo so predvsem komercialno dostopni

protivirusni produkti kot je Norton Antivirus. Možno nevarnost lahko predstavljajo tudi pametne različice PGP, ki se obnašajo kot tista prava, vendar ne delujejo tako, kot bi morale (npr. ne preverjajo pravilno podpisov, dovoljujejo sprejem certifikatov, ki vsebujejo spletne hrošče itd.). Te trojanske različice PGP napadalcem ni težko ustvariti, saj je izvorna koda pri starejših različicah široko dostopna in jo je precej enostavno spremeniti.

Upravljanje s spletnimi piškotki

Orodja za upravljanje s spletnimi piškotki, ki so vgrajena v spletne brskalnike, uporabnikom ponavadi ne zagotavljajo zadostnega nadzora nad prehodnimi in sprejetimi spletnimi piškotki. Za rešitev tega problema so se razvili številni brezplačni ali komercialni programi, ki jih lahko razdelimo v dve skupini: programi, ki imajo za svojo osnovno nalogo upravljanje s spletnimi piškotki (samostojni programi), ter programi, ki upravljajo s škodljivo vsebino na splošno vključujoč spletne piškotke (večnamenski programi) (Ha et al., 12. 10. 2005).

Trenutno so najbolj razširjeni samostojni programi. Nekateri nudijo uporabnikom samo splošne informacije o posredovanih spletnih piškotkih brez orodij za upravljanje z njimi, medtem ko jih drugi vprašajo, kaj narediti s posameznim spletnim piškotkom ter spletno stranjo (nudenje možnosti »sprejmi vse« ali »zavrni vse« za posamezno spletno stran). Za razliko od prehodnih programov je pri večnamenskih upravljanje s spletnimi piškotki običajno obstranskega pomena. Orodja pridejo večinoma že s svojo globalno politiko, ki je nad politiko spletnega brskalnika, pri čemer jih lahko uporabnik nastavi tako, da za nadzor nad spletnimi piškotki uporabi različna filtrirna pravila, vendar pa ta uporabniku ne nudijo dovolj informacij o vrsti in vsebini spletnih piškotkov.

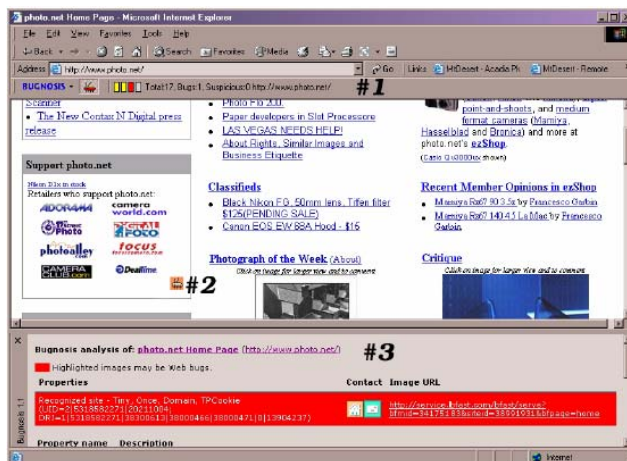
Eden izmed priljubljenih programov za upravljanje s spletnimi piškotki je Cookie Crusher, ki sicer daje uporabnikom informacije o vrsti spletnega piškotka, in ali je ta varen ali ne, vendar pa je njegova največja pomanjkljivost ta, da ne daje nobenih povratnih informacij o načinu njegovega obravnavanja oziroma kategoriziranja. To pomeni, da mora uporabnik popolnoma zaupati programu, medtem ko se odloča o tem, ali določeni spletni piškotek odstraniti ali ga obdržati. V primeru, da sprejme škodljivega, bi lahko to sprožilo zlonamerne napade na njegovo zasebnost, medtem ko bi z brisanjem koristnega lahko povzročil zmanjšanje funkcionalnosti in storitev določene spletne strani. Možna rešitev za omenjeni problem je lahko uporaba sistema za upravljanje z zasebnostjo, ki izkorišča družbene procese (sodelovanje med uporabniki).

Upravljanje s spletnimi hrošči

Program Bugnosis je dodatek k spletnemu brskalniku Internet Explorer, ki odkriva spletne hrošče med navigacijo uporabnika po spletu ter ga obvešča o njihovi prisotnosti. V primeru odkritja, nemudoma opozori z zvokom ter v ločenem oknu prikaže dodatne informacije o najdenem spletnem hrošču (Alsaid, Martin, 22. 1. 2007).

Iz okna Internet Explorerja so razvidne različne informacije (Slika 23). Območje, ki je označeno z #1, je nadzorni del programa Bugnosis in vsebuje padajoči meni, v obliki hrošča oblikovani gumb, merilec nevarnosti ter informacije o spletni strani. Odkriti spletni hrošč, ki je običajno neviden, se nadomesti z grafično ikono hrošča velikosti 18x18 pik (*pixel*), kar prikazuje območje #2. Spodnji del okna, to je območje #3, pa podrobneje prikazuje informacije o spletnem hrošču (URL naslov slike, tehnične značilnosti in izbirne ikone).

Slika 23: Princip delovanja programa Bugnosis



Vir: Alsaid, Martin, 22. 1. 2007

Po svojih funkcionalnostih je Bugnosis zelo enostavno orodje, ki potrebuje dodaten razvoj še na področju e-poštnih spletnih hroščev in P3P. Trenutno je njegova največja pomanjkljivost ta, da spremlja le nadzorovanja spletnih strani, medtem ko ne spremlja nadzorovanja poštne odjemalcev s podprtim HTML branjem. Problem pri slednjih nastopi, če uporabniki pregledujejo e-pošto z vgrajenimi spletnimi hrošči, saj se ob tem naložijo vse zahtevane slike, s čimer se omogoči poročanje tretjim osebam o njihovih aktivnostih branja. Nenazadnje na trgu že obstajajo storitve, ki lahko samodejno ustvarijo e-sporočilo z vgrajenimi spletnimi hrošči. Bugnosis prav tako ne nudi tudi nobene prave pomoči pri kontaktiranju tistih, ki so namestili spletne hrošče. Ena izmed možnih rešitev za iskanje kontaktnih informacij bi bila uporaba P3P politike, te pa program žal še ne zna prebrati.

Upravljanje s spywarom

Za zavarovanje pred naskrivaj nameščenim spywarom ali v primerih, v katerih se je uporabnik pri namestitvi brezplačnega programa strinjal z licenčnimi pogoji (EULA) (lahko vsebuje vgrajeni spyware), uporabi številne programe za njegovo nadzorovanje in odstranjevanje. Glavna težava s katero se danes srečujejo uporabniki, je ločevanje spywara od drugih programov, ki so na njihovih računalnikih ali na internetu, ter odločanje o tem, ali namestiti oziroma odstraniti določen program.

Ponudniki programov za odstranjevanje spywara uporabljajo pri svojih odločitvah o tem, katere programe bodo vključili na odstranjevalni seznam, kombinacijo objektivnega kategoriziranja in pristope točkovanja. Drugi kriteriji so lahko še zgodovina nesprejemljivega

obnašanja, kakovost posredovanih obvestil uporabnikom ter mnenja strokovnjakov in uporabnikov. Ponudniki prav tako sprejemajo veliko individualnih odločitev o tem, kaj narediti s potencialnimi spyware programi (npr. lahko se odločijo za njihovo odstranitev, ignoriranje ali pa obvestijo uporabnika). Ker bi lahko brisanje vseh potencialnih spyware programov povzročilo nedelovanje aplikacij na uporabnikovem računalniku, jih zato večina zgolj obvešča o možnih grožnjah, odločanjem o tem, kaj se bo odstranilo in kaj ne, pa prepuščajo uporabnikom (Good et al., 6. 7. 2005).

Obstoječi programi za odkrivanje in odstranjevanje spywara (npr. Ad-Aware, Spybot itd.) so pogosto učinkoviti, vendar do določene mere tudi omejeni. Največja pomanjkljivost je ta, da ne morejo vedno prepoznati in odstraniti najnovejšega spywara. Med drugim zahteva njihova uporaba tudi posameznikovo zaupanje v program, ki kategorizira spyware. Tudi tu je lahko ena izmed možnih rešitev sistem za upravljanje z zasebnostjo, ki temelji na družbenih procesih in je v primerjavi z obstoječimi programi za odstranjevanje tudi bolj dinamičen (Cranor Faith, Garfinkel, 2005, str. 542).

Upravljanje z nezaželeno e-pošto (SPAM)

Uporabniki e-pošte imajo na voljo številne programe za filtriranje ali blokiranje pošiljateljev SPAM-a, ki se poskušajo pretihotapiti v njihov poštni nabiralnik. Tehnologije filtriranja ostajajo ključna komponenta za zaustavitev SPAM-a, vendar je potreben nadaljnji razvoj za še bolj učinkovito razlikovanje med pravo in nezaželeno e-pošto. V idealnih razmerah bi filtri zagotavljali, da bi uporabnik prejemal samo zeleno e-pošto, vsa ostala pa bi bila premeščena v koš za smeti. Težava, ki se pojavlja v praksi je ta, da filtri pogosto ne-blokirajo in tudi pre-blokirajo. Pri prvem primeru gre za prehod sporočil, ki bi morala biti praviloma blokirana, pri drugem pa za zelena sporočila, ki so bila označena kot SPAM (Consumer Perspectives on Spam, 25. 2. 2007). Filtriranje, ki temelji na vsebini, deluje po tem, ko je bila e-pošta že dostavljena uporabniku. Hkrati zahteva tudi njegovo aktivno sodelovanje, saj mora biti ta neprestano pozoren na mapo za smeti, v katero bi lahko zašla zelena e-sporočila. Študije so pokazale, da je njihova trenutna učinkovitost okoli 90 % ali več, največkrat uporabljeni tehniki pa sta:

- *Rule based*

Ti filtri (npr. Spam Assassin) pregledajo vsebino e-sporočil po vnaprej definiranih besedah ali frazah, ki bi lahko namignile, da gre za SPAM. Njihova glavna pomanjkljivost je težavnost v identifikaciji ključnih besed, ki stalno nakazujejo na SPAM. Medtem ko lahko SPAM pošiljatelji pogosto uporabljajo besede, kot so »sex« ali »viagra«, se lahko te besede uporabljajo tudi za povsem upravičene poslovne namene, še posebej v zdravstveni industriji. Dodatno so se pošiljatelji SPAM-a naučili zakrivanja sumljivih besed z uporabo črkovanja, kot je »S*E*X« ali »VI a a GRR A«. Zaradi tega je skoraj nemogoče razviti slovarje, ki bi lahko identificirali vsako namenoma napačno črkovano SPAM besedo (Judge, 7. 6. 2005).

- *Bayesian*

Ti filtri (npr. Spamprove) so zelo učinkoviti pri filtriranju in zmanjševanju ne-blokiranja. Njihova prednost je ta, da se prilagajajo in učijo na podlagi povratnih informacij uporabnikov, zaradi česar producirajo skozi čas vse boljše rezultate, vendar pa tudi ti niso popolni. Pošiljatelji SPAM-a so namreč prepoznali besede, ki jih filtri privzamejo za SPAM, ter razvili različne načine za vstavljanje navadnega besedila v e-pošto z namenom zmanjšanja skupne SPAM ocene za posamezno sporočilo. Z dodajanjem odstavkov besedil iz novic in knjig lahko ti zmanjšajo učinek visoko rangiranih besed. Dolgoročno bi lahko to povzročilo zmanjšanje učinkovitosti omenjenih filtrov. Drugi način, ki ga uporabljajo, pa je ustvarjanje e-sporočil, ki so manj podobna pravemu SPAM-u, kot je na primer vstavljanje fraze »Here's the link...«. Ta pristop lahko nevtralizira skupno SPAM oceno in napelje uporabnika, da klikne povezavo na spletno stran, ki vsebuje sporočilo SPAM pošiljateljev. Za blokiranje tega SPAM-a bi moral biti filter razvit tako, da bi ta sledil povezavi in nato pregledal vsebino spletne strani, ki jo je uporabnik obiskal. Ta način filtriranja pri Bayesian filtrihi trenutno ni uporabljen, ker bi bil predrag v smislu potrebnih strežniških virov, med drugim pa bi lahko bil uporabljen tudi kot metoda za sprožitev zavračanja storitev komercialnih strežnikov.

4.2.1.2 Tehnologije varovanja identitete

Anonymizer

Razvitih je bilo kar nekaj orodij, ki pomagajo uporabnikom interneta pri ohranjanju njihove anonimnosti. Glavni namen teh orodij je zagotoviti, da se posredovane zahteve spletnim stranem, ne morejo povezati s specifičnim IP naslovom ter tako odkriti identiteto zahtevalca. Anonymizer je tipičen primer spletnega anonimnega orodja.

Princip delovanja orodja Anonymizer temelji na obstoju spletne strani tretje osebe, ki se obnaša kot vmesni člen med uporabnikom in spletno stranjo, ki jo ta namerava obiskati. Kadarkoli želi uporabnik obiskati določeno spletno stran, se pri tem ne vzpostavi neposredna povezava z zahtevanim spletnim strežnikom, ampak se to stori preko Anonymizerjeve spletne strani www.anonymizer.com:8080/desired-site. Z vzpostavitev povezave nato Anonymizer posreduje vse prejete informacije od spletne strani nazaj k uporabniku (Slika 24).



Vir: Gritzalis, 2004, str. 259

Čeprav je Anonymizer zelo enostaven za uporabo in ne zahteva nobenih sprememb na uporabnikovi strojni ali programski opremi, ima tudi določene pomanjkljivosti. Prva je ta, da mora uporabnik zaupati ponudniku Anonymizer storitev, saj lahko njegov strežnik nadzira vse spletne strani, ki jih je uporabnik obiskal, ter tako zbira informacije o njegovem obnašanju. Naslednja pomankljivost je ta, da kljub temu, da je Anonymizer učinkovit pri skrivanju identitete uporabnika in IP naslovov njegovega spletnega brskalnika pred zahtevki izvirnega spletnega strežnika, pa ta tega ne more zagotoviti tudi za komunikacijo med uporabnikovim računalnikom in Anonymizerjevim strežnikom. Nenazadnje je lahko uporabnikova anonimnost ogrožena tudi v primerih, ko se aktivira aplikacija, kot je Real Audio (omogoča poslušanje glasbe preko interneta), saj ta zaobide vmesni strežnik in vzpostavi svojo lastno neposredno povezavo (Gritzalis, 2004, str. 261).

LPWA

Lucentov personalizirani spletni asistent (LPWA) je programski sistem, razvit za podporo uporabnikom pri navigiranju po spletu in sicer na personaliziran, zaseben in varen način, pri tem pa uporablja njegove vzdevke ter druge lastnosti. LPWA ne ustvarja samo varnih, konsistentnih in psevdonimnih vzdevkov za uporabnike, ampak nudi tudi določene storitve, kot so podpora e-pošti in SPAM filtri.

Ta sistem je bil razvit za odpravo odpora uporabnikov, da uporabljajo spletne storitve, ki zahtevajo predhodno oskrbo z določenimi osebnimi informacijami. Delovanje LPWA temelji na vzdevkih za spletne uporabnike, od katerih je vsak sestavljen iz vzdevka za uporabniško ime, vzdevka za geslo in vzdevka za e-poštni naslov. Slednji dovoljuje spletnim stranem pošiljanje e-sporočil uporabnikom, vendar so ta predhodno filtrirana znotraj sistema LPWA in nato lahko tudi selektivno posredovana dejanskemu uporabniku. Uporabljeno filtriranje temelji na prejemnikovem naslovu, kar je učinkovita metoda za odkrivanje in blokiranje SPAM-a.

Pomanjkljivosti sistema LPWA so povezane z implementacijsko shemo, ki jo bo uporabil uporabnik. Če je ta shema centralni vmesni strežnik, potem obstajajo resni pomisleki, saj mora uporabnik zaupati osebam, ki so zadolžene za delovanje vmesnega strežnika na strani www.lpwa.com. Druga slabost te specifične sheme pa je, da je povezava med spletnim brskalnikom in vmesnim strežnikom javna povezava, ki se srečuje z grožnjami prisluškovanja. Med drugim je lahko dolgotrajno tudi pridobivanje informacij od spletnih strani, saj mora biti vsaka zahteva skupaj s povratno informacijo najprej posredovana na www.lpwa.com in potem nazaj. Nenazadnje LPWA tudi ne filtrira JAVA in JavaScript aplikacij, ki lahko posredujejo informacije od spletnega brskalnika nazaj k izvirnemu strežniku.

TRUSTe

Storitev TRUSTe je samoregulacijska iniciativa za zagotavljanje zasebnosti, katere glavni namen je dvigniti stopnjo potrošnikove samozavedi in zaupanja v internet.

TRUSTe pomaga pri izgradnji politike zasebnosti, upoštevajoč pri tem specifične tehnične značilnosti spletne strani kot tudi aplikacije in storitve, ki jih ta nudi. Podrobnosti o politiki zasebnosti so odvisne od ugotovitev poročila po prvem opravljenem pregledu določene spletne strani. Večkratni nadaljnji pregledi pa zagotavljajo, da je delovanje spletne strani v skladu z objavljeno politiko zasebnosti, ter identificirajo morebitne potrebne spremembe. Spletna stran, ki je pridobila pečat zasebnosti, s tem sporoča svojim uporabnikom, da so njihove odkrite informacije zavarovane na način, ki ga je odobrila (in za katerim stoji) kredibilna tretja oseba (TRUSTe).

TRUSTe principi zasebnosti vključujejo (Glee Harrah, McGregor, 2001, str. 468):

- sprejetje in vpeljavo politike zasebnosti,
- objavo in odkritje informacij, ki se zbirajo, ter prakse njihove uporabe,
- možnost izbire in privolitve, kar daje uporabnikom priložnost nadzora nad njihovimi informacijami,
- ukrepe dostopanja z namenom zagotoviti varnost in točnost osebnih informacij,
- ponovno pridobitev pečata in poročanje ustreznim oblastem o imetniku, ki ni uspel zagotoviti skladnosti s politiko.

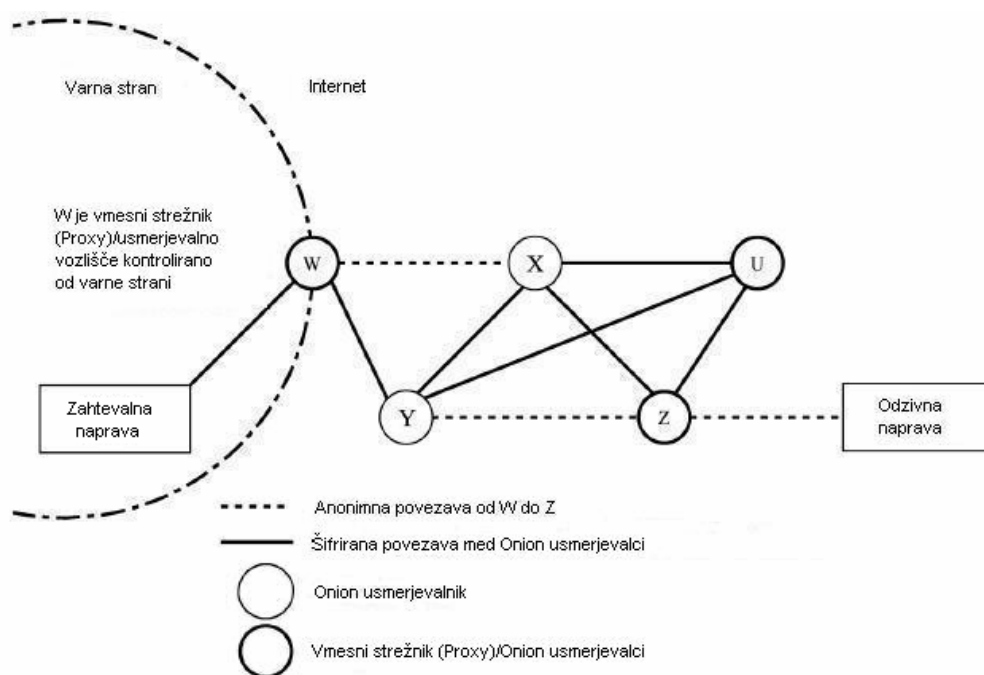
Glavni namen storitve TRUSTe je v potrditvi elementov politike zasebnosti posamezne spletne strani. Iz tega izhaja tudi največja pomanjkljivost in sicer, da ne nudi nobenega varovanja pred zlonamernimi napadi ter pred aktivnimi in pasivnimi povratnimi napadi. Posledica tega je lahko ta, da napadalec izsledí pobudnika spletne zahteve. Ta težava bi se lahko odpravila s kombiniranjem TRUSTe jamstva in varovanjem, ki ga nudijo druge anonimne storitve ali orodja.

Onion Routing

Onion Routing je sistem, ki podpira zasebne komunikacije preko javnih omrežij, kar doseže s pomočjo aplikacijsko neodvisnih, skoraj realno časovnih in dvosmernih anonimnih povezav, ki so odporne tako na napade prisluškovanja kot analize prometa.

Paketi, ki potujejo po anonimnih povezavah Onion Routinga, vsebujejo namesto prikaza izvirnega in namembnega naslova samo informacije o naslednjem in predhodnem preskoku. Ta vrsta povezave lahko pravzaprav nadomesti vhodne povezave. Medtem, ko se slednje uporabljajo kot podpora internetno zasnovanim aplikacijam, se lahko prvo uporablja kot podpora mnogim ostalim nespremenjenim aplikacijam preko vmesnih strežnikov Onion Routinga. Princip delovanja sistema Onion Routing temelji na dinamični gradnji anonimnih povezav znotraj Chaum Mixes omrežja (*Onion Routers*), ki so povezane s stalnim protokolom za nadzor prenosa – TCP povezava (Slika 25).

Slika 25: Princip delovanja sistema Onion Routing



Vir: Gritzalis, 2004, str. 266

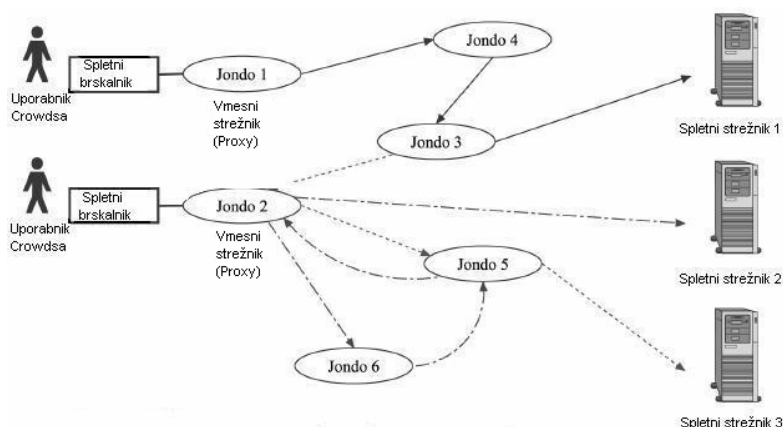
Pomanjkljivost sistema Onion Routing je ta, da je lahko napadalec, ki je zbral zadostno količino podatkov, še vedno sposoben analizirati vzorce uporabljanja in na podlagi teh sprejemati premišljena ugibanja o usmerjevalnih poteh. V primerih, ko določena aplikacija zahteva vzpostavitev realno časovne komunikacije, obstaja tudi možnost odkritja vhodnih povezav, ki bodo vzpostavljene med zahtevalnim in odzivnim vmesnim strežnikom. Ena izmed možnih rešitev je lahko ta, da se napadalce zmede z ustvarjanjem lažnega prometa na mreži, s ciljem doseganja vedno enake količine prometa.

Crowds

Sistem Crowds omogoča pridobivanje informacij preko spleta brez odkritja osebnih informacij zlonamernim tretjim osebam – uporabniku ali računalniškemu sistemu. Njegov snovalski cilj je narediti spletno navigiranje anonimno, s čimer bo mogoče skriti informacije o uporabniku, spletne strani, ki jih je ta obiskal, ter vsebino, ki jo je pridobil od spletnih strežnikov.

Koncept anonimnega Crowds agenta je ta, da lahko član množice ostane anonimen in da lahko skrije svoje aktivnosti v aktivnostih drugih članov te množice. Specifični protokol prepreči spletnemu strežniku zapisovanje kakršnih koli informacij (npr. domensko ime, uporabnikov IP naslov, uporabnikovo računalniško platformo itd.), ki bi se lahko uporabile za identifikacijo uporabnika (Slika 26).

Slika 26: Princip delovanja sistema Crowds



Vir: Gritzalis, 2004, str. 267

Uporabniki sistema Crowds se morajo zavedati tudi nekaterih možnih tveganj. Teoretično lahko namreč kateri koli član množice preneha pošiljati katero koli zahtevo, ki izvira iz množice. Če bi se to zgodilo, bi si spletni strežnik zapisal IP naslov vzpostavljenega procesa, ki se odvija na uporabnikovem računalniku (*jondo*) ter izvorni naslov zahtevalca. Pomanjkljivost Crowds arhitekture je ta, da ne varuje zaupnosti zahtevanih vsebin na svoji poti, vendar bi se to lahko rešilo z uporabo kriptografije. Kot katero koli drugo anonimno orodje zasnovano na vmesnih strežnikih, se da tudi Crowds preslepiti v primerih, ko uporabnikov spletni brskalnik namesti in izvrši mobilne kode, ki vzpostavijo povratno povezavo do strežnika, ki ga je postregel. Nenazadnje je na splošno povečan tudi skupni čas pridobivanja spletnih strani, mrežnega prenosa in nalaganja na računalniku, ki izvršuje »jondo«.

Hordes

Protokol Hordes uporablja številne vmesne strežnike za usmerjanje paketa proti odzivnemu viru, medtem ko za usmerjanje odgovora proti izvornemu viru uporablja večnamenske storitve. Vse skupaj na anonimen način.

Hordes je bil prvi protokol, ki je izkoristil prednosti anonimnih značilnosti ter zmogljivosti, vsebovanih v IP večnamenskem usmerjanju. Ta zagotavlja prejemnikovo anonimnost in sicer z nudenjem najkrajše možne povratne poti, s čimer se zmanjšuje skupna komunikacijska latentnost. Večnamenski naslovi niso povezani z nobeno posebno napravo, ki je priključena na omrežje; namesto tega so enostavne označbe, ki se sklicujejo na prejemnike določene skupine kot celote, brez vedenja o posameznem prejemniku. Število gostiteljev, ki se obnašajo kot prejemniki in njihovi statusi, so dinamični ter nepoznani usmerjevalcem in gostiteljem. Te posebne lastnosti večnamenske komunikacije so zelo cenjene pri varovanju anonimnosti. Nenazadnje Hordes izkorišča večnamensko komunikacijo tudi za povratno pot anonimne komunikacije.

Ena izmed pomanjkljivosti Hordsa je ta, da je lahko prav tako zlorabljen kot katera koli druga, na vmesnem strežniku zasnovana anonimna storitev, saj lahko spletni brskalnik naloži

in izvrši mobilne kode, ki vzpostavijo povratno mrežno povezavo do strežnika, ki ga je postregel. Naslednja pomanjkljivost je tudi, da se lahko pasivni povratni napadi bistveno lažje izvedejo na centralizirana omrežja kot pa na skupino širše porazdeljenih gostiteljev.

Freedom

Sistem Freedom je bil razvit za varovanje zasebnosti uporabnikov, ki so vpleteni v opravila, kot so pošiljanje e-pošte, navigiranje po spletu, oddaja sporočila novičarskim skupinam in sodelovanje v internetnem pogovoru.

Ta sledi arhitekturi uporabnik–strežnik in deluje transparentno z obstoječimi internetnimi aplikacijami. Kadar so uporabljene njegove najboljše storitve, je internetni promet šifriran, preden ta zapusti uporabnikov računalnik in se usmerja preko zasebnih povezav. Uporablja tudi psevdonimne digitalne identitete znane kot »nynms«, ki se uporabljajo na enak način kot običajna spletna identiteta, brez odkritja prave identitete uporabnika.

Največja pomanjkljivost sistema Freedom je možnost napada na uporabnika s posredovanjem obsežne e-pošte, s čimer bi se prisililo uporabnika v njeno dolgotrajno pobiranje preko omrežja Freedom in kar bi lahko izkoristili napadalci za izsleditev povratne povezave do uporabnika. Možno je tudi, da bi nek zelo nevaren napadalec imel nadzor nad opremo ali si zapisoval promet na različnih vstopnih točkah omrežja z namenom, da bi identificiral uporabnika.

GAP

GNUnetov anonimni protokol GAP je nedavno predstavljeni protokol, katerega cilj je doseči anonimen prenos podatkov. Ta predstavlja povsem nov pogled na anonimnost, saj omogoča posamezniku ignoriranje nekaterih tradicionalnih zahtev anonimnosti, s čimer se dopušča omrežnim vozliščem svobodo pri uravnavanju anonimnosti z učinkovitostjo sistema.

GNUnet je »peer-to-peer« omrežje (P2P) in zato ne obstaja vozlišče, ki bi nadziralo omrežje. Model nudi odkrivanje vozlišč (*peers*), šifriranje povezave in oblikovanje e-sporočil. Osnovna aplikacija GNUnet-a je anonimno deljenje datotek z drugimi, pri čemer uporablja shemo, ki razbije datoteke v pakete velikosti 1KB. Ti paketi so nato preneseni s protokolom GAP. Komunikacija med vsemi mrežnimi vozlišči poteka zaupno, kar pomeni, da noben gostitelj zunaj tega omrežja ne more opazovati potujočih podatkov. Med drugim niso določljive niti vrste podatkov, saj so vsi paketi oblikovani tako, da so enakih velikosti.

GAP protokol je bil prilagojen funkcionalnosti »peer to peer« omrežja, kar je mogoče njegova največja pomanjkljivost. Ta sicer varuje anonimnost vozlišč, uporabljajoč pri tem posebne tehnike mrežnega prometa, vendar pa na drugi strani ne more zagotoviti zanesljive dostave paketov, saj so lahko pomnilniki (lokalno shranjevanje) nedosegljivi v primeru zaposlenega vozlišča ali visokega mrežnega prometa. Nenazadnje, več kot vozlišče ustvari prometa, več se mora preusmeriti tujega prometa, da se lahko ohrani lastne aktivnosti.

4.2.1.3 Tehnologije varovanja s privolitvijo

P3P

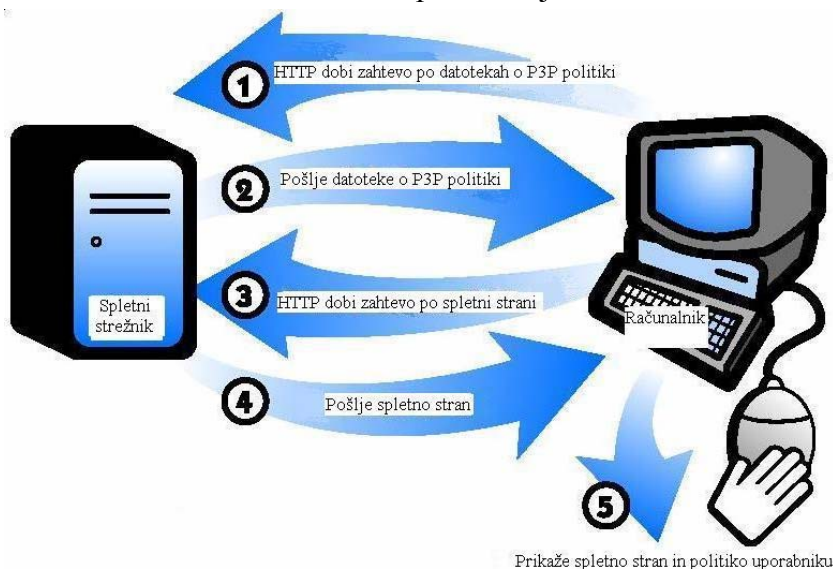
Platforma za preference zasebnosti (P3P) nudi model za informirane spletne interakcije, njen glavni cilj pa je omogočiti uporabnikom, da uveljavljajo svoje preference zasebnosti nad praksami zasebnosti spletnih strani.

P3P aplikacije omogočajo uporabnikom, da so seznanjeni s praksami spletnih strani, da delegirajo odločitve njihovim računalniškim agentom, ko ti želijo in da vzdržujejo odnose s specifičnimi stranmi. Storitev P3P se dopolnjuje tako s tehnologijami, ki onemogočajo prakse, ki bi lahko bile nesprejemljive za uporabnika, kot tudi z regulativnimi in samoregulacijskimi pristopi zasebnosti. Zgoraj omenjene tehnologije vključujejo anonimne in šifrirne tehnike, ki omejujejo informacije, ki jih lahko prejemnik ali prisluškovalec zbira med komunikacijo. Zakoni in industrijske smernice pa na drugi strani opredeljujejo ter določajo pričakovanja glede informacijskih načel in so lahko obvezujoča, ali pa služijo kot vodilo nadaljnjim interakcijam.

P3P besedišče prikazuje naslednje (Borking J., 2005, str. 83):

- kdo zbira podatke;
- kateri podatki se zbirajo in za kakšne namene;
- opt-in in opt-out alternativa uporabe nekaterih podatkov;
- kdo so prejemniki podatkov;
- do katerih informacij nudi kontrolor podatkov dostop;
- obdobje zadrževanja podatkov;
- kako se bodo reševali spori glede politike zasebnosti določene organizacije;
- kje je človeško-berljiva politika zasebnosti.

Slika 27: Princip delovanja P3P



Vir: [URL:<http://www.w3.org/P3P/brochure/full-brochure.pdf>], 10. 12. 2006

Čeprav lahko spletni uporabniki dosežejo sporazum s storitvijo, v kateri se namesto osebnih informacij posreduje posebna identifikatorja, je lahko njihova identiteta kljub temu še vedno izsledljiva preko IP naslova. Pomanjkljivost storitve P3P je tudi ta, da deluje v povezavi z drugimi anonimnimi spletnimi orodji, protokoli in storitvami, saj sama ne more varovati uporabnikove zasebnosti in anonimnosti. Uporabniki lahko odpravijo to pomanjkljivost, če uporabljajo P3P skupaj z nekaterimi drugimi anonimnimi storitvami ali orodji, kot so Anonymizer, LPWA, Onion Routing in Crowds.

P3P uporabniški agenti

P3P uporabniški agent je osebni asistent, zasnovan za pomoč uporabnikom pri razumevanju politike zasebnosti spletne strani v povezavi z njihovimi preferencami zasebnosti. Naloga teh agentov je, da uporabniku natančno in enostavno predstavijo ustreznost omenjene politike. Trenutno najbolj razširjena P3P uporabniška agenta sta IE6 in AT&T Privacy Bird, ki za prikazovanje skladnosti uporabljata okno spletnega brskalnika (Levy E., Gutwin, 2005, str. 482):

– IE6

Agent spletnega brskalnika Internet Explorer (IE6) uporablja P3P »kompaktno politiko«, ki je lahko posredovana v http glavi ob namestitvi spletnega piškotka, za sprejemanje odločitev o njihovem blokiranju. Kadar se politika do spletnih piškotkov na določeni spletni strani ne ujema s preferencami zasebnosti uporabnika, prikaže IE6 okno, prekrito z znakom »ne vstopaj« (Slika 28). Dodatne informacije o konfliktu pa so na voljo ob kliku nanj. Glavna pomanjkljivost IE6 je, da brez popolnih preferenc uporabnika lahko tega le opozarja o osebnih informacijah, ki so shranjene v spletnih piškotkih, ne pa tudi o zbiranju osebnih informacij v spletnih obrazcih.

Slika 28: Ikona zasebnosti pri IE6

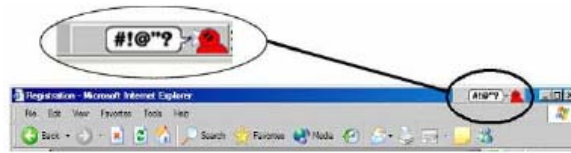


Vir: Levy E., Gutwin, 2005, str. 482

– AT&T Privacy Bird

AT&T ptica zasebnosti implementira celotne P3P in APPEL specifikacije. Ta v vrstici spletnega brskalnika prikazuje ikono ptička, ki spreminja barvo in oddaja zvoke, s čimer označuje ujemanje oziroma neujemanje P3P politike spletne strani s preferencami zasebnosti uporabnika (Slika 29). Omenjena ikona se prav tako uporablja za dostopanje do informacij o politiki zasebnosti in o njeni ustreznosti.

Slika 29: Ikona zasebnosti pri AT&T Privacy Bird



Vir: Levy E., Gutwin, 2005, str. 482

Glavna pomanjkljivost agenta pri ptici zasebnosti je ta, da ni sposoben določiti vnosno polje v spletnem obrazcu, ki je povzročilo ustreznostmi konflikt, medtem ko spletne strani brez vnosnih polj prikazujejo rezultat ustreznosti za celotno stran (P3P specifikacije omejujejo drobljenje informacij o politiki). Predstavitev je vedno enaka ne glede na to ali je eden ali več problemov z ustreznostjo, zaradi česar uporabnik ne ve kdaj so vnosna polja v konfliktu; prebrati mora dodatne informacije, da bi dobil rezultate za vsako vnosno polje.

4.2.2 Primerjalna analiza na enotni osnovi

Tehnologije varovanja na osebni ravni so odvisne le od proizvajalcev programske opreme, na kakšen način se bodo uporabljale, pa je odvisno od vsakega posameznika. Povsem drugače je pri tehnologijah varovanja identitete in s privolitvijo, ki so bolj ali manj odvisne od celotne zgradbe spleta (Jerman Blažič, 2005a, str. 229). Zaradi njihove kompleksnosti in posredovanega zaupanja s strani spletnih uporabnikov, bodo te v nadaljevanju podrobneje analizirane.

Videli smo, da obstaja več različnih načinov za doseganje spletne zasebnosti in anonimnosti pri tehnologijah varovanja identitete in s privolitvijo. Eden izmed teh načinov je bil vstavev nove entitete med pošiljatelja in prejemnika z namenom zakriti identiteto zahtevalca. Primeri teh vmesnih strežnikov so Anonymizer in LPWA. Drug način za doseganje anonimnosti pri spletnih transakcijah je uporaba razvijajočih se vmesnih strežnikov, ki lahko poleg skrivanja pošiljatelja pred prejemnikom varujejo še spletni strežnik in prejemnika pred prisluškovanjem. Primer tega je Onion Routing in do določene mere Crowds in Hordes. Zasebnost se lahko varuje tudi na nivoju komunikacijskega protokola. Tipičen primer je protokol GAP, ki je bil razvit za zagotovitev anonimnega prenosa podatkov v »peer-to-peer« omrežjih. Za bolj splošne namene varovanja zasebnosti je Freedom, ki varuje spletne uporabnike in aplikacije na transparenten način. Nazadnje obstajajo tudi samoregulacijske iniciative zasebnosti, kot je TRUSTe, s ciljem potrjevanja elementov politike zasebnosti spletnih strani, ter modeli kot je P3P, ki omogočajo uporabnikom, da uveljavljajo svoje preference zasebnosti nad praksami zasebnosti spletnih strani.

Stefanos Gritzalis ugotavlja, da se pri razvijajočih se spletnih mehanizmih zasebnosti in varnosti, orodjih, protokolih in storitvah pojavljajo naslednje razlike (Gritzalis, 2004, str. 273):

- obstajajo razlike v ciljih snovanja,
- odvisno od uporabljene tehnologije, se rešuje različna vprašanja zasebnosti in anonimnosti,
- uporabljajo so različne tehnike za doseganje neenakih namenov.

Da bi uravnotežil zgoraj omenjene razlike, je opravil primerjalno analizo in sicer na treh različnih področjih (Tabela 4): **odpornost na varnostne grožnje** (povratni napadi, zlonamerno sodelovanje, prisluškovanje, napadi na velikost in vsebino sporočila, časovni napadi, periodični napadi na povezavo, spletni piškotki in personalizirane storitve), **uporabljene tehnološke rešitve** (zanesljivost in zaupanje, kompleksnost namestitve, zmogljivost in splošna latentnost) in **zadovoljitev uporabnikovih zahtev** (anonimnost povezave, anonimnost podatkov in personalizacija, nizki stroški, uporabnost programa in prijaznost do uporabnika ter dodatne storitve).

Omenjena raziskava je pokazala, da se prednosti ter slabosti vsakega sistema v smislu stopnje varovanja zasebnosti in anonimnosti ne ujemajo. To se je tudi pričakovalo, saj je bil vsak sistem pri snovanju osredinjen na različne cilje. Na primer sistemi, ki temeljijo na enem spletnem vmesnem strežniku, kot sta Anonymizer ali LPWA, se lahko uporabijo za zagotovitev anonimne navigacije, medtem ko so sistemi, kot so Onion Routing, Crowds in Hordes boljši pri varovanju informacij ter preprečevanju napadov. Onion Routing lahko tu predstavlja osnovo, na kateri bi se uporabili drugi protokoli, z namenom izboljšanja stopnje varovanja spletnega uporabnika. Na drugi strani pa se storitve, kot so TRUSTe in P3P, pogajajo, zagotavljajo in periodično preverjajo celovitost ter pravilnost politike zasebnosti posameznih spletnih strani. Freedom je sistem, ki izpolnjuje večino zahtev uporabnikov, še posebej glede stopnje varovanja pred varnostnim grožnjam; vendar veliki stroški na drugi strani zasenčijo vse njegove prednosti. GAP se lahko uporabi v »peer-to-peer« omrežjih, kot je GUNet, in sicer za vpeljavo varnih in anonimnih transakcij med vozlišči. To je še posebej priročno za uporabnike interneta, ki veliko uporabljajo »peer-to-peer« aplikacije za deljenje datotek (npr. GNUtella, KaZaa itd.) ter tiste, ki pogosto kršijo zasebnost in anonimnost svojih vozlišč.

Tehnološki napredek in vse večje potrebe uporabnikov na področju komercialnih internetnih aktivnosti bi morale voditi k nadaljnjim tovrstnim raziskavam. Prodor protokolov, storitev in orodij, ki podpirajo nove tehnologije, kot so SSL/TLS ali IPv6 značilnosti bo najverjetneje zahteval ponovno oceno predstavljene primerjalne analize na enotni osnovi. Nenazadnje bi se lahko v spletno zasebnost in anonimnost vključilo tudi uporabo digitalnega denarja in kreditnih kartic pri spletnih transakcijah. Zanimiva bi bila tudi analiza značilnosti, ki niso bile upoštevane pri snovanju razvijajočih se storitev zasebnosti za elektronsko trgovino, ali glavne razlike v tehnološkem snovanju ter poslovnimi modeli. Prav tako bi se lahko opravila analiza na trenutno zelo aktualnem področju, to so sistemi z vgrajenimi agenti zasebnosti.

Tabela 4: Primerjalna analiza mehanizmov zasebnosti in varnosti, orodij, protokolov in storitev

Kriterij	Odpornost na varnostne gročnje										Uporabljene tehnološke rešitve					Zadovoljitev uporabniških zahtev				
	TBA(A)	TBA(P)	MC	E	MCA/A	TA	FA	CPA	C	PS	R&T	IC	P	OL	CA	DA	P	LC	U	S
Tehnologije																				
Anonymizer	-	-	x	-	-	-	-	-	-	-	H	L	H	L	L	M	x	L	H	L
LP00/A	-	-	x	-	-	-	-	-	+	+	H	M	H	L	L	M	H	H	M	H
TRUSTe	x	x	x	-	-	-	-	-	+	+	H	L	H	L	x	x	x	H	L	L
P3P	x	x	x	-	-	-	-	-	-	+	H	L	H	L	x	x	x	M	M	L
Onion Routing	+	-	+	+	+	-	-	-	-	-	L	H	L	H	H	H	x	H	L	M
Crowds	+	-	+	+	+	-	-	-	-	-	L	H	M	H	H	M	x	M	L	L
Hordes	+	-	+	+	+	-	-	-	-	-	M	H	M	H	H	M	x	M	L	L
Freedom	-	+	x	+	+	-	-	-	+	+	H	M	M	L	H	H	H	L	M	H
GAP	+	+	+	+	+	+	+	+	x	x	L	H	H	L	H	H	x	H	L	M

Ocena: H: visoka, M: srednja, L: nizka, x: ni uporabljeno, +: pozitivno In -: negativno

Oznaka: TBA(A) = povratni napadi (aktivni); TBA(P) = povratni napadi (pasivni); MC = zlonamerno sodelovanje; E = prisluskovanje; MCA/A = napadi na vsebino in velikost sporočila; TA = časovni napadi; FA = obremenitveni napadi; CPA = perioični napadi na povezavo; C = spletni piškotki; PS = personalizirane storitve; R&T = zanesljivost in zaupanje; IC = kompleksnost namestitve; P = zmogljivost; OL = prekomerna latentnost; CA = anonimnost povezave; DA = anonimnost podatkov; P = personalizacija; LC = nizki stroški; U = uporabnost programa; S = dodatne storitve

Vir: Gritzalis, 2004, str. 286

4.2.3 Ocena dosedanje uspešnosti

Poročilo o napredku tehnologij za varovanje zasebnosti (PET) za obdobje od leta 1997 do 2002 navaja, da je v tem času nastalo in prav tako zamrlo veliko različnih tehnologij ter da smo bili priča težavam pri vpeljavi sistemov, ki so temeljili na razširjeni infrastrukturi. Tehnična orodja, ki so nam ostala na voljo, so nekako šibka, izkazalo pa se je tudi, da ne moremo doseči popolnega tehnološkega varovanja. Zaskrbljujoče je predvsem dejstvo, da se je v tem obdobju zgodilo le malo tehnoloških sprememb, še posebej na načine, kot se je to pričakovalo. Namesto tega smo bili priča le povečani uporabi kombinacije družbenega in tehnološkega dialoga (Goldberg, 25. 2. 2007).

Lee Bygrave se je v svojem članku osredinil na pregled težav, ki se pojavljajo pri razvoju in uporabi PET, ter prišel do naslednjih zaključkov (Bygrave A., 2002, str. 135–137):

- ***PET niso ljubljenci***

Tehnologije za varovanje zasebnosti so še vedno daleč od tega, da bi bile naš stalni spremljevalec; trenutno niso dovolj prijazne niti dovolj razumljive. Za večino ljudi ostajajo tako nepoznane, slabo razumljive in popolni tujec v vsakdanjem življenju.

- ***PET se ne izplačajo***

Ekonomski vidik je eden izmed glavnih dejavnikov, ki škoduje PET iniciativam, saj se razvoj PET velikokrat ne izplača. V zadnjem desetletju smo tako bili priča številnim propadlim komercialnim iniciativam, pri čemer PET niso ostale samo tehnologije v iskanju aplikacij – kot tehnologije za invazijo na zasebnost (PIT) – ampak prej tehnologije v iskanju komercialnega preživetja. Dosedanja praksa kaže, da so investicije potrebne za preboj in ostanek na PET trgu, velikokrat bistveno prekoračile finančne prihodke.

- ***PET niso popularne***

Del ekonomskega problema, s katerimi se srečujejo PET iniciative, je tudi pomanjkanje širšega povpraševanja potrošnikov po teh aplikacijah. To pomanjkanje je posledica različnih dejavnikov. Delno je to zaradi nizkega zavedanja potrošnikov o dostopnosti in funkcionalnostih PET kot tudi dejstva, da je skrb glede zasebnosti v javnosti pogosto visoka, medtem ko se to le redko odraža v konkretnih aktivnostih, ki denarno stanejo.

Vzrok za slabo povpraševanje po PET izhaja iz nekaterih njihovih značilnosti in načina njihovega trženja. Posamezna PET aplikacija ima ponavadi omejeno področje uporabnosti (npr. šifriranje e-pošte ali blokiranje spletnih piškotkov), zaradi česar se

mora uporabnik, ki je zelo zainteresiran, da bi zavaroval svojo zasebnost na večih področjih, najprej naučiti in nato tudi pridobiti številne PET od številnih organizacij.

V smislu trženja obstaja predvsem pomanjkanje informacij o trenutno dostopnih produktih, o njihovih razvijalcih in informacije, ki so netehnične narave. Ta tako imenovana informacijska luknja je še posebej problematična zaradi sorazmerno velikega števila kompleksnih produktov skupaj z dejstvom, da so nekatere PET funkcionalnosti za običajne osebe – še posebej psevdonimnost, anonimnost in preverjanje – sorazmerno težavne za pravilno uporabljanje.

Do sedaj so PET dobile tudi zelo malo pravega zagona s strani politikov in drugih glavnih akterjev. Na PET gledajo vlade še naprej z dvomom in antipatičnostjo, saj ogrožajo interese nacionalne varnosti in preprečevanje kriminala. Dogodki 11. septembra v ZDA in napovedana vojna proti terorizmu je naredila politično klimo do PET nedvomno še bolj neprijazno.

- ***PET so lahko PIT***

PET občasno napadejo tudi njihovi lastni zagovorniki. Zaskrbljenost izražajo predvsem nad stopnjo zasebnosti, ki jo dovoljuje posamezno orodje (npr. ali prednjači psevdonimnost, medtem ko je anonimnost pomembnejša, ali upošteva standarde iz direktive o varovanju podatkov ali pa druge manj stroge standarde). Nadalje so zaskrbljeni nad izkušnostjo PET razvijalcev in značajem vzpostavljenega procesa (npr. kako odprt in transparenten je proces) ter kontekstom in učinkom uporabe PET (npr. ali je bila PET uporabljena v procesu z namenom povečanja organizacijske moči na škodo posameznikov, ali je bila PET vpeljana kot povod v PIT).

- ***PET in zakonodaja***

Zakonodaja je eden izmed dejavnikov, ki lahko prav tako ovira razvoj PET. Prvo in najbolj očitno ter hkrati moteče dejstvo je, da v določenih primerih nekatera zakonodajna pravila ali prakse dovoljujejo odkritje osebne identitete. Med drugim so zakonodajna pravila velikokrat tudi preveč dvoumno napisana, da bi lahko bila učinkovito prevedena v PET standarde. Istočasno lahko poskus vpeljave specifičnih PET pravil v zakonodajo z namenom, da bi se povečala njihova uporaba, sproži konflikte s splošno sprejetimi regulativnimi principi. Eden izmed takih principov je, da morajo biti zakonodajna pravila tehnološko nevtralna ali da ne smejo vplivati na konkurenčnost trga.

Vsesplošna raziskava s strani META GROUP za potrebe danskega ministrstva za znanost in razvoj je pokazala še naslednje probleme, povezane s PET (Privacy Enhancing Technologies, 2005, str. 27–29):

- ***Zasebnost v aplikacijah bo pogosto zahtevala dodatne spremembe***

Večina današnjih PET je konceptualno zasnovanih za odpravo pomanjkljivosti v IT sistemih ter postopkih upravljanja z informacijami. PET so običajno dodatki k produktom z namenom, da bi se izboljšal vidik zasebnosti v informacijskih sistemih, ki so bili zgrajeni brez te zahteve.

Vendar ima lahko dodajanje PET v sisteme (npr. nadomeščanje osebnih števil z nevtralnimi identifikatorji) tudi nekatere negativne stranske učinke:

- lahko zmanjša celotno učinkovitost sistema (npr. ko morajo biti iskanja v podatkovnih bazah izvedena z več kriteriji, namesto z enim edinstvenim ključem - številka osebe);
- lahko vodi do manj zanesljivih podatkov (npr. brez vidnih edinstvenih ključev je verjetnost odkrivanja napak manjša - s strani uporabnika ali orodij za vzdrževanje);
- lahko poveča ranljivost sistema za prevare in zlorabe (npr. ko se omeji možnost navzkrižnega preverjanja ene podatkovne baze z drugimi).

To nakazuje, da dodajanje PET v obstoječe aplikacije pogosto zahteva nekatere dodatne spremembe v sistemu, da bi se lahko zagotovila učinkovitost, zanesljivost in robustnost storitve. Te spremembe ponavadi niso pokrite s strani PET dobaviteljev, kar pomeni, da je treba imeti poglobljeno znanje o aplikaciji.

- ***Nadziranje zasebnosti s strani uporabnika lahko vpliva na pravice***

PET orodja in storitve (npr. anonymizer, psevdonymizers itd.) so bila razvita za varovanje identitete spletnega uporabnika pred možnim odkritjem. Vendar lahko uporaba teh orodij pri interakcijah s spletnimi storitvami, ki predvidevajo prisotnost prave identitete, povzroči tudi kršitev poslovnih pravil ponudnika. Drugače povedano, če spletna storitev ni bila razvita za anonimne uporabnike, bi lahko ponudnik ne želel ali pa ne bi mogel izpolniti svojih kasnejših obveznosti (npr. obravnava garancijskih zahtevkov).

- ***Izkoriščanje pomanjkljivosti v zasnovi lahko vpliva na delovanje***

Nekatere PET izkoriščajo luknje v zasnovi obstoječih aplikacij in sicer za dodajanje določene stopnje zasebnosti (npr. z vstavljanjem podatkov v polja, razvita za sprejem edinstvenih identifikacij). V drugih primerih se PET orodja povezujejo z glavami v e-sporočilih, pri čemer izkoriščajo pomanjkljivosti v zasnovi protokola. Te metode so podobne tehnikam, ki jih uporabljajo hekerji, pošiljatelji SPAM-a in programerji virusov; etično niso sprejemljive in lahko resno zmanjšajo zanesljivost in kompatibilnost IT rešitev.

- ***Pomanjkanje standardiziranih rešitev zasebnosti***

Standardizacija lastnosti in rešitev zasebnosti je šele na svojem začetku – trenutno so PET rešitve redko interoperabilne (z izjemami, kot je P3P in jezik EPAL), saj skupno razumevanje konceptov in zahtev še ni bilo doseženo. Zaradi tega lahko imamo večino današnjih PET za nedozorele.

Herman Tavani je šel še dlje in raziskal nekatere izmed načinov, s katerimi PET omogočajo posameznikom upravljanje z zasebnostjo (preko mehanizmov nadzora kot sta izbira in privolitve) ter prišel do naslednjih ugotovitev (Tavani T., Moor H., 2001, str. 9–11):

- ***PET in vloga posameznikove izbire***

Čeprav lahko PET omogočijo uporabnikom določen obseg nadzora nad osebnimi informacijami na začetku spletne transakcije, pa ni nujno da bodo imeli omogočen nadzor nad njihovo uporabo tudi potem, ko so bile te že odkrite spletnim prodajalcem. Nazoren primer tega je incident podjetja Toysmart, ki je po bankrotu prodalo bazo o strankah tretjim osebam, da bi lahko poplačalo del svojih dolgov. Njihovi kupci so sicer imeli določen nadzor nad osebnimi informacijami (nadziranje ali bodo odkrili osebne informacije pri spletnih transakcijah) na osnovi pogojev, ki so bili zapisani v politiki zasebnosti ter pečatu zasebnosti (PET), vendar se je na drugi strani tudi izkazalo, da se posameznikom ni moglo zagotoviti, da bodo njihove posredovane informacije varovane tudi v prihodnosti.

- ***PET in princip zavestne privolitve***

V določenih komercialnih spletnih aktivnostih, vključujoč tiste, ki vsebujejo uporabo PET, princip zavestne privolitve ne deluje vedno tako dosledno, kot bi sicer pričakovali. Primer so lahko uporabniki, ki prostovoljno privolijo v posredovanje osebnih informacij za določen namen ali za eno transakcijo, pri čemer niti najmanj ne pomislijo, da bi se lahko te informacije uporabile za povsem druge namene. Čeprav ta problem ni edinstven samo za PET, se je zaskrbljenost glede sekundarne uporabe osebnih podatkov še povečala, predvsem zaradi določenih spletnih aktivnosti, vključujoč transakcije e-poslovanja. Ne glede na to, ali uporabniki privolijo v zbiranje osebnih informacij, se jim mora dodeliti tudi eksplicitna izbira, ali bodo privolili ali ne v prihodnjo uporabo teh informacij za sekundarne namene. Vse PET spletnim uporabnikom ne nudijo te eksplicitne možnosti.

Potrditev ali zavrnitev hipoteze:

Na podlagi predstavljenih dejstev v četrtem poglavju lahko v celoti potrdimo uvodoma postavljeno hipotezo, da tehnologije za varovanje zasebnosti na internetu niso popolnoma dodelane in učinkovite.

5 PRIPOROČILA IN USMERITVE ZA PRIHODNOST

Priporočila in usmeritve se nanašajo na razvoj bolj dodelanih in učinkovitih tehnologij za varovanje zasebnosti (PET), upoštevajoč pri tem trenutne raziskave na področju sistemov za upravljanje identitete. Za podprtje bogatih in storitveno naravnanih interakcij, ki jih želijo uporabniki interneta, bi morale varovanje zasebnosti doseči naslednje zahteve (Berendt, Günther, Spiekermann, 2005, str. 105–106):

- PET bi morale biti vedno pod popolnim nadzorom spletnega uporabnika;
- PET bi morale nadzorovati storitve tretjih oseb, podobno, kot to dela P3P, in seznaniti spletnega uporabnika o možnih problemih. Z opazovanjem bi se morale naučiti tudi uporabnikovih preferenc ter dinamičnega spreminjanja nastavitvev;
- PET bi morale zapisovati interakcije spletnih storitev in ustvariti informacijsko bogate profile na strani odjemalcev. Z veliko previdnostjo bi lahko bili deli teh profilov dostopni marketingu ali »peer-to-peer« omrežjem;
- PET bi morale imeti enostavne uporabniške vmesnike in zasebnosti prijazne privzete nastavitve;
- PET bi morale nuditi upravljanje identitete, pri čemer bi dovoljevale uporabnikom prevzemanje novih psevdonimov ob vsakokratnem ponovnem vstopu na spletno stran ter varovati profile na strani odjemalcev;
- PET bi morale dekontekstirati. Prepoznavanje in blokiranje nevarnih interakcij bi lahko bilo samodejno, če bi bile PET sposobne razumeti vse interakcije. Ker pa niso, morajo zaposliti svoje uporabniške vmesnike za podprtje uporabnikovega načina razmišljanja.

V strokovni literaturi zasledimo številne dejavnike, ki lahko pomembno vplivajo na prihodnost tehnologij za varovanje zasebnosti (PET). Najpogostejši bodo v nadaljevanju podrobneje predstavljeni.

5.1 Zagotavljanje trga

Ljudje vidijo različna gonila razvoja in sprejetja PET na trgu (Privacy Enhancing Technologies, 2005, str. 32):

- ***Uporabniki PET***
 - Zavedanje javnosti glede zasebnosti predstavlja eno izmed glavnih gonil PET.
 - Veliko komercialnih organizacij vidi konkurenčno prednost tudi v PET, saj zagotavlja nudenje dobrih rešitev zasebnosti, kredibilnost in zaupanje.
 - Splošna občutljivost do SPAM-a in drugih vsiljivcev zasebnosti bo uporabnike še bolj spodbudila k uporabi PET in pristopov za varovanje zasebnosti.

- Podjetja, ki uporabljajo sisteme za upravljanje s strankami, prepoznavajo, da je kakovost podatkov veliko boljša pri podjetjih s politiko zasebnosti kot pri tistih, ki zbirajo katere koli podatke o strankah.
 - Napadi lažnega predstavljanja in tatovi zasebnosti so gonilo splošnega povpraševanja po PET, najpogosteje predvsem zaradi nevarnosti in strahu pred izgubo denarja.
 - Nekateri uporabniki menijo, da bi certifikacija lahko pomagala izbrati prave PET, medtem ko drugi predlagajo neke vrste javnih regulativ za opredelitev kdaj in kje je uporaba določene PET primerna ali celo zahtevana.
- ***Proizvajalci PET***
 - Večina dobaviteljev rešitev in storitev zasebnosti prepozna, da je slabo razumevanje v javnosti glede vprašanj in vrednosti zasebnosti pomembna ovira za njihovo uspešnost.
 - Dobavitelji čakajo na regulative s strani javnih ustanov, in skladnost z njimi bo nedvomno pomembno gonilo za boljše sprejetje PET.
 - Ocenjevanje tveganj zasebnosti pridobiva popularnost, kar bi nenazadnje lahko pripeljalo do večjega povpraševanja po PET.
 - ***Ustanove in PET***
 - Znaki zaupanja (npr. TRUSTe, BBBOnline itd.) so prepoznani kot glavno gonilo, saj omogočajo uporabniku lažje odločanje, včasih pa lahko vplivajo tudi na odločitve o javnih nakupih.
 - E-vladne iniciative bi lahko bile gonilo za rešitve zasebnosti, če bi se ustanove odločile za vključitev funkcij zasebnosti bodisi kot sestavni del bodisi kot možnost.

Boljše razumevanje vprašanj zasebnosti in uporaba ustreznih PET pri uporabnikih e-storitev je danes ključnega pomena za uspešnost na PET trgu. Trendi na tem področju so usmerjeni predvsem v:

- ***Demonstracijo projektov***

Veliko organizacij izvaja demonstracije projektov, kjer izvršujejo transakcije ali interakcije brez običajne identifikacije uporabnika in sicer z uporabo alternativnih načinov in tehnologij za vzpostavitev potrebne povezave v transakciji (npr. biometrija, pametne kartice itd.). Demonstracija projektov zasebnosti je relevantna za številne sektorje, kot so storitve na področju zdravstva, nakupovanja, investicij itd. Najbolj cenjeni so tisti, ki se začnejo z analizo in če je mogoče tudi s prenovitvijo poslovnega modela ter informacijskega toka transakcij.

- ***Raziskave o sprejetju***

Druga pomembna iniciativa je izvajanje raziskav v javnosti o percepcijah glede vprašanj in vrednosti zasebnosti. Tukaj imajo raziskave, ki vključujejo osebe z izkušnjami bistveno večjo težo kot navadne javnomnenjske raziskave. Najbolj cenjene so tiste, ki so opravljene v kombinaciji z izbrano demonstracijo projekta, kjer imajo sodelujoči neposredne izkušnje glede uporabe PET rešitev (npr. raziskava o sprejetju, ki je povezana z implementacijo P3P tehnologije na izbranih spletnih straneh ali storitvah).

- ***Vključitev zasebnosti pri pregledih***

Veliko ustanov že vrsto let izvaja enostavne preglede o prisotnosti politike zasebnosti na spletnih straneh. Zaradi vse večjega zavedanja glede vprašanj zasebnosti se predvideva, da se bo to preverjanje še naprej razvijalo (npr. ocenjevanje vsebine politike, preverjanje skladnosti storitve, ocenjevanje zahtevanih osebnih informacij z bogatostjo in uporabnostjo storitve).

- ***Rešitve zasebnosti znotraj podjetij***

Javne in zasebne organizacije se zavedajo vse večje odgovornosti do varovanja zasebnosti svojih strank ter zaposlenih. Upravljanje z identiteto in dovoljenji notranjih/zunanjih uporabnikov je tako postal pomemben del njihovih aplikacij in storitev, prav tako pa tudi vpeljava ustrezne politike zasebnosti pri ponudnikih storitev za njihovo zunanjo podobo. Predvideva se, da bodo tehnologije zasebnosti, ki jih ponujajo tretje osebe dosegale bistveno manjšo popularnost, saj so nekatere PET funkcionalnosti že vključene v mnoge standardne storitve. Kljub temu bodo te še vedno ključne pri storitvah brez PET funkcionalnosti ter za uporabnike, ki imajo malo zaupanja v ponudnike storitev.

Na mednarodnem področju potekajo številni projekti (iniciative), ki so neposredno povezani s PET in lahko vplivajo na dogajanja na PET trgu:

- ***Projekt platforma za preference zasebnosti (P3P)***

<http://www.w3.org/P3P/>

P3P je specifikacija, razvita s strani World Wide Web konzorcija (W3C). Ko je implementirana v spletne strani in spletne brskalnike, prinaša uporabnikom (ki želijo odločati, kdaj in pod kakšnimi pogoji bodo odkrili svoje osebne informacije) enostavnost in točnost. Čeprav P3P ne nudi varovanja zasebnosti, lahko znatno poveča transparentnost in se uporabi kot podpora ostalim prizadevanjem za izboljšanje varovanja zasebnosti.

- ***Projekt testiranja in ocenjevanja tehnologij za varovanje zasebnosti (PETTEP)***

<http://www.ipc.on.ca/>

PETTEP sestavlja globalna skupina strokovnjakov za zasebnost in varovanje podatkov, ki prihajajo tako iz vladnih kot gospodarskih organizacij in ki delajo na razvoju mednarodno sprejetih testnih in ocenjevalnih kriterijev za funkcije zasebnosti v informacijskih sistemih. Ta skupina zbira in strukturira primerna informacijske načela (FIP) ter jih uvršča v okvir skupnih kriterijev. Namen je izgradnja okvira za formalno ocenjevanje, lahko pa so tudi načela za snovanje rešitev zasebnosti.

- ***Avtorizacijski jezik zasebnosti za podjetja (EPAL)***

<http://www.zurich.ibm.com/csc/>

EPAL je formalni jezik za določevanje praks zasebnosti podjetja, ki ga je razvil IBM-ov inštitut za raziskovanje zasebnosti. Podjetja ponavadi obljubijo svojim strankam določeno stopnjo zasebnosti in sicer preko izjave zasebnosti ali platforme za preference zasebnosti (P3P). Jezik EPAL se lahko nato uporabi za izpolnjevanje omenjenih obljub. S samodejno vpeljavo specifičnih praks zasebnosti se podjetjem namreč omogoči, da delujejo v skladu z danimi obljubami.

- ***Projekt upravljanje z zasebnostjo in identiteto za Evropo (PRIME)***

<http://www.prime-project.eu.org/>

PRIME je evropski projekt, ki rešuje vprašanja povezana z upravljanjem digitalne identitete in zasebnostjo v informacijski družbi. Namen tega projekta je razviti koncepte in produkte na področju upravljanja identitet.

V prihodnosti bodo lastnosti zasebnosti najverjetneje vgrajene v IT infrastrukturo kot sestavni del aplikacijskih platform (npr. v operacijski sistem, sistem za upravljanje z bazami podatkov in razvojni model). To pomeni, da bodo današnji neodvisni ponudniki PET najverjetneje še naprej ostali obstranski igralci oziroma bodo v svoje lastne produkte in storitve vgrajevali tehnologije infrastrukturnih dobaviteljev.

5.2 Inovativno snovanje

Model in proces zasebnosti

Model zasebnosti, ki ga je razvil Benjamin Brunk, lahko predstavlja uporabno sredstvo za ocenjevanje prednosti in slabosti številnih orodij zasebnosti in varnosti. Na drugi strani lahko pomaga posameznikom tudi z nudenjem ustreznih orodij za sprejemanje premišljenih

odločitev, ko gre za njihovo zasebnost. Omenjeni model sestavlja pet kategorij, v katerih so lastnosti zasebnosti opisane glede na način varovanja (Tabela 5).

Tabela 5: Model zasebnosti

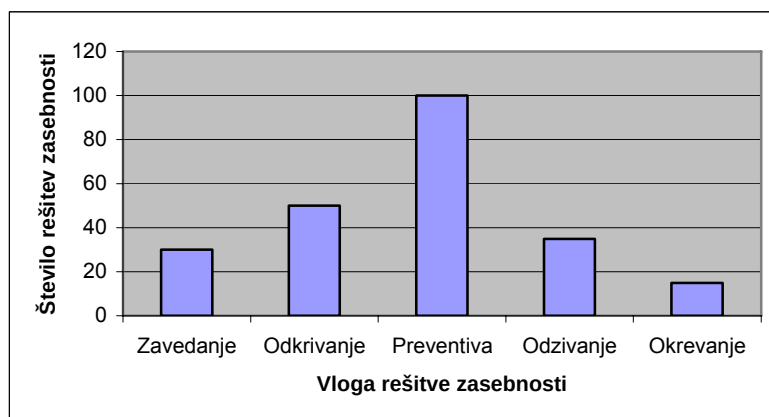
Kategorija	Opis
Zavedanje	Vse, kar priskrbi informacije brez potrebnega angažiranja uporabnika. Lastnosti so informativne in pomagajo uporabnikom pri nadzoru situacije.
Odkrivanje	Orodja ali lastnosti, ki preiščejo ali odkrivajo za možne probleme. Ta orodja pogosto delujejo v ozadju; iskalniki virusov in škodljivih vsebin.
Preventiva	Lastnost ali orodje, ki je uporabljeno kot previdnostni ukrep. Šifriranje ali digitalna potrdila so po naravi preventivna. Varno brisanje elektronskih dokumentov je dober primer preventivnih lastnosti.
Odzivanje	Izvajanje aktivnosti po odkritju problema je odzivanje. Primeri odzivanja vključujejo preklic ukradene kreditne kartice in blokiranje dohodnega mrežnega prometa od določenih IP naslovov.
Okrevanje	Lastnosti in orodja, ki uporabniku pomagajo vzpostaviti normalno stanje. Primer okrevanja je obnovitev zadnjega dobrega stanja in ponovna namestitve okvarjenih datotek.

Vir: Cranor Faith, Garfinkel, 2005, str. 410

Na osnovi razvitega modela opravljena raziskava o trenutno dostopnih rešitvah zasebnosti na spletu (npr. orodja, sistemi, storitve itd.), je pokazala naslednja dejstva in s tem povezane možnosti za nadaljnji razvoj (Cranor Faith, Garfinkel, 2005, str. 417–419):

- 19 % rešitev zasebnosti je vsebovalo le eno tipično lastnost zasebnosti, 47 % pa pet ali manj, kar je zgovoren dokaz o potrebi po kompleksnejših sistemih zasebnosti, ki bi vključevali več lastnosti zasebnosti. Prevladujoča kategorija med rešitvami zasebnosti je bila preventiva, najmanj pa okrevanje (Slika 30).
- Lastnosti zavedanja so sicer prisotne v rešitvah zasebnosti, vendar bi se dalo z njimi narediti še kaj več, saj je oskrba uporabnikov z znanjem ena izmed najboljših možnih obramb. Datoteke pomoči tu predstavljajo minimum za doseganje osnovnega zavedanja. V uporabnikov vmesnik bi lahko bile vgrajene boljše lastnosti zavedanja za pomoč pri sprejemanju odločitev (npr. podobne rešitve kot so pop-up sporočila, grafični merilniki).
- Današnje rešitve zasebnosti imajo zelo malo lastnosti odzivanja in okrevanja. Okrevanje je glavni problem v zasebnosti, saj ko se določeno informacijo posreduje in je ta zlorabljena, ni več poti nazaj. Tudi če imajo rešitve zasebnosti določena orodja za odzivanje in okrevanje, jih ta ponavadi ne vgradijo dovolj dobro v orodje kot celoto.

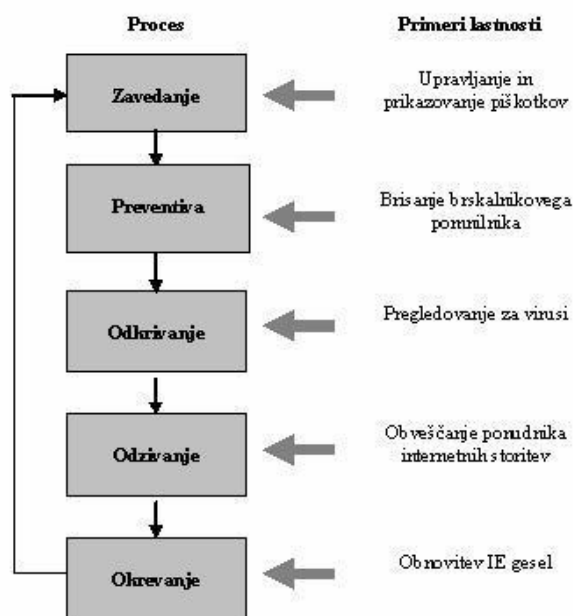
Slika 30: Kategorizacija trenutno dostopnih rešitev zasebnosti



Vir: Cranor Faith, Garfinkel, 2005, str. 418

Avtor predlaga, da se na zasebnost gleda bolj naravno in sicer kot na stalno odvijajoči se proces, upoštevajoč pri tem razviti model (Slika 31), v katerem univerzalno rešitev zasebnosti predstavljajo tiste rešitve, ki nudijo lastnosti za vsako izmed petih kategorij (predpostavka, da so kompleksnejše rešitve boljše in da dajejo uporabniku več nadzora nad zasebnostjo). Proces se začne s splošnim zavedanjem potreb in vprašanj glede zasebnosti ter vključuje povratne informacije od vsake nadaljnje stopnje, kar izboljša znanje uporabnika in s tem sposobnost sprejemanja zavestnih odločitev.

Slika 31: Proces zasebnosti



Vir: Cranor Faith, Garfinkel, 2005, str. 414

Zasebnost in HCI

HCI je podpodročje računalniške znanosti, ki preučuje interakcijo ljudi z računalniki, njegove korenine pa segajo v začetek 80. let s pojavom osebnih računalnikov in enouporabniških vmesnikov. Od takrat se je veda razširila še na metodologije snovanja, uporabnosti,

inteligentnih vmesnikov, prilagodljivih vmesnikov itd. V širšem kontekstu HCI ne obravnava samo procesov (npr. kako so sistemi uporabljeni, snovani in razviti) in produktov (npr. sistemov in njihovih vmesnikov), ampak tudi poglede (npr. kulturne in organizacijske kontekste, ki podpirajo oziroma onemogočajo razvoj sistemov ali kako drugače vplivajo nanje). Zasebnost tako kot varnost vključuje vse zgoraj naštetе nivoje. Poznavanje uporabnikov in njihovega pogleda na računalniške sisteme lahko bistveno izboljša mehanizme zasebnosti.

Znotraj HCI je kar nekaj znanstvenih smernic, ki so neposredno zanimive za raziskovanje zasebnosti in snovanje mehanizmov zasebnosti (Cranor Faith, Garfinkel, 2005, str. 384):

- Razmislek o osnovni zasnovi – snovanje, namenjeno splošni uporabnosti in ocenjevanju uporabnosti (uporabnosti inženiring)

Zadnjih 20 let je bilo vloženega veliko zanimanja in truda v izboljšanje uporabnosti računalnikov. Danes je splošno znano dejstvo, da tudi moderna programska oprema ne sme ignorirati uporabnosti, saj v nasprotnem primeru potencialni uporabniki ne bodo sprejeli ali uporabljali lastnosti, ki so pretežavne za uporabo. Reševanje zahtev po uporabnosti je tako postal pomemben del večine razvojnih metodologij (npr. pri razvoju programov se je to vključilo v prototipiranje). Vse to skupaj prepoznava potrebo po snovanju, razvoju in testiranju skupaj z uporabniki z namenom, da se zgradi uporabne sisteme.

Mehanizmi zasebnosti pri tem niso nobena izjema, saj se jih lahko obravnava v številnih pogledih kot katero koli drugo kritično lastnost platforme ter se jih rešuje z obstoječimi metodami uporabnostnega inženiringa (npr. kontekstualno snovanje, protokoli glasnega razmišljanja, nizko in visoko dodelani prototipi itd.).

- Kako ljudje sodelujejo med seboj s pomočjo in preko sistemov (računalniško podprto kooperativno delo – CSCW)

Pomembna veja HCI je računalniško podprto kooperativno delo, ki se je začelo v poznih 80. letih. Sprva je vključevalo le razmišljanja o kooperativnem delu, kasneje pa tudi različne oblike koordiniranja in družbene organiziranosti. Večina začetnega dela na CSCW je enostavno prezrla vprašanja zasebnosti: raziskovalci so namreč predvidevali, da ljudje, ki delajo skupaj na projektu nimajo nobenih razlogov za skrivanje informacij drug pred drugim. Zanimanje CSCW raziskovalcev na področju zasebnosti se je začelo s pojavom stranskih učinkov dela med oddaljenimi prostori, ki so bili elektronsko povezani preko zvoka in videa.

Mehanizmi zasebnosti se soočajo s problemom različnega pogleda ljudi na interakcije z drugimi ljudmi (odvisno od okoliščin v katerih se znajdejo, se ti velikokrat različno predstavijo). CSCW raziskave, ki so pomembne za zasebnost se lahko na grobo delijo

v tri kategorije (medijsko prostorske aplikacije, kolaborativne aplikacije, ki se nanašajo na zasebnost in študije zasebnosti v povezavi z zavedanjem).

- Kako se posamezniki razlikujejo v svojih sposobnostih in kako to vpliva na vmesnik človek – računalnik (individualne razlike in toleriranje)

Številne raziskave so pokazale, da posamezniki ne gledajo enako na zasebnost in to velja tudi pri e-trgovanju. Vrsta in stopnja skrbi segmentira populacijo v različne skupine (zagovorniki zasebnosti, zaskrbljeni v manjši meri in pragmatiki).

- Vloga HCI pri naslednji generaciji arhitektur (vsesplošno računalništvo – ubicomp)

Trenutno obstaja velik interes HCI znanosti v raziskovanju vsesplošnega računalništva še posebej na področju resničnostnih aplikacij (kjer digitalni svet prevlada nad fizičnim), senzorno zasnovani zabavi (geo-igrice) in uporabnikom osredotočenih vmesnikov za »ubicomp« prostore. V okoljih vsesplošnega računalništva obstaja resna zaskrbljenost glede zasebnosti, saj lahko nameščeni senzorji spremljajo posameznika v okolici ter med drugim brez vsakršnega obvestila ali privolitve zbirajo celo osebne podatke.

Raziskave na področju vsesplošnega računalništva so šele na začetku, vendar pričakujemo, da bodo čez čas dodale svoj prispevek k mehanizmom zasebnosti.

Kritični dejavniki snovanja zasebnosti

Kljub pridobljenim izkušnjam iz opravljenih raziskav (ankete, intervjuji, analize itd.) in znanju snovanja je za mnoge ljudi upravljanje z zasebnostjo v sistemih še vedno pretežavno. V veliki meri je to zaradi zasnove teh sistemov, ki uporabnikom preprečujejo razumevanje zasebnosti med njeno uporabo, kot tudi izvajanje smiselnih aktivnosti preko njih. Čeprav se določeni kritični dejavniki pojavljajo zelo pogosto, jih veliko sistemov še vedno ne upošteva. Nekateri od teh sistemov (npr. spletni brskalnik) so povzročili veliko polemik glede zasebnosti, medtem ko so se drugi temu uspešno izognili (npr. takojšnje sporočanje) ter doživeli velik komercialni ali družbeni uspeh. Kritične dejavnike lahko delimo na tiste, ki primarno vplivajo na uporabnikovo razumevanje zasebnosti v sistemu, in na tiste, ki primarno vplivajo na sposobnost sprejemanja smiselnih aktivnosti preko sistema (Lederer et al., 2004, str. 441).

- Razumevanje
 - Zapostavljanje možnega toka informacij

Snovalci ne bi smeli spregledati narave in obsega možnega odkritja informacij s strani sistema. Uporabniki lahko zavestno uporabljajo sistem le v primeru, ko popolnoma razumejo namen vključene zasebnosti. Ti nameni so vrsta posredovanih informacij,

komu se posredujejo, medij po katerem se posredujejo, dolžina zadrževanja, možnost nenamernega odkritja, prisotnost opazovalcev (tretjih oseb) in zbiranje meta informacij. Razjasnitev možnosti sistema po posredovanju osebnih informacij je ključnega pomena za uporabnike, da lahko predvidijo posledice njegove uporabe.

– *Zapostavljanje dejanskega toka informacij*

Snovalci ne bi smeli prikrivati dejanskega odkritja informacij preko sistema. Uporabniki bi morali razumeti, katere informacije so se odkrile in kateri osebi. Odkritje bi jim moralo biti nemudoma sporočeno, če to ne bi bilo mogoče, pa bi se jim moralo posredovati vsaj obvestilo v razumnem času. Povratna informacija naj bi uporabnike zadostno informirala, vendar ne preobremenila oziroma odvrnila od njihovega trenutnega dela.

• Aktivnosti

– *Poudarjanje nastavitve nad aktivnostmi*

Snovalci naj ne bi zahtevali preobsežnega nastavljanja v sistemu, za izgradnjo in upravljanje z zasebnostjo. Uporabnikom bi morali omogočiti prakticiranje zasebnosti kot naravno posledico njihove vključenosti v sistem. Nastavljanje zasebnosti je neuspešno zaradi vsaj dveh razlogov. Prvi je ta, da uporabniki pri tem ravnajo povsem intuitivno, drugi pa ta, da se je z nastavljanjem preferenc prelahko oddaljiti od konteksta v katerem se te uporabljajo. Na splošno ljudje ne nastavljajo tako, da bi eksplicitno zavarovali zasebnost, ampak rajši sodelujejo v določenih aktivnostih, ki so že podprte z regulativami zasebnosti.

– *Pomanjkanje trde-mehke kontrole*

Snovalci ne bi smeli spregledati učinkovitega mehanizma za zadrževanje in posredovanje informacij. Uporabniki so navajeni izključiti zadevo s pomočjo trdih kontrol (npr. gumb za vklop-izklop) ko želijo, da se določena operacija prekine. Poleg tega bi se lahko v nekaterih primerih uporabile tudi mehke kontrole (npr. drsniki za uravnavanje stopnje). Trde-mehke kontrole je ponavadi enostavno vpeljati in pogosto odražajo dejansko stanje z neposrednimi povratnimi odgovori, s čimer osvobajajo uporabnika od razmišljanja o tem, ali je preference nastavil pravilno.

– *Omejevanje uveljavljenih praks*

Snovalci naj ne bi ovirali uporabnikov pri prenosu že uveljavljenih družbenih praks na razvijajoče se tehnologije. Medtem, ko lahko v prvih zasnovah primanjkuje ustrezne podpore za nujne primere, ker se ustrezna praksa še ni mogla razviti pred vpeljavo novega sistema, bi se morali ti izogibati vsaj omejevanju uveljavljenih družbenih praks. S podpiranjem vlog, pričakovanj in praks, ki se uporabljajo v okolju v katerega

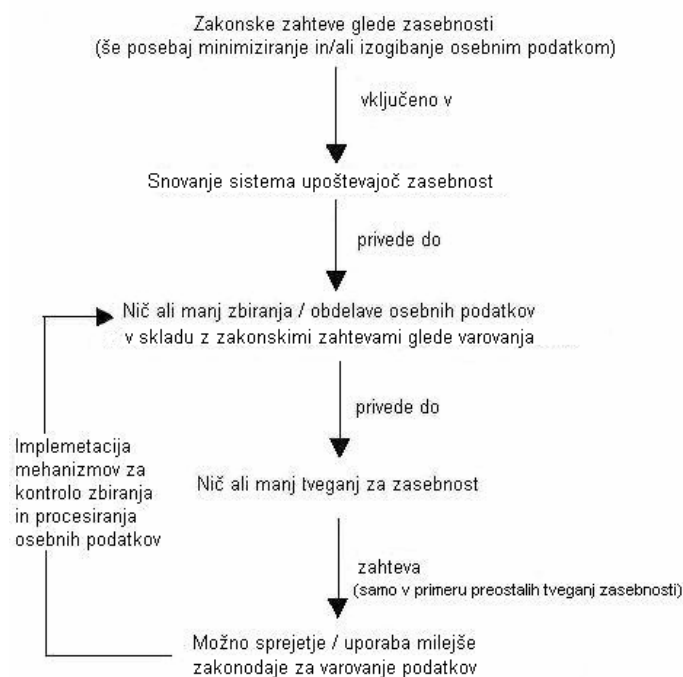
bo nov sistem vpeljan, lahko snovalci akumulirajo naravna prizadevanja uporabnikov po prenosu obstoječih veščin na nove medije.

5.3 Izobraževanje javnosti

Izobraževanje o zasebnosti in njihovih tehnologijah je zelo pomembno za dvig zavesti in kompetenc snovalcev sistemov, IT strokovnjakov za varnost in management ter uporabnikov interneta (Fischer Hübner, Lindskog, 8. 1. 2007).

Snovalci sistemov bi morali biti odgovorni za zakonsko dovoljen in etično sprejemljiv način snovanja sistemov, zaradi česar bi morali znati oceniti tveganja zasebnosti v IT/komunikacijskih sistemih ter poznati osnovne koncepte tehnologij za varovanje zasebnosti. Uporabniki ponavadi ne sodelujejo v procesu snovanja sistema, kar pomeni, da ne morejo izraziti svojih interesov in pravic glede zasebnosti, zato je zelo pomembno, da jih snovalci sistemov predhodno primerno obravnavajo. Tako kot pri kontrolah varnosti, je ključnega pomena, da so razvijajoče se kontrole zasebnosti upoštevane že na začetku in da so vgrajene v zasnovo sistema (slika 32).

Slika 32: Izogibanje tveganjem zasebnosti z njeno vgraditvijo v sistem



Vir: Fischer Hübner, Lindskog, 8. 1. 2007

Kompetence na področju PET so izrednega pomena za IT varnostne strokovnjake in menedžerje zaradi naslednjih razlogov:

- povečane potrebe potrošnikov po zasebnosti in produktih zasebnosti,
- nastanek novega in verjetno rastočega trga PET,
- PET so postale popularno raziskovalno področje.

Nekatere PET niso nujno najbolj učinkovito sredstvo za vpeljavo zasebnosti, razen če imajo uporabniki poglobljeno tehnično znanje o njihovi uporabi. Orodja za šifriranje so primeri takih tehnologij, ki se pogosto znajdejo le v rokah posameznikov. Zaradi tega potrebujejo uporabniki interneta dodatna izobraževanja o pravicah in tveganjih zasebnosti ter o možnostih samovarovanja z uporabo PET. Nenazadnje je ključnega pomena, da se podobna izobraževanja vpelje in izvaja še:

– *na univerzah*

Za povečanje kompetenc računalniških strokovnjakov na področju PET bi se moralo ponuditi dodatna izobraževanja v okviru učnih programov računalniške ali systemske smeri. Ker so ponavadi PET implementirane skupaj z drugimi bolj varnostnimi mehanizmi (npr. kriptografski protokoli), naj bi se omenjena izobraževanja izvajala znotraj predavanj o IT varnosti. Med drugim nobena izmed znanih knjig o računalniškem varovanju ne vsebuje pomembnih vidikov PET. Obstajajo sicer določene knjige o kriptografiji, ki na kratko obravnavajo PET, in še nekaj drugih, ki obravnavajo bolj specifične vidike zasebnosti in PET. Zato bi moral seznam literature, ki je namenjen PET tečajem, obvezno vključevati tudi članke iz časopisov, konferenčne papirje in tehnična poročila;

– *v gospodarstvu*

Menedžerji in prodajalci na internetu so se začeli zavedati dejstva, da je zasebnost spletnim uporabnikom vse pomembnejša. Lep primer tega je velika količina spletnih strani, ki imajo že objavljeno politiko zasebnosti. Vendar podrobno branje razkrije, da zasebnost spletnega uporabnika kljub vsemu ni bila spoštovana. Prav tako ni povsem znano, koliko od teh izjav se dejansko izvaja, ali kako se zagotavlja anonimno zbiranje podatkov. To lahko povzroči spletnemu uporabniku nemalo težav pri odločanju, ali je uporabljena tehnologija vredna zaupanja in ali učinkovito varuje zasebnost. Zaradi tega je zelo pomembno širiti kompetence tudi med ljudmi, ki razvijajo produkte ali strani za internet. Predlaga se ločena izobraževanja in sicer za produktne in linijske menedžerje, specialiste ter snovalce.

5.4 Standardizacija zasebnosti

Da bi dosegli masovno uporabo in merljivost PET v informacijskih sistemih, je potrebno standardizirati principe zasebnosti, ki so vsebovani v direktivah EU ter primernih informacijskih načelih. Raziskava tehnične univerze v Dresdnu je pokazala, da standardizacija zasebnosti ne vodi samo do znatnega zmanjšanja stroškov, ampak tudi do zmanjšanja tveganj v raziskavah in razvoju. Pokazalo se je tudi, da imajo standardi kot oblika tehnološkega transferja pozitiven vpliv na inovativnost ter da družbeno pomembni standardi vodijo do umika standardov in praks, ki so preživeli tehnično, znanstveno ali družbeno vrednost. Standardi zasebnosti bi med drugim promovirali tudi vgrajeno varovanje ter izločevali

produkte in storitve, ki bi vodili do groženj zasebnosti. Prav tako bi spodbujali in odprli trge za nove produkte in storitve z vgrajenim varovanjem zasebnosti.

Poleg tega obstaja še več razlogov, zakaj so standardi zasebnosti potrebni in zakaj je zelo pomembno, da se spoprimemo z izzivom razvoja celovitih standardov (Borking J., 3. 10. 2005):

- ***Zmanjšanje stroškov globalnega prilagajanja***

Domena zasebnosti je v številnih državah po svetu zelo hitro postala zakonsko urejeno področje. Posledica tega je bilo sprejetje množice nacionalnih zakonodaj, ki so na globalni ravni povzročile stroške, povezane s prilagajanjem. EU je to težavo rešila z direktivami zasebnosti, s katerimi je poenotila zakonodaje med svojimi članicami. Kljub temu je zunaj njenih meja ostalo še vrsto drugih zakonodaj, ki so nekje bolj nekje pa manj podobne omenjenim direktivam. Pri izgradnji globalnih standardov bi se morala zakonodaja razbiti na ključne komponente, ki bi jih lahko uporabile kot osnovo za pisanje modela za standarde zasebnosti.

- ***Zmanjšanje tveganj razvoja novih tehnologij***

Standardi zasebnosti so nujni, da se zagotovi obvladovanje stroškov pri razvoju novih tehnologij in da se vzpostavi okolje, v katerem lahko inovativne rešitve razvijajo tako mala in srednja kot velika podjetja. Standardi so tudi ključnega pomena, da razvijalci novih tehnologij dobijo orodja, ki jih potrebujejo pri ustvarjanju produktov in storitev (rešitev). Razvoj tehnologije v okolju, ki nima določenih standardov je zelo tvegano, saj so razvijalci in prodajalci prepuščeni ugibanjem pri razlaganju zakonodaje. V primeru nepravilne odločitve je lahko njihova tehnologija neustrezna, posledično pa so viri neupravičeno porabljeni. Nenazadnje standardi zasebnosti zmanjšujejo potreben čas za prihod na trg, saj se lahko razvijalci zanesejo na globalne standarde in tako ne zapravljajo svojega časa ali virov za razvijanje lastnih standardov.

- ***Povečanje prostovoljnega prilagajanja***

Prostovoljno prilagajanje je nujno potrebno pri implementiranju zakonodaje. Vendar je to še posebej težavno za proizvajalce na področju tehnologij, upoštevajoč pri tem kompleksnost razumevanja številnih aplikacij številnih zakonodaj. Pisci zakonov lahko tu pomagajo s promoviranjem in omogočanjem prostovoljnega prilagajanja preko razvoja podrobnih in celovitih standardov ter vodičev. Prilagajanje se lahko nenazadnje pospeši tudi z zmanjšanjem stroškov pri implementiranju.

- ***Premišljeno vodenje omejenih virov***

Premišljeno vodenje na področju tehnologij zasebnosti je nujna sestavina za implementacijo masovne uporabe in sprejetja PET. Za razliko od ostalih razvijajočih se tehnologij obstaja na področju PET resno pomanjkanje virov in znanja. Da bi se zagotovilo pravilno in primerno pisanje tehnoloških standardov za PET, je treba zagotoviti kritično maso znanja in virov. V nasprotnem primeru bi lahko razvoj omenjenih standardov pripeljal do promocije standardov, ki ne dosegajo zakonsko predpisanih zahtev.

- ***Odprava stroškov prilagajanja***

Stroški prilagajanja so lahko ogromni, če mehanizmi prilagajanja niso v celoti in podrobno opredeljeni. Trenutno obstaja namreč zelo malo zakonov oziroma če sploh kakšen, ki opredeljuje, kako so lahko tehnološke rešitve implementirane, da se bo hkrati zadostilo tudi zakonskim zahtevam. Standardi PET bodo tu nudili standarde za prilagajanje in tako zmanjšali stroške prilagajanja.

6 RAZISKAVA O ZASEBNOSTI MED UPORABNIKI INTERNETA

S tem poglavjem skušam predstaviti in posredovati celovito sliko o zasebnosti med uporabniki interneta v slovenskem prostoru. Opravljena empirična raziskava služi kot spremljajoči vir predhodnim poglavjem, v katerih so bila predstavljena vprašanja, povezana z zasebnostjo v informacijski družbi in prizadevanja za njeno učinkovito varovanje. Nenazadnje lahko to raziskavo uporabimo tudi kot osnovo za nadaljnje podobne raziskave v javnosti. Poudariti pa moram, da je treba zaradi manjšega števila vzorca določene ugotovitve jemati s previdnostjo.

6.1 Namen in cilji raziskave

Namen raziskave je preveriti zavedanje uporabnikov interneta o zasebnosti, kako se ti obnašajo na internetu, ter katere pristope in tehnologije za varovanje zasebnosti uporabljajo. Cilj raziskave je pokazati uporabnikom interneta, da varovanje njihove zasebnosti ni zgolj domena tretjih oseb, kot so vladne ustanove ali organizacije, ampak da lahko pri tem tudi sami aktivno sodelujejo.

6.2 Načrt raziskave

Oprelitev pridobljenih podatkov

Odločil sem se za pridobivanje primarnih podatkov, ki sem jih zbral zgolj za ta namen. Pri načrtovanju raziskave sem se opiral tudi na sekundarne podatke, ki so mi bili v pomoč pri

oblikovanju cilja raziskave, pri oblikovanju uvodoma postavljene hipoteze in pri sestavljanju vprašalnika. V svojih ugotovitvah pri interpretiranju rezultatov sem se opiral na podatke, ki sem jih pridobil v raziskavi.

Raziskovalna metoda

Primarne podatke sem zbral z raziskovalno metodo anketiranja in sicer s pomočjo pripravljenega vprašalnika (Priloga 1). Ta je bil zaprtega tipa, v obliki ocenjevalnih lestvic.

Raziskovalni inštrument

Pri sestavljanju vprašalnika sem se zgledoval po podobnih že opravljenih raziskavah ter strokovni literaturi, ki obravnava zasebnost na internetu. Vprašalnik sestavlja 27 trditev, ki sem jih razdelil v tri vsebinske sklope. Vprašanja si sledijo v logičnem zaporedju od bolj splošnih proti bolj zahtevnim, in pri katerih je moral anketiranec svoje strinjanje oziroma nestrinjanje s trditvami razvrstiti od 1 do 5. Pri tem je vrednost 1 pomenila, da se s trditvijo v celoti ne strinja, vrednost 5 pa, da se s trditvijo v celoti strinja.

Prvi vsebinski sklop se nanaša na zavedanje uporabnikov interneta o zasebnosti. Trditve so vključevale predvsem splošna prepričanja povezana z zasebnostjo na internetu in s pridobivanjem informacij.

Drugi vsebinski sklop se nanaša na obnašanje uporabnikov na internetu. Trditve so vključevale predvsem upoštevanje že uveljavljenih dobrih praks in glede ostalih navad pri njihovem navigiranju po internetu.

Tretji vsebinski sklop se nanaša na uporabo pristopov in tehnologij za varovanje zasebnosti pri uporabnikih interneta. Trditve so vključevale predvsem uporabo pristopov v okolju oken (spletni brskalnik in poštni odjemalec) in uporabo tehnologij za varovanje zasebnosti (programi in sistemi).

Načrt vzorčenja

Ciljno populacijo sem določil na podlagi konec leta 2004 opravljene RIS-ove raziskave »Uporaba interneta«. Pri sestavi vzorca sem se osredinil na osebe, ki uporabljajo internet dnevno ali skoraj vsakodnevno, kar je predstavljalo $n = 100$ oseb. Kot usmeritev sem uporabil sorazmerne deleže za posamezne kategorije, predstavljene v spodnji tabeli (spol, starost), medtem ko sem izobrazbo razdelil le v tri skupine (srednja šola 44 %, visoka šola 30 %, šolajoči dijaki in študentje 26 %).

Tabela 6: Demografske značilnosti uporabnikov in neuporabnikov interneta v Sloveniji

		Uporablja internet vsak dan ali skoraj vsak dan	Uporablja internet tedensko in manj kot skoraj vsak dan	Uporablja internet mesečno ali redkeje in manj kot tedensko	Uporabniki interneta	Neuporabniki interneta	Skupaj
SPOL	Moški	56,2 %	53,0 %	49,3 %	54,1 %	43,7 %	49,9 %
	Ženski	43,8 %	47,0 %	50,7 %	45,9 %	56,3 %	51,6 %
	Skupaj	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %
STAROST	Do 19	16,3 %	33,6 %	28,3 %	23,3 %	5,4 %	20,0 %
	20 do 29	31,3 %	22,2 %	19,7 %	26,8 %	6,5 %	22,3 %
	30 do 49	40,4 %	36,0 %	42,7 %	39,5 %	31,2 %	36,4 %
	Nad 49	12,1 %	8,2 %	9,3 %	10,5 %	56,8 %	50,4 %
	Skupaj	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %
IZOBRAZBA	Nedokončana OŠ	0,4 %	0,0 %	1,3 %	0,4 %	8,7 %	10,3 %
	Osnovna šola	1,5 %	4,8 %	4,4 %	2,9 %	32,4 %	31,2 %
	Poklicna šola	13,1 %	21,5 %	29,9 %	18,2 %	33,4 %	26,7 %
	Srednja šola	29,1 %	24,3 %	23,1 %	26,8 %	16,7 %	24,0 %
	Višja in visoka šola	29,8 %	12,0 %	8,9 %	21,2 %	3,8 %	17,5 %
	Šolajoči	26,1 %	37,4 %	32,5 %	30,4 %	5,0 %	25,8 %
	Skupaj	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %	100,0 %
	N	673	361	195	1,229	1,133	2,362

Vir: [URL:http://www.ris.org/uploadi/editor/uporaba_interneta_2004_15.rar], 8. 9. 2006, str.

49

Oblika komuniciranja

Pri izvedbi ankete sem v manjši meri izbral osebni stik (pri sorodnikih), v večji meri pa neosebni stik in sicer s posredovanjem vprašalnika prijateljem, njihovim prijateljem in znancem ter s posredovanjem e-pošte naključnim osebam. Za ta pristop sem se odločil predvsem zaradi zamudnosti pri osebnem stiku in v izogib hitremu odgovarjanju s strani anketirancev na večje število vprašanj.

Omejitve in možne napake

Raziskava z vprašalnikom je zajela populacijo polnoletnih oseb in to ne glede na področje zaposlitve oziroma šolanja. Ker je informatika kot znanost precej zahtevna za razumevanje, sem poskušal v vprašalniku postavljene trditve kar najbolj poenostaviti in jih prilagoditi znanju običajnih uporabnikov interneta. Prav tako sem vprašalnik pred tem preizkusil na določenem številu oseb z namenom, da bi v nadaljevanju pridobil čim bolj točne podatke.

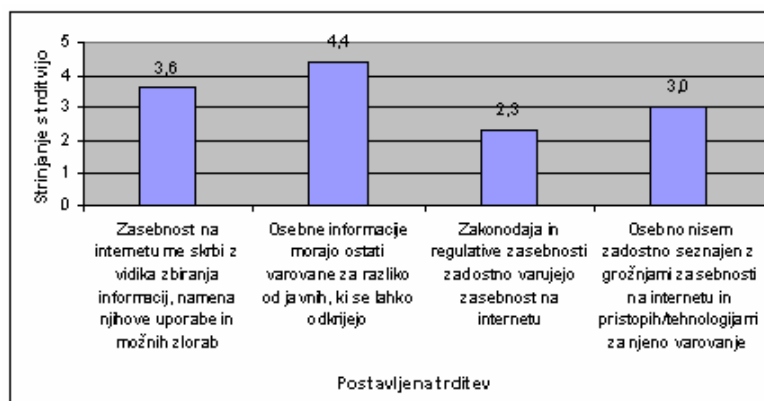
6.3 Rezultati raziskave in njihova interpretacija

Podatke, ki sem jih dobil z anketiranjem, sem računalniško obdelal v programu Microsoft Excel 2000. Podatke sem razvrstil in jih nato uredil, analizo podatkov ter interpretacijo rezultatov pa podajam v nadaljevanju.

6.3.1 Zavedanje uporabnikov o zasebnosti

Pri trditvah glede prepričanj o zasebnosti (Slika 33), so se uporabniki interneta večinoma strinjali, da jih zasebnost na internetu skrbi z vidika zbiranja informacij, namena njihove uporabe in možnih zlorab ter da morajo biti osebne informacije (npr. ime, naslov, e-pošta, telefonska številka itd.) varovane, javne pa se lahko odkrijejo. Manj so se strinjali, da zakonodaja in regulative zadostno varujejo njihovo zasebnost na internetu, pretežno pa, da niso zadostno seznanjeni z grožnjami zasebnosti na internetu ter pristopi in tehnologijami za njeno varovanje.

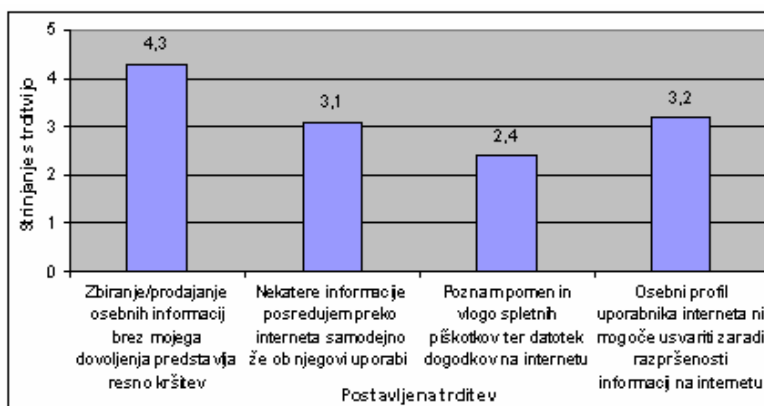
Slika 33: Prepričanja uporabnikov interneta glede zasebnosti



Vir: Vprašalnik; Zavedanje o zasebnosti na internetu

Pri trditvah glede prepričanj o pridobivanju informacij na internetu (Slika 34), so se uporabniki interneta večinoma strinjali, da zbiranje in prodajanje osebnih informacij med podjetji in državnimi ustanovami brez njihovega dovoljenja predstavlja resno kršitev. Pretežno so se strinjali, da nekatere informacije preko interneta posredujejo samodejno že ob njegovi uporabi (npr. IP naslov računalnika, vrsto operacijskega sistema, naslov predhodne spletne strani itd.) ter da osebni profil uporabnika interneta ni mogoče ustvariti zaradi odprte narave interneta in posledične razpršenosti informacij. Manj pa so se strinjali, da poznajo pomen in vlogo spletnih piškotkov ter datotek dogodkov na internetu.

Slika 34: Prepričanja uporabnikov interneta glede pridobivanja informacij

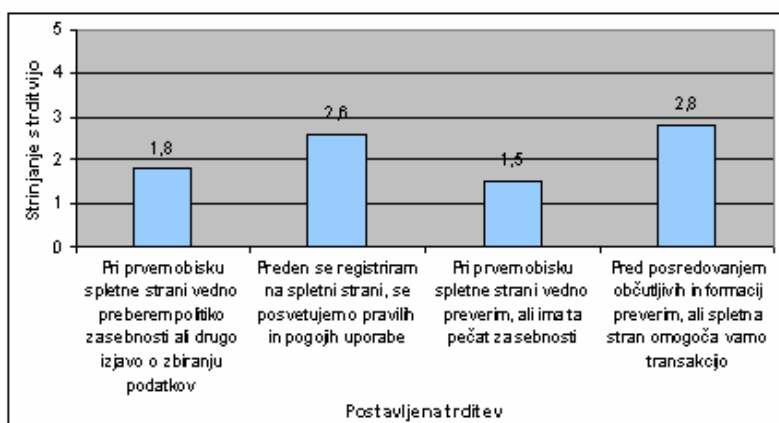


Vir: Vprašalnik; Zavedanje o zasebnosti na internetu

6.3.2 Obnašanje uporabnikov na internetu

Pri trditvah glede upoštevanja dobrih praks pri navigiranju po internetu (Slika 35), so se uporabniki interneta v manjši meri strinjali, da pri prvem obisku spletne strani preberejo politiko zasebnosti ali drugo izjavo o zbiranju osebnih informacij ter da preverijo ali ima spletna stran pečat zasebnosti (npr. certifikat Trustee). Pretežno so se strinjali, da se pred registracijo na spletni strani (npr. ustvarjanje uporabniškega računa) posvetujejo o pravilih in pogojih uporabe ter da pred posredovanjem občutljivih informacij (npr. EMŠO, številka zdravstvene in bančne kartice itd.) preverijo, ali spletna stran omogoča varno transakcijo (npr. certifikat VeriSign).

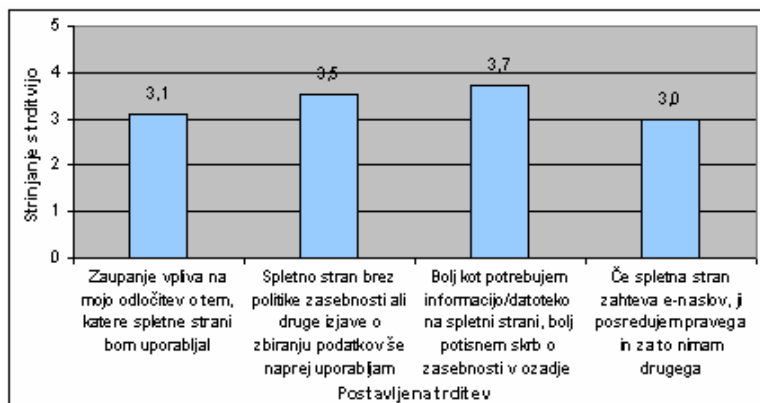
Slika 35: Upoštevanje dobrih praks med uporabniki interneta pri navigiranju



Vir: Vprašalnik; Obnašanje na internetu

Pri trditvah glede ostalih navad pri navigiranju po internetu (Slika 36), so se uporabniki interneta pretežno strinjali, da zaupanje vpliva na njihovo odločitev o tem, katere spletne strani bodo uporabljali, ter da spletni strani posredujejo svoj pravi e-naslov kadar to zahteva in za to nimajo drugega. Večinoma so se strinjali, da bolj kot potrebujejo informacijo ali datoteko na določeni spletni strani, bolj so pripravljeni potisniti skrb o zasebnosti v ozadje in da spletno stran brez politike zasebnosti ali druge izjave o zbiranju podatkov ponavadi še naprej uporabljajo.

Slika 36: Ostale navade med uporabniki interneta pri navigiranju

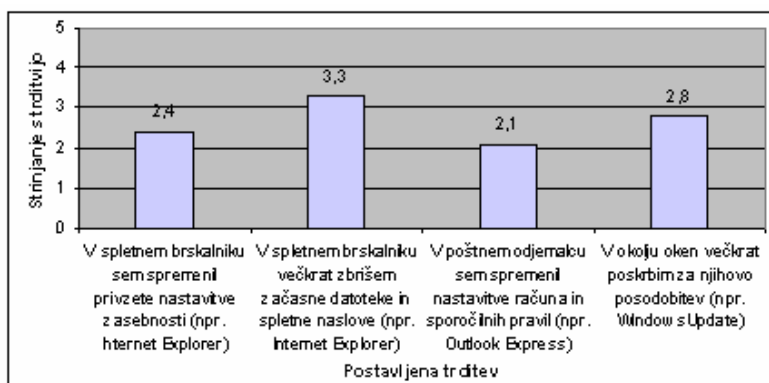


Vir: Vprašalnik; Obnašanje na internetu

6.3.3 Uporaba pristopov in tehnologij za varovanje zasebnosti

Pri trditvah glede uporabe pristopov v okolju oken (Slika 37), so se uporabniki interneta v manjši meri strinjali, da so v spletnem brskalniku spremenili privzete nastavitve zasebnosti (sprejemanje in zavračanje spletnih piškotkov) in da so v poštnem odjemalcu spremenili privzete nastavitve za e-pošto (varni prenos in filtriranje pošte) svojim potrebam varovanja. Pretežno so se strinjali, da večkrat poskrbijo za posodobitev okolja oken z varnostnimi in servisnimi paketi ter da zbrisejo začasne datoteke (spletni piškotki in datoteke) in spletne naslove v mapi zgodovina.

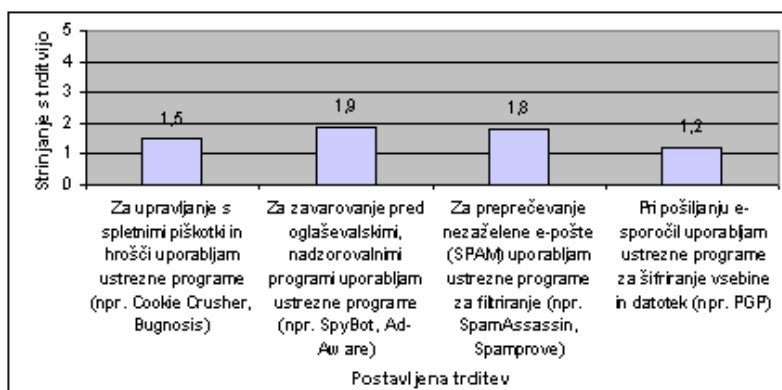
Slika 37: Uporaba pristopov v okolju oken pri uporabnikih interneta



Vir: Vprašalnik; Uporaba pristopov in tehnologij za varovanje zasebnosti na internetu

Pri trditvah glede uporabe klasičnih PET programov (Slika 38), so se uporabniki interneta v manjši meri strinjali (ali pa sploh ne), da uporabljajo ustrezne programe za upravljanje s spletnimi piškotki in hrošči, za zavarovanje pred Spywerom (oglaševalskimi, nadzorovalnimi in zlonamernimi programi), za filtriranje nezaželene e-pošte (SPAM) ter za šifriranje besedila in datotek pri pošiljanju e-sporočil, z namenom preprečevanja vpogleda v vsebino tretjim osebam.

Slika 38: Uporaba klasičnih PET programov pri uporabnikih interneta

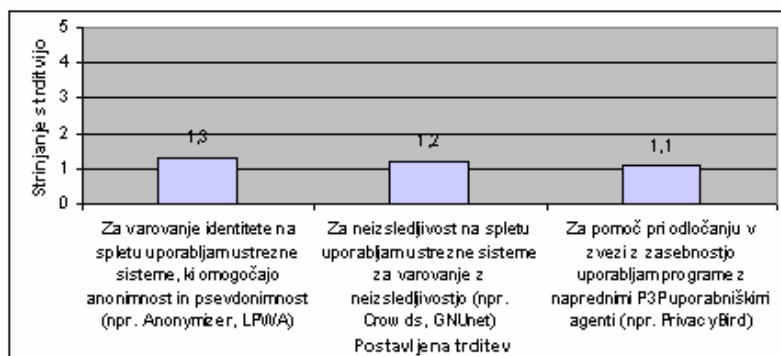


Vir: Vprašalnik; Uporaba pristopov in tehnologij za varovanje zasebnosti na internetu

Pri trditvah glede uporabe naprednih PET sistemov in programov (Slika 39), se uporabniki interneta v celoti niso strinjali, da uporabljajo ustrezne sisteme za varovanje identitete, za

varovanje z neizsledljivostjo ter ustrezne programe, ki vsebujejo napredne P3P uporabniške agente.

Slika 39: Uporaba naprednih PET sistemov in programov pri uporabnikih interneta



Vir: Vprašalnik; Uporaba pristopov in tehnologij za varovanje zasebnosti na internetu

6.4 Ugotovitve raziskave

Raziskava je pokazala, da uporabnike zasebnost na internetu na splošno skrbi z vidika zbiranja informacij, njihove uporabe in možnih zlorab, ter da pričakujejo, da so osebne informacije varovane, javne pa se lahko odkrijejo. Prepričani so tudi, da zakonodaja in regulative trenutno ne varujejo zadostno njihove zasebnosti na internetu. Na drugi strani sporočajo, da niso zadostno seznanjeni z obstoječimi grožnjami zasebnosti na internetu ter s pristopi in tehnologijami za njeno varovanje. Če podjetja ali državne ustanove zbirajo in prodajajo njihove osebne informacije, pričakujejo, da bodo te za to pridobile njihovo predhodno dovoljenje. Uporabniki interneta so sicer seznanjeni z dejstvom, da nekatere informacije posredujejo samodejno že s samo uporabo interneta, vendar pa ne povsem glede zmogljivosti današnjih tehnologij, ki lahko že selektivno zbirajo in povezujejo informacije na internetu ter na podlagi tega ustvarjajo njihove osebne profile. Prav tako se ugotavlja, da ti ne poznajo zadostno osnovnega principa delovanja interneta (pomen in vloga spletnih piškotkov ter datotek dogodkov).

Previdnost uporabnikov pri navigiranju po internetu je trenutno zelo slaba, saj ne upoštevajo dobrih praks in tako na spletnih straneh le redko preberejo politiko zasebnosti oziroma drugo izjavo o zbiranju podatkov ter se ne posvetujejo o pogojih in pravilih uporabe. Podobno velja tudi za preverjanje, ali ima določena spletna stran pečat zasebnosti oziroma ali omogoča varno transakcijo. Iz tega lahko sklepamo, da uporabniki interneta posvečajo premalo pozornosti obstoječim elementom varovanja zasebnosti, s pomočjo katerih bi lahko bistveno varneje navigirali po internetu in s tem posledično zmanjšali izpostavljenost svoje zasebnosti. Prav tako se je pokazalo, da so njihove navade povsem drugačne, ko se znajdejo na internetu, saj pogosto še naprej uporabljajo spletne strani brez objavljene politike zasebnosti ali druge izjave o zbiranju podatkov, ali pa spletni strani posredujejo kar svoj pravi e-naslov v zameno za določeno korist. Nenazadnje se njihovo zaupanje ne pridobi samo s preverjenimi elementi varovanja zasebnosti, ampak pogosto že kar z lepo oblikovano spletno stranjo in uglednostjo podjetja.

Pri uporabi pristopov in tehnologij za varovanje zasebnosti s strani uporabnikov interneta je stanje nezadovoljivo in celo kritično. V internetnih aplikacijah, kot sta spletni brskalnik in poštni odjemalec, uporabljajo predvsem nezahtevne pristope (npr. brisanje spletnih piškotkov in datotek, spletnih naslovov itd.) ter do določene mere pristop rednega posodabljanja okolja oken z varnostnimi in servisnimi paketi., bistveno manj pa pristope spreminjanja privzetih nastavitev zasebnosti in varnosti (npr. sprejemanje in zavračanje spletnih piškotkov, določevanje filtrirnih pravil za e-pošto, vzpostavitev varne povezave s strežnikom itd.). Nasplošno, uporaba pristopov za varovanje zasebnosti v okolju oken ni zadovoljiva, kljub dejstvu, da so ti zelo pomembni zaradi že znanih slabosti internetnih aplikacij. Še bolj zaskrbljujoče je stanje pri tehnologijah za varovanje zasebnosti. Uporabo klasičnih PET programov (npr. za upravljanje s spletnimi piškotki in hrošči, za zavarovanje pred spywarom, za preprečevanje nezaželene e-pošte itd.) zasledimo bolj ali manj le pri redkih posameznikih, medtem ko je uporaba naprednih PET sistemov in programov (npr. za varovanje identitete, za varovanje z neizsledljivostjo, programe z naprednimi P3P uporabniškimi agenti, itd.) širši javnosti povsem tuja. Na podlagi tega lahko sklepamo, da je zasebnost uporabnikov interneta ogrožena bolj kot kdajkoli prej.

Potrditev ali zavrnitev hipoteze:

Na podlagi predstavljenih dejstev v šestem poglavju lahko v celoti potrdimo uvodoma postavljeno hipotezo, da se uporabniki interneta zavedajo zasebnosti, vendar so na internetu neprevidni ter se ne poslužujejo pristopov in tehnologij za varovanje zasebnosti.

7 SKLEP

Zasebnost ima veliko sprejetih definicij in dimenzij, saj obstajajo različni pogledi nanjo. Kot družbeno in pravno vprašanje je bila dolgo časa skrb sociologov, filozofov in odvetnikov. S širšo uporabo modernih IT sistemov in komunikacijskih omrežij v smislu nekajkratnih dnevnih aktivnosti (npr. bančna opravila, komuniciranje s prijatelji itd.), se je postavila dodatna zahteva, to je varovanje elektronske zasebnosti posameznika. Kadar govorimo o informacijski zasebnosti, nasplošno mislimo na zasebnost osebnega komuniciranja in zasebnost osebnih podatkov. Ta je sestavljena iz treh ključnih domen: tehnične, regulatorne in sociološke, njeno glavno vprašanje pa je povezano z nadzorom nad zasebnimi informacijami.

Internet omogoča učinkovito in nedrugo zbiranje informacij, običajno brez dovoljenja uporabnikov interneta in z edinstvenimi načini. Danes večina spletnih strani zbira vsaj eno izmed osebnih informacij, glavni razlog za tako množično zbiranje pa je njihova denarna vrednost. Med drugim so spletne strani sposobne ustvariti tudi osebne profile svojih potrošnikov in sicer s povezovanjem osebno identifikacijskih informacij (npr. ime, e-poštni naslov, domači naslov itd.) ter demografskih informacij (npr. spol, preference itd.). Vse to pri

uporabnikov interneta povzroča splošno zaskrbljenost glede njihovih zasebnih pravic, vendar je na drugi strani treba poudariti, da imajo ti različne preference in usmeritve do zasebnosti.

V državah, kjer najbolj učinkovito varujejo zasebnost, uporabljajo tako nadzorne in sektorske zakone, kot samoregulacijo in tehnologije zasebnosti. Pri slednjih programi in sistemi zagotavljajo različne stopnje zasebnosti in varnosti komuniciranja. Prav tako so tudi različno učinkovite, saj so lahko nekatere slabo zasnovane, drugi pa so lahko zasnovane za lažje zakonsko dostopanje. Trenutne raziskave, ki potekajo na področju zasebnosti uporabnikov, opredeljujejo pot za varovanje zasebnosti v smislu štirih zahtev, to pa so anonimnost, psevdonimnost, nepovezljivost ter neopazovanost.

Grožnje zasebnosti v informacijski družbi prihajajo iz različnih virov, kot so tehnologije, vlade in korporacije, in to v obliki nadzorovanja posameznikov ali zbiranja njihovih podatkov. Komercialne spletne strani zbirajo podatke s pasivnimi kot tudi aktivnimi načini, pri čemer se uporabnik tega zaveda ali pa tudi ne. Trenutno največkrat uporabljane oblike zbiranja so: z datotekami dogodkov, s spletni piškotki in hrošči, s spletni računi in obrazci ter z nezaželeno e-pošto in škodljivimi programi. Tu je treba vedeti, da se podatki ne zbirajo samo za komercialne ali osebne namene, kar tudi največkrat ogroža zasebnost, ampak tudi za povsem operativne namene, kot je zagotavljanje delovanja interneta ali nudenja personaliziranih rešitev uporabnikom interneta.

Uporabniki interneta lahko varujejo svojo zasebnost s pomočjo pristopov in tehnologij za varovanje zasebnosti. Namen prvih je predvsem odpraviti določene že znane slabosti v zasnovi internetnih aplikacij, kot sta spletni brskalnik in poštni odjemalec ter tako zmanjšati tveganja zasebnosti. Namen drugih, pa je predvsem kompleksno varovanje uporabnikove zasebnosti pri navigiranju po internetu in interakciji z drugimi udeleženci v sodobni družbi, uporabljajoč elektronske komunikacije.

Pregled in analiza pristopov za varovanje zasebnosti v okolju oken je pokazala, da lahko uporabniki interneta z njihovo pomočjo izboljšajo zasebnost, vendar pa ima na drugi strani spreminjanje privzetih nastavitev v internetnih aplikacijah tudi določene pomanjkljivosti, saj lahko to vpliva na njihovo kasnejšo zmogljivost oziroma lahko prepreči številne napredne in prilagojene rešitve pri interakciji uporabnika z internetom. Nenazadnje je tudi pregled in analiza tehnologij za varovanje zasebnosti (PET), ki naj bi učinkovito varovale zasebnost, pokazala določene pomanjkljivosti, predvsem na področju zagotavljanja odpornosti na varnostne grožnje (npr. prisluškovanje, napadi na vsebino, časovni napadi itd.) ter v manjši meri na področju uporabljenih tehnoloških rešitev (npr. anonimnost povezave, prekomerna latentnost itd.) in zadovoljitvi uporabnikovih zahtev (npr. personalizacija, dodatne storitve itd.).

Ocena dosedanje uspešnosti PET na podlagi njihovega desetletnega obstoja je pokazala, da se soočajo s številnimi problemi – od tega, da niso prijazne in razumljive uporabnikom, da se njihov razvoj pogosto ekonomsko ne izplača, da niso popularne v javnosti ter da so včasih lahko celo napadalne do zasebnosti. Drugi problemi so povezani še z dodajanjem PET v

obstoječe sisteme, z izkoriščanjem napak v slabi zasnovi aplikacij s strani PET, s pomanjkanjem standardiziranih rešitev zasebnosti in nadzorovanjem zasebnosti s PET tam, kjer to ni predvideno. Med drugim, PET svojim uporabnikom ne nudijo zadostnega nadzora nad osebnimi informacijami potem, ko se te odkrijejo spletnim prodajalcem in večina uporabnikom tudi ne nudi izbire, ali bodo privolili v prihodnjo uporabo teh informacij za sekundarne namene. Na osnovi dejstev v tem in predhodnem odstavku je bila v magistrskem delu postavljena hipoteza, da tehnologije za varovanje zasebnosti na internetu niso popolnoma dodelane in učinkovite, v celoti potrjena.

Priporočila in usmeritve za prihodnost se tako nanašajo na razvoj bolj dodelanih ter učinkovitih PET, ki bodo podprle bogate in storitveno naravnane interakcije na internetu. V strokovni literaturi zasledimo številne dejavnike, ki lahko pomembno vplivajo na prihodnost PET. Prvi dejavnik je zagotavljanje trga, znotraj katerega je treba doseči boljše razumevanje vprašanj zasebnosti, uporabo ustreznih tehnologij pri njihovih uporabnikih in nadaljevati z mednarodnimi PET projekti. Inovativno snovanje je naslednji dejavnik, s katerim bi lahko snovalci preko uporabe osnovnega modela/procesa zasebnosti, upoštevanjem izkušenj s področja HCI znanosti ter izogibanjem kritičnim dejavnikom, zagotovili zrelejše PET. Dejavniki izobraževanja javnosti o zasebnosti in PET je zelo pomemben za dvig zavesti in kompetenc tako uporabnikov interneta kot strokovnjakov na univerzah in v gospodarstvu. Ključni dejavnik je tudi standardizacija principov zasebnosti, ki jih vsebujejo direktive Evropske unije in primerna informacijska načela. Standardi zasebnosti ne bi zmanjšali samo stroškov, ampak tudi tveganja pri raziskavah in razvoju, promovirali bi vgrajeno varovanje ter izločevali produkte in storitve, ki bi vodili do groženj zasebnosti.

Spremljajoča empirična raziskava o zasebnosti med uporabniki interneta je pokazala, da se ti na splošno zavedajo zasebnosti na internetu, vendar pa ne poznajo dovolj osnovnega principa delovanja interneta. Previdnost uporabnikov pri navigiranju po internetu je trenutno zelo slaba, saj ne upoštevajo dobrih praks, s pomočjo katerih bi lahko bistveno varneje navigirali po internetu in s tem posledično zmanjšali izpostavljenost svoje zasebnosti. Prav tako se je pokazalo, da so njihove navade povsem drugačne, ko se znajdejo na internetu. Pri uporabi pristopov in tehnologij za varovanje zasebnosti je stanje povsem nezadovoljivo in celo kritično. V internetnih aplikacijah v okolju oken, se uporabniki poslužujejo predvsem nezahtevnih pristopov (npr. brisanje spletnih piškotkov in datotek, spletnih naslovov itd.) ter do določene mere pristop rednega posodabljanja okolja oken z varnostnimi in servisnimi paketi, bistveno manj pa pristope spreminjanja privzetih nastavitev zasebnosti in varnosti (npr. sprejemanje in zavračanje spletnih piškotkov, vzpostavitev varne povezave s strežnikom itd.). Še bolj zaskrbljujoče pa je stanje pri tehnologijah za varovanje zasebnosti. Uporabo klasičnih PET programov (npr. za upravljanje s spletnimi piškotki in hrošči, za preprečevanje nezaželene e-pošte itd.) zasledimo bolj ali manj le pri redkih posameznikih, med tem ko je uporaba naprednih PET sistemov in programov (npr. za varovanje identitete, za varovanje z neizsledljivostjo, programe z naprednimi P3P uporabniškimi agenti, itd.) širši javnosti povsem tuja. Na osnovi dejstev v tem odstavku je bila v magistrskem delu postavljena hipoteza, da se uporabniki interneta zavedajo zasebnosti, vendar so na internetu neprevidni ter se ne poslužujejo pristopov in tehnologij za varovanje zasebnosti, v celoti potrjena.

V magistrskem delu smo videli, da je zasebnost na internetu v današnji informacijski družbi vse bolj ogrožena in da je njeno učinkovito varovanje pogosto zapleteno ter odvisno od številnih drugih dejavnikov. Z vsakim dnem naša zasebnost na internetu tako vse bolj izginja, zato je treba ukrepati takoj. Pripravljena priporočila in usmeritve bi lahko tu predstavljala pomemben korak k spreobrnitvi trenutnega toka dogajanj.

8 LITERATURA IN VIRI

8.1 Literatura

1. Ackerman S. Mark, Cranor Faith Lorrie, Reagle Joseph: Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. B.k.: ACM Conference on Electronic Commerce, 1999, str. 1–8.
2. Alsaid Adil, Martin David: Detecting Web Bugs With Bugnosis. [URL:<http://www.cs.uml.edu/~dm/pubs/bugnosis-pet2002.pdf>], 22. 1. 2007.
3. An Introduction to Cryptography. B.k.: Network Associates, Inc., June 2001. 86 str.
4. Berendt Bettina, Günther Oliver, Spiekermann Sarah: Privacy in E-Commerce: Stated Preferences vs. Actual Behavior. B.k.: Communication of the ACM, Vol. 48, 2005, No. 4, str. 101–106.
5. Borking J. John: The use and value of privacy-enhancing technologies. Bristol: The Glass Consumer, National Consumer Council, 2005, str. 69–95.
6. Borking J. John: Privacy Standards for Trust. [URL:<http://www.privacyconference2005.org/fileadmin/PDF/borking.pdf>], 3. 10. 2005.
7. Bygrave A. Lee: Privacy-Enhancing Technologies: Caught between a Rock and a Hard Place. B.k.: Privacy Law & Policy Reporter, Vol. 9, 2002, str. 135–137.
8. Chung Winnie, Paynter John: Privacy Issues on the Internet. Proceedings of the 35 th Hawaii International Conference on System Sciences. [URL:http://www.hicss.hawaii.edu/HICSS_35/HICSSpapers/PDFdocuments/INISC02.pdf], 25. 3. 2007.
9. Clark Roger: Introduction to Dataveillance and information Privacy, and Definitions of Terms. [URL:<http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html>], 1. 4. 2007.
10. Cranor Faith Lorrie: The Role of Privacy Enhancing Technologies. Considering Consumer Privacy: A Resource for Policymakers and Practitioners. Washington D.C.: Center for Democracy & Technology, 2003, str. 80–83.
11. Cranor Faith Lorrie, Garfinkel Simson: Security and Usability: Designing Secure System that People can Use. B.k.: O'Reilly Media, Inc., 2005. 738 str.
12. Debussere Frederic: The EU E-Privacy Directive: A monstrous Attempt to Starve the Cookie Monster ?. B.k.: International Journal of Law and Information Technology, Oxford University Press, Vol. 13, 2005, No. 1, str. 70–97.
13. Earp B. Julia, Baumer David: Innovative Web Use to Learn about Consumer Behavior and Online Privacy. B.k.: Communication of the ACM, Vol. 46, April 2003, No. 4, str. 81–83.
14. Fischer Hübner Simone, Lindskog Helena: Teaching Privacy-Enhancing Technologies. Karlstad University. [URL:<http://citeseer.ist.psu.edu/cache/papers/cs/25136/http:zSzzSzprivacy.lindskog.wsSzteachpet.pdf/teaching-privacy-enhancing-technologies.pdf>], 8. 1. 2007.

15. Garfinkel Simson, Spafford Genne: Web Security, Privacy & Commerce, 2nd Edition. B.k.: O'Reilly Media, Inc., 2002. 735 str.
16. Glee Harrah Cady, McGregor Pat: Protect your Digital Privacy. Survival Skills for the Information Age. B.k.: QUE, 2001. 652 str.
17. Goldberg Ian: Privacy-Enhancing Technologies for the Internet, II: Five years later. [URL:<http://www.freehaven.net/anonbib/papers/petfive.pdf>], 25. 2. 2007.
18. Good Nathaniel et al.: Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware. Symposium on Usable Privacy and Security 2005. [URL:<http://cups.cs.cmu.edu/soups/2005/2005proceedings/p43-good.pdf>], 6. 7. 2005.
19. Gritzalis Stefanos: Enhancing Web privacy and anonymity in the digital era. B.k.: Information Management & Computer Security, Emerald Group Publishing Limited, Vol. 12, 2004, No. 3, str. 255–288.
20. Ha Vicki et al.: The Cookie Conundrum: Examining the Dual Nature of Cookies. University Ave.. [URL:<http://www.cs.dal.ca/research/techreports/2005/CS-2005-18.pdf>], 12.10.2005.
21. Jerman Blažič Borka: Tehnike in tehnologije za varovanje zasebnosti v elektronskih komunikacijah: modeli zaščite (I del). Ljubljana: Varstvoslovje, let. 7, 2005, št. 2, str. 123–131.
22. Jerman Blažič Borka: Pregled tehnologij za varovanje zasebnosti v elektronskih komunikacijah: predstavitev in ocena njihove uporabnosti–PET (II del). Ljubljana: Varstvoslovje, let. 7, 2005a, št. 3, str. 227–243.
23. Kavakli Evangelia, Kalloniatis Christos, Gritzalis Stefanos: Addressing Privacy: Matching User Requirements with Implementation Techniques. University of the Aegean. [URL:<http://www.aueb.gr/pympe/hercma/proceedings2005/H05-FULL-PAPERS-1/KAVAKLI-KALLONIATIS-GRITAZALIS-1.pdf>], 12. 12. 2006.
24. Lederer Scott et. al.: Personal Privacy through understanding and action: five pitfalls for designer. B.k.: Personal and Ubiquitous Computing, Vol. 8, November 2004, No. 6, str. 440–454.
25. Levy E. Stephen, Gutwin Carl: Improving Understanding of Website Privacy Policies with Fine-Grained Policy Anchors. Chiba: Proceedings of the 14th international conference on World Wide Web, May 2005, str. 480–488.
26. Loring B. Tracie: An Analysis of the Informational Privacy Protection Afforded by the European Union and United States. B.k.: 37 Texas International Law Journal, 2002, str. 421–460.
27. Lundblad Nicklas: Privacy in a Noise Society. Stockholm: Scandinavian Studies in Law, Almqvist and Wiksell, Vol. 47, September 2004, str. 349–371.
28. Martin David, Wu Hailin, Alsaïd Adil: Hidden Surveillance by Web Sites: Web Bugs in Contemporary Use. B.k.: Communication of the ACM, Vol. 46, 2003, No. 12ve, str. 258–264.
29. Oppliger Rolf: Privacy-enhancing technologies for world wide web. B.k.: Computer Communications 28, 2005, str. 1791–1797.
30. Ponnuram K.: Usable Privacy and Security: Introduction to Privacy. [URL:<http://cups.cs.cmu.edu/courses/ups-sp06/notes/060124.pdf>], 24. 1. 2006.

31. Privacy Enhancing Technologies. B.k.: META Group Report v 1.1., March 2005. 40 str.
32. Privacy and Ubiquitous Network Societis. B.k.: International Telecommunication Union, March 2005. 30 str.
33. Privacy Online. B.k.: Federal Trade Commission, June 1998. 62 str.
34. Privacy Online: OECD Guidance on Policy and Practise. Paris: OECD publications, 2003. 390 str.
35. Seničar Vanja, Jerman Blažič Borka, Klobučar Tomaž: Privacy-Enhancing Technologies-approaches and development. B.k.: Computer Standards & Interfaces, 25, 2003, str. 147–158.
36. SPAM 2005. Washington D.C: Center for Democracy & Technology, March 2005. 69 str.
37. Stafford F. Thomas, Urbaczewski Andrew: Spyware: The Ghost in the Machine. B.k.: Communications of the Association for Information System, Vol. 14, 2004, str. 291–306.
38. Stahl Carsten Bernd: Privacy and Security as Ideology. De Montfort University. [URL:http://www.cse.dmu.ac.uk/~bstahl/publications/2006_Privacy_Security_Ideology_LSPI.pdf], 20. 3. 2007.
39. Stalder Felix: The Voiding of Privacy. B.k.: Sociological Research Online, Vol. 7, August 2002, No. 2. 33 str.
40. Tavani T. Herman, Moor H. James: Privacy Protection, Control of Information, and Privacy–Enhancing Technologies. B.k.: Computer and Society, March 2001, str. 6–11.
41. The Security–Privacy Paradox. B.k.: The Information and Privacy Commissioner/Ontario and Deloitte&Touche, August 2003. 19 str.
42. Turner C. Eric, Dasgupta Subhasish: Privacy on the Web: An Examination of User Concerns, Technology, and Implications for Business Organizations and Individuals. B.k.: Information Systems Management, Winter 2003, str. 8–18.
43. Watt Nicole et al.: On–line Privacy: An analysis of the gaps between consumer privacy expectation, Australian legislation and implementation on Australian Web Sites. B.k.: ColleCTER, 2001, str. 118–131.

8.2 Viri

1. Anand Ashish: Application Level Cryptography: Combinational Stream & Block Ciphering Using Double Encryption Algorithms. Maharishi Dayanand University. [URL:http://www.infosecwriters.com/text_resources/pdf/App_Level_Cryptography.pdf], 10. 1. 2007.
2. Chul Huh Soon: Invasion of Privacy v. Commercial Speech? [URL:<http://www.albanylawreview.org/articles/INVASIONOFPRIVACYVCOMMERCIALSPEECHREGULATIONOFSPAMWITHACOMPARATIVECONSTITUTIONALPOINTOFVIEW.pdf>], 6. 2. 2007.
3. Configuring Internet Explorer for Practical Security and Privacy – Part 1. [URL:<http://www.malwarehelp.org/configuring-internet-explorer1.html>], 12. 2. 2007.

4. Consumer Perspectives on Spam. International Telecommunication Union. [http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf], 25. 2. 2007.
5. Desktop Application Security Tehnical Implementation Guide. B.k.: Defence Information Systems Agency, Version 3, Release 0, February 2006. 103 str.
6. Internet Explorer Safety. James Madison University. [URL:http://www.jmu.edu/computing/security/info/ie/ie.shtml], 3. 4. 2007.
7. Judge Paul: How Spammers Fool Spam Filters. [URL:http://www.securitydocs.com/library/3436], 7. 6. 2005.
8. Market View: A New Cookie Cutter for Classifying Web Cookies. Ballardvale Research. [URL:http://www.ballardvale.com/pdf/MV%20-%20Cookies.pdf], 27. 8. 2005.
9. Outlook Express 6. Education Service Group: University of Victoria. [URL:http://web.uvic.ca/comped/online/outlookexp/outlookexp.pdf], 10. 8. 2004.
10. Otterloo van Sieuwert: A security analisys of Pretty Good Privacy. B.k.: September 2001. 86 str.
11. PHR-2004 Overview of Privacy. Privacy International. [URL:http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82589], 13. 11. 2004.
12. Pitsenbarger Trent, Bartock Paul: Outlook E-Mail Security in the Midst of Malicious Code Attacks. B.k.: National Security Center, Version 3.1, December 2004. 32 str.
13. Rotenberg Marc: Preserving Privacy in the Informational Society. [URL:http://www.unesco.org/webworld/points_of_views/rotenberg_1.html], 6. 1. 2007.
14. Securing your E-mail client – Outlook Express Part 1. [URL:http://www.malwarehelp.org/securing-your-e-mail-client-outlookexpress1.html], 1. 2. 2007.
15. Spam: What to Do about Junk E-Mail. St. Norbert College. [URL:http://www.snc.edu/compserv/handouts/spam.htm], 17. 1. 2005.
16. Thorson J. Stuart, Sedore M. Christopher: SPAM and Personal Data Privacy. [URL:http://www.sai.syr.edu/facultypapers/Spam%20and%20Personal%20Data%20Privacy.pdf], 2. 3. 2007.
17. Windows XP Service Pack 2: Technologies Overview. [URL:http://www.microsoft.com/windowsxp/sp2/technologiesoverview.mspx], 4. 8. 2004.
18. 2006 International Privacy Survey: Ranking by Countries. Privacy International. [URL:http://www.privacyinternational.org/survey/phr2005/aboutphrtable.pdf], 13. 3. 2007.

PRILOGE

Priloga 1: Vprašalnik.....	1
Priloga 2: Slovar slovenskih prevodov tujih izrazov in kratic	3

Priloga 1: Vprašalnik

Spol: M Ž

Starostna skupina : do 19 let 20-29 let 30-49 let nad 49 let

Stopnja izobrazbe: srednja šola visoka šola šolajoč (dijak, študent)

Internet uporabljam: dnevno tedensko mesečno

A) ZAVEDANJE O ZASEBNOSTI NA INTERNETU

PROSIM, OZNAČITE VAŠE STRINJANJE OZIROMA NESTRINJANJE S TRDITVAMI

1 = s trditvijo se v celoti ne strinjam 2 = s trditvijo bi se v manjši meri strinjal 3 = trditev pretežno velja 4 = trditev v veliki meri drži 5 = trditev drži v celoti	1	2	3	4	5
1. Menim, da morajo osebne informacije (npr. ime, naslov, e-pošta, telefonska številka itd.) ostati varovane za razliko od javnih informacij, ki se lahko odkrijejo.					
2. Zasebnost na internetu me skrbi z vidika zbiranja informacij, namena njihove uporabe, njihovega varovanja ter možnosti zlorab.					
3. Zbiranje in prodajanje osebnih informacij med podjetji ter državnimi ustanovami brez mojega dovoljenja predstavlja kršitev zasebnosti.					
4. Zaradi odprte narave interneta in posledične razpršenosti informacij ni mogoče ustvariti mojega osebnega profila.					
5. Nekatere informacije posredujem preko interneta samodejno (npr. IP naslov računalnika, vrsto operacijskega sistema, naslov predhodne spletne strani itd.).					
6. Po mojem prepričanju zakonodaja in regulative zasebnosti zadostno varujejo mojo zasebnost na internetu.					
7. Na področju interneta poznam pomen in vlogo spletnih piškotkov (Cookies) in datotek dogodkov (Log files).					
8. Osebno nisem zadostno seznanjen s tehnologijami, ki ogrožajo zasebnost na internetu ter pristopi in tehnologijami za njeno varovanje.					

B) OBNAŠANJE NA INTERNETU

PROSIM OZNAČITE VAŠE STRINJANJE OZIROMA NESTRINJANJE S TRDITVAMI

1 = s trditvijo se v celoti ne strinjam 2 = s trditvijo bi se v manjši meri strinjal 3 = trditev pretežno velja 4 = trditev v veliki meri drži 5 = trditev drži v celoti	1	2	3	4	5
9. Preden se registriram na določeni spletni strani, se posvetujem o pravilih in pogojih uporabe 'Terms and Conditions'.					
10. Če spletna stran zahteva e-poštni naslov, ji posredujem mojega osebnega in za to ne uporabljam drugega.					

11. Pri prvem obisku spletne strani vedno poiščem in preberem politiko zasebnosti ali drugo izjavo o zbiranju osebnih informacij.					
12. Spletno stran, ki nima objavljene politike zasebnosti ali druge izjave o zbiranju osebnih informacij, kljub temu še naprej uporabljam.					
13. Pri prvem obisku spletne strani vedno preverim, ali ima pečat zasebnosti (certifikat od BBBonline, TRUSTe itd.) o doslednem spoštovanju objavljene politike zasebnosti.					
14. Zaupanje vpliva na mojo odločitev o tem, katere spletne strani bom uporabljal (npr. ugled podjetja, dobro oblikovana spletna stran).					
15. Bolj kot potrebujem informacijo/datoteko na določeni spletni strani, bolj potisnem skrb o zasebnosti v ozadje.					
16. Pred posredovanjem občutljivih informacij (npr. EMŠO, številka zdravstvene in bančne kartice itd.) preverim, ali spletna stran omogoča varno transakcijo (certifikat od VeriSign, StarField itd.).					

C) UPORABA PRISTOPOV IN TEHNOLOGIJ ZA VAROVANJE ZASEBNOSTI NA INTERNETU

PROSIM OZNAČITE VAŠE STRINJANJE OZIROMA NESTRINJANJE S TRDITVAMI

1 = s trditvijo se v celoti ne strinjam 2 = s trditvijo bi se v manjši meri strinjal 3 = trditev pretežno velja	4 = trditev v veliki meri drži 5 = trditev drži v celoti	1	2	3	4	5
17. Pri spletnem brskalniku (npr. Internet Explorer) sem spremenil privzete nastavitve zasebnosti (stopnjo sprejemanja/zavračanja piškotkov) mojim potrebam varovanja.						
18. Osebo večkrat poskrbim, da v spletnem brskalniku (npr. Internet Explorer) zbrišemčasne datoteke (spletni piškotki in datoteke) ter počistim mapo zgodovina (naslovi spletnih strani).						
19. Pri poštnem odjemalcu (npr. Outlook Express) sem spremenil privzete nastavitve poštnega računa in sporočilnih pravil (varni prenos in filtriranje pošte) mojim potrebam varovanja.						
20. V okolju oken večkrat poskrbim za njihovo posodobitev (sistema in internetnih aplikacij) (npr. WindowsUpdate)						
21. Za učinkovito preprečevanje nezaželene e-pošte (SPAM) v poštnem odjemalcu (npr. Outlook Express) uporabljam ustrezne programe za filtriranje (npr. SpamAssassin, Spamprove itd).						
22. Da zavarujem svojo identiteto na internetu uporabljam ustrezne sisteme, ki zagotavljajo anonimnost oziroma psevdonimnost (npr. Proxy strežnik, LPWA itd).						
23. Za učinkovito upravljanje s spletnimi piškotki in hrošči uporabljam ustrezne programe (npr. Cookie Crusher, Bugnosis itd).						
24. Pri pošiljanju e-sporočil preko interneta uporabljam ustrezne programe za šifriranje vsebine in datotek (npr. PGP, itd.) z namenom preprečiti možnosti vpogleda tretjim osebam v samo vsebino.						

25. Da se obvarujem pred Spywarom (oglaševalskimi, nadzorovalnimi in zlonamernimi programi) uporabljam ustrezne programe (npr. SpyBoot, Ad-Aware itd).					
26. Ker ne želim, da me izsledijo na podlagi mojih internetnih aktivnosti, uporabljam ustrezne sisteme za varovanje z neizsledljivostjo (npr. GUNet, Crowds itd).					
27. Uporabljam programe z naprednimi P3P uporabniškimi agenti, ki mi pomagajo pri odločanju v zvezi z mojo zasebnostjo (npr. Privacy Bird).					

Priloga 2: Slovar slovenskih prevodov tujih izrazov in kratic

ActiveX		Tehnologija, ki omogoča prenos in zagon programov
APPEL	A P3P Preference Exchange Language	Jezik za izmenjavo P3P preferenc
Cookies		Spletni piškotki
CSCW	Computer Supported Cooperative Work	Računalniško podprto kooperativno delo
DoS	Denial of Service	Zavrnitev storitve
EPAL	Enterprise Privacy Authorization Language	Jezik za pisanje politike zasebnosti podjetij
EPIC	Electronic Privacy Information Center	Informacijski center za elektronsko zasebnost, ki osvešča javnost glede varovanja zasebnosti
EULA	End User License Agreement	Sporazum o načinu uporabe proizvajalčevega programa
FIP	Fair Information Practices	Primerna informacijska načela
FTC	Federal Trade Commission	Ameriška zvezna komisija za trgovino
GIF	Graphic Interchange Format	Slikovni rastrski format
HCI	Human Computer Interaction	Znanost, ki preučuje interakcijo ljudi z računalniki
HTML	Hyper Text Markup Language	Spletni programski jezik
HTTP	Hiper Text Transfer Protocol	Opredeljuje komunikacijo med strežnikom in odjemalcem
IDEA	International Data Encryption Algorithm	Mednarodni algoritem za simetrično kriptografijo
IP naslov		Naslov računalnika v omrežju - stalni ali dinamičen
IPv6	Internet Protocol version 6	Nova generacija internetnega protokola
IT	Information Technology	Informacijska tehnologija
Java		Objektno orientiran programski jezik
Java Script		Skriptni jezik za programiranje spletnih strani
Jondo		Vzpostavljen proces, ki poteka na uporabnikovem računalniku
KB	KiloByte	Enota za količino podatkov

		oziroma velikost pomnilnika
LPWA	Lucent Personalized Web Assistant	Lucentov personalizirani spletni asistent (sistem)
Mail Logs		Poštna datoteka dogodkov
Node		Vozlišče ali računalnik, ki je vključen v omrežje
OECD	Organisation for Economic Co-operation and Development	Organizacija za ekonomsko sodelovanje in razvoj
Onion Routers		Usmerjevalniki sistema Onion Routing
Opt-in opt-out		Upoštevanje privolitve oziroma zavrnitve uporabnika, za izvajanje določenih internetnih aktivnosti
Peers		Vozlišča
PET	Privacy Enhancing Technologies	Tehnologije za varovanje zasebnosti
PETTEP	Privacy Enhancing Technology Testing & Evaluation Project	Projekt testiranja in ocenjevanja tehnologij za varovanje zasebnosti
PGP	Pretty Good Privacy	Program za varovanje e-pošte ali datotek (šifriranje)
Phishing		Lažno predstavljane
PI	Privacy International	Združenje za človekove pravice, ki opazuje nadzorovanja in napade na posameznikovo zasebnost
PIT	Privacy Invasive Technologies	Tehnologije, ki napadajo zasebnost
Pixel		Najmanjša točka v sliki
Plugin		Vstavek, ki nudi na zahtevo specifične funkcije
Pop-up		Oglaševalske reklame ali sporočila, ki se prikažejo kot pojavno okno
PRIME	Privacy and Identity Management for Europe	Projekt upravljanja z zasebnostjo in identiteto za Evropo
Privacy Policy		Politika zasebnosti, vsebovana na določenih spletnih straneh
Privacy Seal		Pečat zasebnosti, vsebovan na določenih spletnih straneh
Proxy		Vmesni strežnik
P2P	Peer to Peer	Internetno zasnovano omrežje, ki omogoča skupini uporabnikov izmenjavo datotek
P3P	Platform for Privacy Preferences	Plaforma za preference zasebnosti
RAT	Remote Administration Trojans	Oddaljeni administrativni Trojani (oblika Spywara)
RIS	Raba Interneta v Sloveniji	Institucija v Sloveniji, ki se ukvarja z raziskovanjem uporabe interneta
RSA	(R. Rivest, A. Shamir, L. Adleman)	Algoritem za asimetrično kriptografijo
Safe Harbour		Sporazum med ZDA in EU o izboljšanju varovanja informacij (Varni pristan)
SPAM		Nezaželena elektronska pošta
Spoofing		Kraja občutljivih informacij

Spyware		Razred programov, ki se namestijo na računalniku za namene nadzorovanja, oglaševanja itd.
SSL	Secure Socet Layer	Protokol, ki omogoča šifrirano povezavo med strežnikom in odjemalcem
TCP	Transport Control Protocol	Protokol za nadzor prenosa podatkov
TLS	Transport Layer Security	Protokol, ki omogoča šifrirano povezavo med strežnikom in odjemalcem (naslednik SSL)
UBE	Unsolicited Bulk E-mail	Nenaročena masovna elektronska pošta (drugo ime za SPAM)
Ubicomp		Vsesplošno računalništvo
UCE	Unsolicited Commercial E-mail	Nenaročena komercialna elektronska pošta (drugo ime za SPAM)
URL	Uniform Resource Locator	Način edinstvenega določevanja lokacije na internetu (npr. naslovi spletnih strani)
Web Bugs		Spletni hrošči
Web Logs		Spletna datoteka dogodkov
W3C	World Wide Web Consortium	Organizacija, ki skrbi za razvoj spleta in postavitve standardov ter tehničnih priporočil
XML	eXtensible Markup Language	Standard za zapis strukturiranih dokumentov na internetu
XP SP2	XP Service Pack 2	Storitveni paket za posodobitev okolja oken XP