Masarykova univerzita

Filozofická fakulta

Ústav české literatury a knihovnictví

Kabinet informačních studií a knihovnictví

Hana Habermannová

PET, ISA a soukromí na internetu

Bakalářská diplomová práce

Vedoucí práce: PhDr. Michal Lorenz, Ph.D.

2012

Bibliografický záznam

HABERMANNOVÁ, Hana. *PET, ISA a soukromí na internetu*. Brno, 2012. 65 s. Bakalářská práce. Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví. Vedoucí práce PhDr. Michal Lorenz, Ph.D.

Anotace

Předkládaná práce s názvem *PET, ISA a soukromí na internetu* seznamuje čtenáře s problematikou ochrany soukromí uživatele na internetu, přičemž se zaměřuje především na představení technologií na ochranu soukromí na internetu, na tzv. Privacy Enhancing Technologies (PET). Tyto technologie jsou již ve světě dobře známy, proto je cílem této práce uvést PET i do českého prostředí. Na téma je pohlíženo po stránce technologické i legislativní. V neposlední řadě práce přináší náhled do světa nejmodernějších technologií, které vykonávají úkoly zadané uživatelem zcela automaticky. Jedná se o inteligentní softwarové agenty (Intelligent Software Agent, ISA), kteří mmj. spolupracují s PET na ochraně uživatelova soukromí na internetu. Cílem této práce je tedy upozornit na možná nebezpečí, která se dotýkají uživatelova soukromí na internetu, představit moderní technologie PET, jež mohou soukromí ochránit, a uvést jednu z „inteligentních“ technologií (ISA), která s PET úzce souvisí.

Annotation

Presented thesis entitled "PET, ISA and privacy on the Internet" introduces readers to the issue of user privacy on the Internet, focusing primarily on introducing technologies for the protection of privacy on the Internet, so-called Privacy Enhancing Technologies (PET). These technologies are already well known in the world, therefore the aim of this study is to introduce the PET into Czech environment. The topic is percieved in terms of

technology and legislative. Last but not least, the thesis provides insight into the world's most advanced technologies to perform tasks specified by the user automatically. It is an Intelligent Software Agent (ISA), which apart from other things cooperates with PET in protecting user privacy on the Internet. The aim of this thesis is to highlight the dangers which affect user privacy on the Internet, introduce PET modern technology that can protect privacy, and include one of the "smart" technologies (ISA), which is closely linked with PET.

Klíčová slova

Soukromí, internet, ochrana soukromí na internetu, Privacy Enhancing Technologies, PET, Intelligent Software Agent, inteligentní agent, ISA.

Keywords

Privacy, internet, internet privacy protection, Privacy Enhancing Technologies, PET, Intelligent Software Agent, intelligent agent, ISA.

Prohlášení

Prohlašuji, že jsem předkládanou bakalářskou diplomovou práci vypracovala samostatně s využitím uvedených pramenů a literatury.

V Brně dne 27. 4. 2012 *Hana Habermannová*

Poděkování

Děkuji za cenné rady a vedení mé bakalářské diplomové práce panu PhDr. Michalu Lorenzovi, Ph.D., přátelům a rodině za trpělivost a podporu, Liance Kociánové a Antonii Hoškové za to, že mi byly motivací při psaní této práce.

Obsah

ÚVOD

Soukromí a právo na soukromí jsou považovány za základní předpoklad fungování člověka ve společnosti a mimo ni. O to více je kladen důraz na jejich zachování a ochranu. Právě ochrana soukromí se stává klíčovou v současné době, která je charakteristická přesahem ICT do reálného života, kdy se již neobejdeme bez internetu, technologií a aplikací, které nám v mnohém usnadňují pracovní i soukromý život. Na druhé straně ale mohou být také „viníky“ ve sporu mezi námi a hrozbami pro naše soukromí.

Ve své bakalářské diplomové práci se zabývám soukromím na internetu, na které my jako jeho uživatelé dost často zapomínáme, a problematiku porušování práva na soukromí, zveřejňování údajů, včetně těch citlivých a osobních, podceňujeme. Dále představím možnosti ochrany soukromí za využití PET, a to s náhledem do legislativy a různých doporučení. Ruku v ruce s PET jdou i ISA agenti, kteří mohou k ochraně soukromí přispět v dobrém i špatném slova smyslu. Agentům bude věnována poslední část práce.

Práce je tedy členěna do tří hlavních kapitol:

I. **SOUKROMÍ NA INTERNETU**, kde se věnuji vymezení základních pojmů z oblasti soukromí na internetu nebo také „tradičním“ hrozbám, které na uživatele internetu „číhají“. Zaměřím se i na to, jak na celou věc pohlíží legislativa a konsorcia.

II. **PET**, jež tvoří jádro celé práce, neboť zde popisuji v českém prostředí dosud nezmiňované technologie a možnosti na ochranu soukromí.

III. **ISA**, kapitola, která se týká inteligentních technologií umožňujících chránit, ale i ohrožovat soukromí prostřednictvím PET.

Mým záměrem je popsat další možnosti ochrany soukromí v podobě PET, zasadit je do kontextu problematiky soukromí na internetu a uvést taktéž moderní „inteligentní“ technologie (ISA), které se soukromí dotýkají.

V zahraničních zdrojích se ve stále větší míře objevují články, které PET vykládají a blíže specifikují. Není tomu tak ale v českém prostředí, proto vznikla tato práce, v jejíž silách ale není předložit zcela komplexní přehled o tematice. Zaměřím se proto na základní uvedení do problému, aby čtenář získal povědomí o rychle se rozvíjejícím způsobu ochrany dat. Ve své práci identifikuji stěžejní oblasti tématu v rozebírané literatuře a jiných zdrojích a uspořádávám je do přehledné struktury s cílem předložit základní náhled do tématu *PET, ISA a soukromí na internetu*.

Vládním i komerčním zájmem je urychlit proces implementace PET do nejrůznějších systému s cílem zvýšit bezpečnost osobních dat a informací obecně pro každého uživatele internetu. Legislativa si je vědoma, že soukromí je potřeba chránit, přičemž vznikají stále nová a nová doporučení a zákony, které se toto snaží řešit. Ochrana je z jejich pohledu důležitá právě kvůli zachování základního lidského práva na soukromí, dále kvůli rozvoji digitální ekonomiky na internetu či kvůli e-governmentu. Legislativním záměrem je zvyšovat důvěryhodnost a bezpečnost internetu pro každodenní činnosti občana státu.

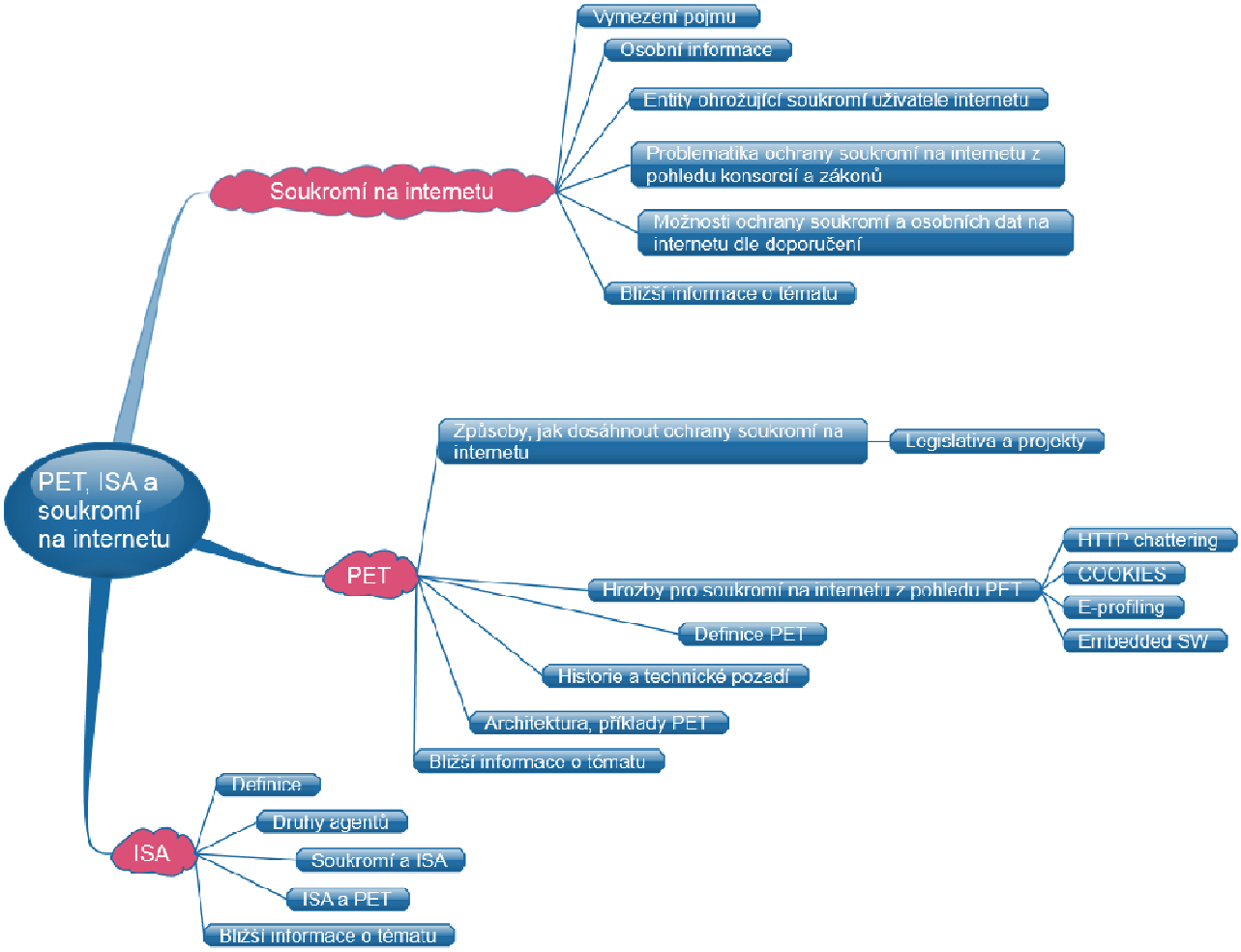
Mou snahou je, aby po přečtení předkládané práce čtenář věděl, že existují hrozby, které se mohou dotýkat i jeho soukromí, a jak se tyto hrozby projevují. Dále zjistí, že existují legislativní opatření a různá doporučení, které se snaží soukromí a nejen osobní informace chránit, stejně tak jako technologické možnosti v podobě PET, jež se stávají moderním nástrojem v boji proti útokům na naše soukromí. Čtenář získá přehled o tom, co jsou to PET, jak fungují či jaké jsou příklady jejich využití v praxi, seznámí se s inteligentními softwarovými agenty (ISA) a zjistí, co mají společného s PET a soukromím. Čtenář-uživatel tedy výsledně získá aktuální ucelený základní přehled o soukromí na internetu, PET a ISA.

Pro další výklad je nutné definovat, s jakými klíčovými pojmy ve své práci operuji. Jedná se o:

Soukromí na internetu (Internet Privacy), které rozšiřuje pohled na základní vymezení soukromí do prostředí internetu. Často bývá definováno jako právo na soukromí týkající se skladování nejen osobních dat, jejich poskytování třetím stranám a v neposlední řadě

odhalování dat v prostředí internetu. Druhým pojmem jsou **PET (Privacy Enhancing Technologies)**, tj. technologie zvyšující ochranu soukromí uživatele na internetu. Jedná se o obecný termín označující skupinu nástrojů, aplikací a mechanismů, které za předpokladu, že jsou začleněny do online služeb, aplikací nebo systémů, umožňují uživatelům chránit jejich soukromí a osobní informace v těchto prostředích. Posledním z primárních pojmů je **ISA (Intelligent Software Agent)**, což je softwarový mechanismus, který vykonává zadané úkoly s minimálním úsilím ze strany uživatele.

Jednotlivé pojmy zasazuji do kontextu s oblastmi, které přehledně mapuje následující grafika:



Obrázek 1 Zmapování oblastí tématu prostřednictvím aplikace NovaMind 5[1]

[1] Domovské stránky aplikace, kde je možné program získat a vyzkoušet: http://www.novamind.com/

1. SOUKROMÍ NA INTERNETU

"Soukromí nebylo nikdy tak důležité jako dnes,
v době internetu, WWW a chytrých telefonů."[2]
(Barack Obama)

1.1 Vymezení pojmu

Vývoj informačních technologií spolu s rozmachem internetu přinášejí řadu otázek, na které starší generace nemusely hledat odpovědi a jež jsou aktuální právě v dnešní době, která je charakteristická přesahem technologií do reálného života. Přesně tak je tomu v případě našeho soukromí, jež je konfrontováno s internetem. Vzniklo označení "soukromí na internetu", které se mmj. týká i toho, jak jedinec zachází se svými soukromými a osobními daty na internetu.

Soukromí na internetu lze tedy definovat jako schopnost kontrolovat, jaké informace o sobě člověk prozrazuje prostřednictvím internetu a kdo všechno má přístup k těmto informacím.

V této části práce zaměřené právě na soukromí na internetu definuji pojem „osobní informace", uvedu možné bezpečnostní hrozby, které se soukromí a osobních informací týkají, zaměřím se na to, jak se na tuto problematiku dívají zákony a různá doporučení, a na závěr uvedu přehled zdrojů, které se tématu soukromí věnují detailněji.

[2] „Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones." [vlastní překlad]
WEITZNER, Danny. We Can't Wait: Obama Administration Calls for A Consumer Privacy Bill of Rights for the Digital Age. In: *The White House Blog* [online]. Washington, D.C., 23. 2. 2012 [cit. 2012-04-04]. Dostupné z: http://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age

1.2 Osobní informace

Osobní informace je kostrou našeho soukromí. Legislativa na ni pamatuje v podobě zákona 101/2000 Sb. o ochraně osobních údajů. „Osobní informace“ je tu definována jako „jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“[3].

Mezi osobní informace, které jsou „náchylné“ ke zneužití na internetu, patří:

- PII (personally identifiable information)[4], což jsou osobní identifikační údaje, např. jméno a příjmení, datum a místo narození, státní příslušnost, rodinný stav, rodné číslo a číslo OP, adresa a telefonní číslo, elektronická adresa, atp, či osobnostní charakteristiky zahrnující fotografie nebo biometrické údaje;
- non-PII (non-PII information), tj. neosobní identifikační údaje, např. uživatelovo chování na webové stránce.

1.3 Entity ohrožující soukromí uživatele internetu

Soukromí a osobní informace mohou být díky velkému množství hrozeb v nebezpečí, neboť se staly výnosným artiklem ve světě obchodu. Kdo vlastní informace o svých zákaznících, může mnohem lépe zacílit reklamu na své produkty a tím i více vydělávat. Následuje přehled několika hrozeb, které se týkají narušení soukromí uživatele internetu a jež jsou nejčastěji zmiňovány v literatuře.

[3] Česká republika. Zákon č. 101/2000 Sb.: o ochraně osobních údajů. In: *Zákony ČR online*. § 4. 2011. [cit. 2012-04-02]. Dostupné z: http://www.zakonycr.cz/seznamy/101-2000-Sb-zakon-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu.html

[4] MCCALLISTER, Erika, Tim GRANCE a Karen SCARFONE. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology.* [online] National Institute of Standards and Technology: Computer Security Dicision. 2010, s. 2.1 – 2.2. [cit. 2012-04-02]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

1.3.1 Data mining

První z hrozeb je tzv. data mining. Jedná se o proces automatického sběru dat, při kterém se data extrahují z nejrůznějších databází, v nichž se skladují. Využívá se např. v oblasti competitive či business intelligence pro strategické či taktické rozhodování. Organizace ale také mohou např. sledovat, jaké stránky navštěvujeme, a filtrovat z nich informace potřebné pro následné zasílání cílených reklam, které jsou založeny na naší vyhledávací historii. Tyto reklamy se pak objevují ve formě nevyžádané pošty či nabídky produktů, které na nás „vyskočí" po dalším příchodu na stránku (jedná se o tzv. behaviorální cílení reklamy). Data mining totiž umožňuje vytváření šablon předpovědí, díky kterým je systém schopný naučit se uživatelovo chování na dané webové stránce.[5]

Data mining je jednou z nejdůležitějších oblastí, kterou pokrývají PET ve smyslu ochrany uživatele před nepřiměřeným sběrem dat.

1.3.2 Ztráta identity (identity theft)

„Krádež (zcizení) identity je nedovolené shromažďování a používání osobních údajů, obvykle za účelem kriminální činnosti."[6] Dostanou-li se uživatelovy osobní údaje do nepovolaných rukou, mohou být zneužity a uživatel následně poškozen. Ve světě internetu vzrůstá počet podvodů, jejichž předmětem je zcizování citlivých osobních informací zejména pro finanční prospěch, přičemž se peníze nejsnadněji získávají díky útokům na kreditní karty. Mezi takové útoky patří metody jako phishing nebo pharming.

1.3.3 Phishing

„Slovem phising se označují podvodné emailové útoky na uživatele internetu, jejichž cílem je vylákat důvěrné informace. Nejčastěji jsou to údaje k platebním kartám včetně PINu nebo různé přihlašovací údaje k účtům. Nemusí jít jenom o účty přímo bankovní, ale

[5] Guide to Data Mining: What is Data Mining?. *Data-Mining-Guide.net* [online]. © 2005 [cit. 2012-04-05]. Dostupné z: http://www.data-mining-guide.net/

[6] NYKODÝMOVÁ, Helena. Bojíte se krádeže své identity?. *Lupa.cz* [online]. 16. 8. 2006 6:30 [cit. 2012-04-24]. Dostupné z: http://www.lupa.cz/clanky/bojite-se-kradeze-sve-identity/

také ostatních organizací, kde dochází k manipulaci s penězi, např. PayPal, eBay, Skype či Google.“[7]

1.3.4 Pharming

„Pharming využívá speciální počítačové programy, které uživatele při přihlášení do internetového bankovnictví přesměrují na stránky, jež sice vypadají jako stránky jeho banky, ale ve skutečnosti jsou pouze jejich napodobeninou. Zde pak klienta požádají o zadání všech přihlašovacích hesel a kódů. Pokud tak klient učiní, mohou se neoprávnění uživatelé přihlásit do internetového bankovnictví pod jeho jménem […] a následně mu mohou nepozorovaně odčerpat peníze z jeho účtu.“[8]

1.3.5 Web Bugs

Web bugs (známé také jako *tracking bug*, *tag*, *tracking pixel*, *pixel tag či 1×1 gif)* jsou objekty umístěné na webové stránce nebo v emailu. Umožňují vzdálenou kontrolu činnosti uživatele bez jeho vědomí. Bugs sledují, jaké stránky uživatel navštívil a jak se na nich choval. Je jedním ze způsobů, jak sledovat, kdo zrovna čte danou webovou stránku, popř. email, kdy a z jakého počítače. Webové bugy, které mají na práci veškerou sledovací činnost, mohou mít podobu malého obrázku umístěného kdekoli na stránce nebo v emailu.

1.3.6 Spam

„Spam je nevyžádané sdělení (nejčastěji reklamní) masově šířené internetem. Původně se používalo především pro nevyžádané reklamní emaily, postupem času tento fenomén postihl i ostatní druhy internetové komunikace, např. diskusní fóra, komentáře

[7] Co je to phishing?. *Www.hoax.cz* [online]. 2010-2012 [cit. 2012-04-02]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing
[8] Phishing a Pharming. *Www.bezpecnyinternet.cz* [online]. [?] [cit. 2012-04-02]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

nebo instant messaging. Používá se též zkratka UBE/UCE (unsolicited bulk/commercial rmail).“[9]

1.3.7 Botnets

Jako poslední z hrozeb (nikoli ze všech možných) zde uvádím tzv. botnets, což je označení pro softwarové agenty nebo pro internetové roboty, kteří fungují zcela automaticky. Botnet označuje síť počítačů infikovaných speciálním softwarem, který je řízen z jednoho centra. Následně provádí nežádoucí činnost, jako je rozesílání spamu, DDoS útoky, rozšiřování virů, útoky na počítače a servery atd.[10]

1.4 Problematika ochrany soukromí na internetu z pohledu konsorcií a zákonů

Soukromí se stalo jednou z prioritních oblastí zájmů velkých institucí i vlád jednotlivých států po celém světě. S rozmachem internetu a informačních technologií se proto vyskytla potřeba soukromí chránit všemi dostupnými prostředky. Vedle technologií na ochranu soukromí vznikají proto různá doporučení, směrnice, ale i zákony, které prostor soukromí na internetu upravují a zabezpečují. Děje se tak v rámci jednotlivců, organizací, států, ale i v rámci celého světa.

Např. **Charta základních práv EU** říká, že „každý má právo na ochranu osobních údajů, které se ho týkají. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem.“[11]

[9] Spam. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 15. 3. 2012 [cit. 2012-04-02]. Dostupné z: http://cs.wikipedia.org/wiki/Spam
[10] What is botnet?. *Www.microsoft.com* [online]. © 2012 [cit. 2012-04-02]. Dostupné z: http://www.microsoft.com/security/resources/botnet-whatis.aspx
[11] Evropská unie. Článek 8: Ochrana osobních údajů. In: *Listina základních práv Evropské unie*. 2007. Dostupné z: http://eur-lex.europa.eu/cs/treaties/dat/32007X1214/htm/C2007303CS.01000101.htm

Příkladem je i další iniciativa EU, tzv. **Open Trusted Computing (OpenTC)**, která se zaměřuje na výzkum a rozvoj projektů týkajících se vzniku a rozvoje důvěryhodných a bezpečných systémů založených na open source modelech. Cílem OpenTC je ochrana proti hrozbám, chybám a závadám.[12]

Zákon č. 101/2000 Sb., o ochraně osobních údajů vymezuje práva a povinnosti správců systémů při zpracování osobních údajů v **§ 5**, kde se mmj. říká, že
„správce je povinen stanovit účel, k němuž mají být osobní údaje zpracovány, stanovit prostředky a způsob zpracování osobních údajů […], shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu, uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování […], zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny […]“[13].

Aktuálně vzniká řada nových dokumentů, které se o nutnosti ochrany soukromí a osobních informací vyjadřují taktéž, často s velkým apelem na rychlost, s jakou budou přijata opatření pro zajištěné této ochrany. Např. americký prezident Barack Obama v listině ***Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promting Innovation in the Global Digital Economy***[14] z února letošního roku, která se stala návrhem zákona o soukromí v informační éře, představuje tento návrh jako vodítko pro uživatele, aby věděli, co mohou očekávat od těch, kdo sbírají uživatelská osobní data, a nastavuje správcům manipulujícím s daty podmínky pro práci s daty.

[12]OpenTC. *Www.opentc.net* [online]. [?] [cit. 2012-04-02]. Dostupné z: http://www.opentc.net/index.php?option=com_content&task=view&id=29&Itemid=45
[13] Česká republika. Zákon č. 101/2000 Sb.: o ochraně osobních údajů. In: Zákony ČR online. § 5. 2011. [cit. 2012-04-02]. Dostupné z: http://www.zakonycr.cz/seznamy/101-2000-Sb-zakon-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu.html
[14] USA. Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promting Innovation in the Global Digital Economy. In: *The Consumer Privacy Bill of Rights*. Washington: The White House, 2012. Dostupné z: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

1.5 Možnosti ochrany soukromí a osobních dat na internetu dle doporučení

Všichni uživatelé znají „nějaké“ rady a doporučení, jak s internetem zacházet, čeho se vyvarovat a jak zvýšit bezpečnost při práci s ním. V následujících odstavcích se zaměřím na uvedení těch doporučení, která jsou často zmiňována jako základní a v různých zdrojích se o nich hovoří s podobným důrazem.

Tvůrcem takových doporučení je i **Federal Trade Commission**, která stanovila 5 principů ochrany soukromí, jež byly publikovány pod názvem *Fair Information Practice Principles*[15]. Jejich obsahem jsou tyto zásady:

- ***Notice/Awareness*** – za nejzákladnější princip je považován princip „varování“, kdy by uživatelům měly být poskytnuty informace o informační praxi předtím, než od nich budou vyžadována osobní data. Bez varování totiž uživatel nemůže učinit relevantní rozhodnutí zda vůbec, popř. v jakém rozsahu může svá data odhalit. K tomu, aby mohl uživatel správně rozhodnout, by měl znát tyto informace: identifikace toho, kdo data vyžaduje, kdo je sbírá, pro jaké účely budou data využita, komu budou případně data poskytnuta ve smyslu třetích stran, dále povahu toho, jak jsou data sbírána a jakými prostředky (např. přímá žádost či elektronické sledování), zda je poskytování údajů dobrovolné nebo povinné a jaké podmínky z obou variant vyplývají, a jakým způsobem ten, kdo data vyžaduje, zajišťuje např. zachování důvěrného charakteru poskytnutých dat.

- ***Choice/Consent*** – druhý základní princip je zaměřen na uživatelovu volbu a souhlas, čímž se rozumí poskytnutí alternativ uživateli o tom, jak mají být jím poskytnuté informace použity. Existují dva režimy voleb: „opt-in“, který vyžaduje souhlas ze strany uživatele ke sběru a/nebo použití informací, a „opt-out“ režim, který vyžaduje svolení k zamezení sběru a/nebo použití takových informací.

[15] *Fair Information Practice Principles*. *FEDERAL TRADE COMMISSION* [online]. [?], 2007 [cit. 2012-04-02]. Dostupné z: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

- ***Access/Participation*** se týká uživatelovy možnosti získat data o své osobě u správce dat a vznášet námitky proti případné nesprávnosti a neúplnosti.

- ***Integrity/Security*** – čtvrtý princip se týká správnosti a zabezpečení dat, jako je použití pouze solidních zdrojů dat, poskytování přístupu uživateli k datům a zničení nehodících se dat nebo jejich konverze do anonymní formy.

- ***Enforcement/Redress*** – je zřejmé, že základní principy ochrany soukromí mohou být efektivní pouze tehdy, pokud existuje mechanismus, který by je chránil. Mezi alternativní přístupy patří „samoregulace", dále „legislativa", která by vytvořila opatření pro uživatele, a/nebo „regulační schémata" vymahatelná skrze civilní a trestné postihy.

Podobně i **OECD** identifikuje následující *Fair Information Practices*[16]:

- **Collection Limitation –** sběr osobních dat by měl být omezen určitými limity a tato data by měla být získána férově a dle zákona.
- **Data Quality –** osobní data by měla být relevantní k účelu, pro který jsou používána.
- **Purpose Specification –** účel, pro který jsou data sbírána, by měl být specifikován ne později než ve chvíli, kdy jsou sbírána.
- **Use Limitation –** osobní data by neměla být odhalena, snadno k dispozici nebo jinak použita pro jiné účely než předem specifikované, kromě těch, jejichž odhalení je povoleno přímo samotným uživatelem nebo právní autoritou.
- **Security Safeguards –** osobní data by měla být chráněna uvážlivými opatřeními proti hrozbám, např. proti ztrátě nebo neautorizovanému přístupu, destrukci, modifikaci nebo zveřejnění dat.

[16] MCCALLISTER, Erika, Tim GRANCE a Karen SCARFONE. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology*. [online] National Institute of Standards and Technology: Computer Security Dicision. 2010, s. 2.3 – 2.4. [cit. 2012-04-02]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

- **Openness –** měla by existovat obecná ustanovení otevřeného přístupu ohledně rozvoje, praxe a politiky s respektem k osobním datům.
- **Accountability –** správce dat by měl být zodpovědný za míru splnění výše uvedeného.

Příkladem webového serveru, který poskytuje potřebné informace o online hrozbách a jejich prevenci, je **Get Safe Online**[17] server. Jeho tvůrci uvádí důležité rady, jak nebýt obětí počítačové kriminality a na co si dávat pozor.

Na prvním místě radí, abychom si své soukromé informace nechali pro sebe, popř. jak být při nakládání s nimi anonymní. Tvůrci webu vycházejí z otázky, proč zveřejňovat své osobní informace na internetu, když bychom je nikdy nedali komukoli na ulici. Následuje několik tipů, jak být na internetu anonymní:

- při zveřejňování osobních informací se držet hesla „dvakrát měř, jednou řež“,
- použít jednorázové, anonymní emailové účty pro webové stránky, které žádají emailovou adresu za účelem registrace (např. od Hotmail nebo Yahoo!, kteří poskytují volné emailové adresy),
- dávat si pozor na cookies,
- myslet na to, že naši komunikaci může někdo monitorovat,
- použít zašifrované odkazy pro citlivou komunikaci, např. VPN spojení s kanceláří;
- používat šifrování,
- použít bezpečný web během nakupování a online komunikaci s bankou,
- mít oddělený soukromý a pracovní účet,
- být opatrný při používání veřejně přístupných počítačů a Wi-Fi sítí a hotspotů,
- zkontrolovat, zda má webová stránka skutečně reálné telefonní číslo nebo adresu,
- číst si „politiky soukromí“ při registraci do služby,
- používat silná hesla a nikomu je nesdělovat,
- udržovat počítač zabezpečený a aktualizovaný.

[17] Protect your privacy. GET SAFE ONLINE. *Get Safe Online*: *Free expert advice* [online]. © 2012 [cit. 2012-04-02]. Dostupné z: http://www.getsafeonline.org/nqcontent.cfm?a_id=1132

1.6 Bližší informace o tématu

Tématem soukromí a jeho ochrany se v českém i zahraničním prostředí zabývá poměrně velké množství prací. V současné době je toto téma velmi aktuální, a proto se jejich počet rychle zvyšuje. Zabývají se i oblastmi, které mi rozsah této práce neumožnil pokrýt. Proto uvádím další odkazy na zdroje, které problematiku soukromí rozšiřují o různé pohledy.

Např. Helen Nissenbaum[18] se ve své práci zamýšlí nad problémy, kterým naše soukromí musí čelit. Jedná se např. o monitoring osob a činností, GPS navigační systémy, RFID technologie, skladování dat v masivních databázích, zveřejňování dat, online publikování, sociální sítě versus soukromí, technologie na sledování lidí, právo na soukromí atd. Zabývá se také soukromím po stránce etické a legislativní.

Zpráva *Privacy online: fair information practices in the electronic marketplace: a report to Congress*[19], která se stala výstupem amerického výzkumu zaměřeného na online obchody a nakupování ve vztahu ke zveřejňování osobních dat a odhalování soukromí, přináší zajímavé výsledky o tom, jaké informace jsou po uživatelích při nakupování požadovány a jaké informace jsou uživatelé ochotni poskytnout.

Soukromím se v českém prostředí zabývá i řada akademických prací, např. práce od Ivy Zadražilové[20], která věnuje pozornost informačním hrozbám na internetu, možnostem a technologiím, které porušují soukromí, či možnostem ochrany soukromí. V neposlední řadě se zamýšlí i nad trendy a budoucími tendencemi v oblasti soukromí.

Zahraniční disertační prací je *Building Values into the Design of Pervasive Mobile Technologies*[21] od Carol Shilton, která se zabývá tzv. „values-sensitive designem“, kdy

[18] NISSENBAUM, Helen Fay. *Privacy in context*: *technology, policy, and the integrity of social life*. Stanford, Calif.: Stanford University Press, 2010, 288 s., [cit. 2011-11-26]. Dostupné z WWW: <http://dl.dropbox.com/u/17936902/NISSENBAUM%20-%20Privacy%20in%20Context.pdf>. ISBN 978-0-8047-5237-4.

[19] FEDERAL TRADE COMMISSION. *Privacy online: fair information practices in the electronic marketplace*: *a report to Congress* [online]. 2000 [cit. 2012-04-02]. Dostupné z: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

[20] ZADRAŽILOVÁ, Iva. *Nebezpečí zneužití osobních informací v době globálního monitoringu s přihlédnutím k možnostem ochrany soukromí*. Brno: Masarykova univerzita, Filozofická fakulta, Ústav české literatury aknihovnictví, 2009. 143 s. Vedoucí bakalářské práce PhDr. Michal Lorenz.

[21] SHILTON, Katherine Carol . *Building Values into the Design of Pervasive Mobile Technologies* [online]. Los Angeles : University of California, 2011 [cit. 2011-04-04]. [pdf online]. Dostupné z WWW: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1866783>.

se věnuje soukromí a jeho hodnotám, které je potřeba implementovat do návrhů mobilních technologií. Těmito hodnotami jsou morálka, etika či sociální aspekty.

Bezpečnost a důvěryhodnost jsou nezbytnými vlastnostmi, které vyžadujeme po vstupu do kyberprostoru. Jak můžeme zajistit, aby naše soukromí, osobní data a informace byly zabezpečeny? V následující kapitole předkládám jedno z řešení v podobě technologií na ochranu soukromí na internetu, které se na tuto otázku zaměří po stránce legislativní a technologické.

2. PET('s)

V této stěžejní kapitole se zabývám definováním toho, co se skrývá pod označením PET, popř. PET's, jak na PET pohlíží projekty Evropské unie, dále se věnuji bližšímu popisu PET, příkladům a hrozbám, které se týkají soukromí uživatele na internetu.

Identifikování těchto hrozeb a technologií, které mohou být použity pro jejich ochranu, může poskytnout uspokojující ochranu soukromí v rámci všech sítí, které se dnes používají. Tyto technologie jsou známy jako Privacy Enhancing Technologies (PET) a pro českého čtenáře - uživatele internetu, nejsou tak známé, jak je tomu např. v USA nebo některých státech Evropské unie.

Právě proto je cílem této kapitoly především představení těchto technologií, jejich popis, princip fungování a zasazení do kontextu se soukromím na internetu a inteligentními SW agenty. Na téma se zaměřím z pohledu technologického, ale i legislativního.

2.1. Způsoby, jak dosáhnout ochrany soukromí na internetu

Jak již bylo řečeno v úvodu práce, tak PET představují nástroj na ochranu soukromí na internetu. Nejlepších výsledků ale dosahují ve spolupráci s dalšími možnostmi ochrany soukromí, které lze dle článku *Privacy-Enhancing Technologies – approaches and development*[22] dělit na:

- ochranu zabezpečenou vládou státu,
- ochranu za využití PET,
- samoregulaci, poctivou informační praxi, kodexy chování a
- vzdělávání uživatelů a IT profesionálů o informačním soukromí.

V předkládané práci nastíním ochranu zabezpečenou vládními i nevládními organizacemi, a především ochranu soukromí za využití PET.

[22] SENIČAR, Vanja, Borka JERMAN-BLAŽIČ a Tomaš KLOBUČAR. Privacy-Enhancing Technologies : approaches and development. *Computer Standards* [online]. 2003, roč. 25, č. 2, s. 147-158 [cit. 2012-04-03]. ISSN 09205489. DOI: 10.1016/S0920-5489(03)00003-5. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0920548903000035

2.1.1. Legislativa a projekty

Díky zvyšujícímu se vlivu internetu a přesouvání komerční sféry do jeho prostor se začala objevovat ve stále větší míře i bezpečnostní rizika pro uživatelovo soukromí. Proto začaly vznikat nejrůznější stupně ochrany po stránce legislativní, ať už v podobě doporučení, směrnic, kodexů nebo jednotlivých zákonů. V této práci se zaměřím na pohled především Evropské unie, která poměrně obsáhle a detailně pokrývá nejrůznější oblasti informačního soukromí.

V následujících odstavcích přiblížím iniciativu EU v procesu ochrany informačního soukromí uživatelů v rámci komunikačních sítí, především internetu, a to právě s přihlédnutím k implementaci PET do bezpečnostních opatření.

Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)

Tato směrnice EU definuje nutnost přijetí ochranných prostředků kvůli zvyšujícím se útokům proti informačnímu soukromí uživatele. Zabývá se např. tím, jak mají být zpracovávána data získaná od uživatelů, co už je považováno za nežádoucí jednání a doporučuje některé kroky ke zvýšení ochrany soukromí. Tato směrnice mmj. říká:

„[…] v případě sítí veřejných komunikací je nutno přijmout zvláštní právní, regulační a technická ustanovení na ochranu základních práv a svobod fyzických osob a ochranu oprávněných zájmů právnických osob, zejména s ohledem na zvyšující se kapacitu automatického uchovávání a zpracování údajů týkajících se účastníků a uživatelů […]. Tzv. špionážní software (spyware), webové štěnice (web bugs), skryté identifikátory a jiné podobné nástroje mohou pronikat do koncového zařízení uživatele bez jeho vědomí s cílem získat přístup k informacím, uchovávat skryté informace nebo sledovat činnost uživatele a mohou vážně narušit soukromí těchto uživatelů. Použití takových nástrojů by mělo být povoleno pouze k oprávněným účelům s vědomím uživatelů, kterých se dotýká.

[…] Pokud jsou takové nástroje, jako například ´cookies´, určeny pro oprávněný účel, jako je usnadnit poskytování služeb informační společnosti, jejich použití je povoleno pod podmínkou, že uživatelé jsou jasně a přesně informováni […] o účelu cookies či podobných nástrojů a je zajištěno, aby uživatelům byly známy informace, které se ukládají do koncového zařízení, jež používají. Uživatelé musí mít možnost odmítnout, aby cookies nebo podobné nástroje byly ukládány do jejich koncových zařízení […]. Metody podávání informací, nabízení práva odmítnout nebo vyžadování souhlasu je nutno provádět způsobem co možná nejvíce vstřícným vůči uživateli […]“[23].

Velký krok v zacházení s cookies podniká v současné době Velká Británie, která v nařízení *Guidance on the rules on use of cookies and similar technologies*[24], jehož autorem je nevládní organizace ICO (Information Commissioner's Office), specifikuje zacházení s cookies. Po jeho vstoupení v platnost, které je stanovené na 26. května 2012, musí webové stránky svým uživatelům říct, že se na nich cookies vyskytují, vysvětlit, jakou činnost vykonávají a získat uživatelův souhlas s uložením cookies na jeho zařízení. Toto nařízení se ale nebude týkat všech typů cookies, nepostihne např. ty cookies, které se využívají pro ukládání zboží do uživatelova nákupního košíku v elektronickém obchodě.[25]

[23] Evropská unie. Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací: Směrnice o soukromí a elektronických komunikacích. In: *Úřední věstník L 201*. 2002. [online]. [cit. 2012-04-03]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:CS:HTML

[24] Guidance on the rules on use of cookies and similar technologies. INFORMATION COMMISSIONER'S OFFICE. *Http://www.ico.gov.uk/* [online]. 2. vyd. 13. 12. 2011 [cit. 2012-04-21]. Dostupné z: http://www.ico.gov.uk/global/search.aspx?allwords=Guidance%20on%20the%20rules%20on%20use%20of%20cookies%20and%20similar%20technologies&collection=ico&start=0

[25] 'Action needed' to meet UK's cookie tracking deadline. In: *Www.bbc.com* [online]. 18. 4. 2012 [cit. 2012-04-21]. Dostupné z: http://www.bbc.com/news/technology-17745938

Sdělení Komise Evropskému parlamentu a Radě o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PET)

Další sdělení v rámci EU informuje především o možnostech ochrany soukromí za využití PET. Nachází se tu ale i zajímavý postřeh, a to že „[…] zatímco ve skutečnosti nesou právní odpovědnost za dodržování pravidel na ochranu údajů správci údajů, určitou odpovědnost za aspekty ochrany údajů ze společenského a etického hlediska nesou i jiné subjekty. To zahrnuje i ty, kteří navrhují technické specifikace a již ve skutečnosti vytvářejí anebo zavádějí aplikace anebo operační systémy.“[26]

Komise zastává názor, že PET by se měly rozvíjet a šíře využívat zejména tam, kde jsou osobní údaje zpracovávány prostřednictvím sítí ICT. Komise dále předpokládá, že širší používání PET by zlepšilo ochranu soukromí, stejně jako by napomohlo při plnění pravidel na ochranu osobních údajů. Využívání PET by mělo doplnit stávající právní rámec a donucovací mechanismy. Pokud mají být PET obecně využívány, musí být navrženy, vyvinuty a vyrobeny. Ačkoli tyto činnosti jsou již do určité míry prováděny ve veřejném a soukromém sektoru, Komise je toho názoru, že tyto činnosti je potřeba urychlit. Za tímto účelem je třeba stanovit potřebu PET a jejich technologické požadavky, přičemž v rámci výzkumu a technologického rozvoje by měly být vyvinuty odpovídající nástroje.[27]

[26] Evropská unie. Sdělení Komise Evropskému parlamentu a Radě o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PETs). [online]. Brusel, 2007, s. 3. [cit. 2012-04-03]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:CS:PDF

[27] Evropská unie. Sdělení Komise Evropskému parlamentu a Radě o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PETs). [online]. Brusel, 2007. [cit. 2012-04-03]. Dostupné z: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:CS:PDF

ENISA (European Network and Information Security Agency)

Obrázek 2 Logo projektu[28]

ENISA je evropská síťová a informační agentura, která pracuje pod záštitou EU. Cílem tohoto projektu je vytvořit z webu ENISA evropský rozcestník pro výměnu informací, zkušeností a znalostí na poli informační bezpečnosti. Základní misí Agentury je dosáhnout vysokého stupně efektivity síťové a informační bezpečnosti uvnitř EU. ENISA pomáhá Evropské komisi, členským státům a obchodnímu sektoru zabránit síťovým a informačním bezpečnostním problémům. ENISA se taktéž zabývá bezpečností v oblastech důvěryhodných aplikací a služeb (The Secure Applications and Services – SAS), v jejím hledáčku jsou mmj.:

- služby založené na cloudu,
- management rizik,
- zvyšování vzdělanosti a povědomí o rizicích,
- totožnost, soukromí a důvěryhodnost,
- odolnost veřejných komunikačních sítí a služeb.[29]

[28] ENISA: European Network and Information Security Agency. *Enisa* [logo online]. 2005-2012 [cit. 2012-04-03]. Dostupné z: http://www.enisa.europa.eu/
[29] ENISA: European Network and Information Security Agency. *Enisa* [online]. 2005-2012 [cit. 2012-04-03]. Dostupné z: http://www.enisa.europa.eu/

PRIME (Privacy and Identity Management for Europe)

Obrázek 3 Tzv. „PRIME toolbox“, který zahrnuje bezpečnostní prvky ve vztahu k různým prostředím[30]

Významný je i další z řady projektů zaměřených na zajištění ochrany soukromí na internetu. Jedná se o projekt PRIME, jehož smyslem je management soukromí a identity. Cílem PRIME je demonstrovat uskutečnitelná řešení pro „privacy enhancing identity management“ dodáním potřebného rámce, požadavků, architektury, designových směrnic, protokolů a prototypů, které jsou hodnoceny z multidisciplinární perspektivy.

Iniciativa PRIME vychází z vědomí, že se v dnešním online světě musí každá osoba vypořádat s množstvím účtů a datových nastavení. Díky tomu vzniká řada tzv. „neúplných identit“ („partial identities“) a má se za to, že budou hrát klíčovou roli v budoucnosti elektronických služeb stejně tak jako bezpečnost při jejich používání. PRIME se zaměřuje na řešení pro identity management, který zvyšuje bezpečnost, podporuje koncové uživatele a jejich soukromí.

V projektu se dovídáme mmj. o tom, že formou identity managementu je i rozhodování lidí, jaké informace, komu, kde atd. sdělí. Identita osoby se skládá z mnoha

[30] About PRIME. *PRIME* [obrázek online]. 2004-2012 [cit. 2012-04-03]. Dostupné z: https://www.prime-project.eu/about/

dílčích identit, kde každá reprezentuje osobu ve specifickém kontextu nebo roli. Identity management znamená výběr a rozvoj příslušných částečných identit s respektem k momentálním potřebám aplikací. Identity management systém kontrolovaný samotným uživatelem umožňuje vypořádat se s množstvím uživatelských účtů a hesel.

Cílem PRIME je poskytnout uživatelům kontrolu nad jejich osobními daty. Velkou důvěru vkládají právě do PET, o nichž se domnívají, že by měly být stále rozvíjeny a častěji implementovány.[31, 32]

2.2. Hrozby pro soukromí na internetu z pohledu PET

O hrozbách pro soukromí na internetu jsem se zmínila již výše v souvislosti s definováním soukromí a jeho možných hrozeb. Nyní se zaměřím na vytyčení těch hrozeb, které jsou z pohledu PET vyhodnoceny jako zásadní a na které si PET „troufá" po stránce jejich minimalizování, či úplného potlačení. Parafrázuji přitom článek *Privacy-Enhancing Technologies: approaches and development*[33], který se na hrozby z pohledu PET zaměřuje podrobněji.

2.2.1. HTTP chattering

Jednou z nejpoužívanějších služeb mezi komunikačními sítěmi je webové prohlížení umožněné HTTP protokolem. Protokol HTTP neumí uchovávat stav komunikace (tato vlastnost je nepříjemná pro implementaci složitějších procesů přes HTTP, např. internetový obchod potřebuje uchovávat informaci o identitě zákazníka, o obsahu jeho „nákupního košíku" apod.). K tomuto účelu byl protokol HTTP rozšířen o tzv. HTTP

[31] PRIME PROJECT. *Privacy and Identity Management for Europe* [online]. 2004-2012 [cit. 2012-04-03]. Dostupné z: https://www.prime-project.eu/

[32] Me, Myself and I! Manage your identities safely. *PRIME – Privacy and Identity Management for Europe* [online]. [?] [cit. 2012-04-03]. Dostupné z: https://www.prime-project.eu/press_room/leaflets/Prime-Primer-2pager.pdf

[33] SENIČAR, Vanja, Borka JERMAN-BLAŽIČ a Tomaš KLOBUČAR. Privacy-Enhancing Technologies : approaches and development. *Computer Standards* [online]. 2003, roč. 25, č. 2, s. 148-150 [cit. 2012-04-03]. ISSN 09205489. DOI: 10.1016/S0920-5489(03)00003-5. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0920548903000035

cookies, které umožňují serveru uchovávat informace o stavu komunikace na počítači uživatele. Cookies jsou v tomto případě mechanismem umožňujícím administrátorům identifikovat, buď podle jména nebo IP adresy, uživatele, který provedl na webové stránce nějaké operace nebo vyplnil data v nějakém formuláři.

2.2.2. COOKIES

Autoři Seničar, Jerman-Blažič a Klobučar[34] se ve svém článku zaměřují právě na cookies, v nichž vedle výhod spatřují i několik nebezpečných nevýhod. Uvádějí, že za cookie se v protokolu HTTP považuje malé množství dat, které WWW server pošle prohlížeči, jenž je uloží na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá serveru zpět. Cookies běžně nejsou nebezpečné, slouží např. k rozlišování jednotlivých uživatelů, ukládá se do nich obsah „nákupního košíku" v elektronických obchodech, uživatelské předvolby atd. Cookies byly ale také vytvořeny s úmyslem přesněji zamířit inzerci či monitorovat chování uživatele, zjistit jeho zájmy a preference atd. Cookies mohou být nebezpečné pro ochranu soukromí. Web, který navštívíme, je schopný si díky cookies ukládat libovolné informace o uživateli, které stránky a jak často navštěvuje, jaké informace vyhledává apod. Informace získané díky cookies lze snadno využít pro cílenou reklamu, pro výzkumy chování uživatelů na webové stránce aj. V cookies jsou často skladovány citlivé informace. Jejich obsahy jsou teoreticky přístupné komukoli schopnému zachytit cookies na internetu. Cookies mohou být nástrojem těchto nežádoucích aktivit:

2.2.2.1. Monitoring

Uživatelská identifikace skrze cookies je často považována za invazi do soukromí osob. Lidé mají svobodu vkročit do obchodu zcela anonymně a bez nakupování či aktivit, které jsou monitorovány nebo zaznamenávány. Legislativa zabývající se soukromím se domnívá, že by tomu tak mělo být i v online prostředí. Cookies dávají souhlas třetím stranám k prozkoumání aktivit jednotlivců, pokud mají přístup k jejich počítači a cookie

[34] Seničar, Jerman-Blažič a Klobučar, ref. 33.

souborům. Cookies tak mohou prozradit mnohé o uživatelově osobních informacích, preferencích, zvycích a chování na internetu aj.

2.2.2.2. Vyzrazení dat

Elektronické obchody, které získávají osobní informace o svých uživatelích, skladují data prostřednictvím cookies. Tato data mohou vyměňovat s jinými stránkami (obchodní partneři, reklamní partneři atd.). To naznačuje, že osobní informace dodávané dobrovolně na jedné stránce mohou být použity ke sledování nebo identifikování jednotlivce na jiných stránkách, kde by uživatel tato data nikdy dobrovolně nezveřejnil.

2.2.2.3. Omezená kontrola

Koncoví uživatelé mají velmi malou kontrolu nad obsahem a použitím cookies. Některé prohlížeče umožňují potlačit činnost cookies. Bohužel to ale může způsobit, že některé stránky nebudou fungovat vůbec. Ti, kdo se rozhodnou cookies akceptovat, nemají zaručeno, jak s nimi bude zacházeno a jak bude jejich obsah skladován a využíván.

2.2.2.4. Sběr dat

Cookies se dají také využít pro sběr osobních dat, pokud možno nenápadně, a to skrze mechanismy známé jako „webové bugy“[35].

2.2.3. E-Profiling

Jak článek[36] uvádí dále, tak cookies hrají svou roli i v činnosti zvané e-profiling. E-profiling je proces budování databází, které obsahují preference, aktivity a charakteristiky uživatele. Toto odvětví se významně rozrostlo s rozmachem elektronických

[35] viz tato práce, s. 15
[36] Seničar, Jerman-Blažič a Klobučar, ref. 33.

obchodů. Pro tyto databáze je příznačné, že schraňují reference milionů webových klientů. Mnoho obchodních webových stránek se spojuje s komerčními informačními firmami za účelem jisté provize. Tyto stránky umožňují díky cookies monitorovat klientovy aktivity na hostovské stránce a zaznamenat data, která byla poskytnuta webovému serveru. Uživatelovy zájmy, surfovací modely a volby při nakupování jsou skladovány pod jedním profilem v databázi bez vědomí či svolení uživatele. Tato informace je následně použita pro reklamu nebo služby, které mají být nabídnuty na přidružených webových stránkách. Organizace účastnící se těchto aktivit zdůrazňují, že tyto činnosti jsou v zájmu uživatelů, neboť jim poskytují více přizpůsobení a řízení služeb skrze web. Avšak mnozí vidí v e-profilingu porušení základních práv na soukromí, protože jsou data sbírána a distribuována bez souhlasu uživatele.

2.2.4. Embedded Software

Další z hrozeb na sebe může brát podobu softwaru, jehož hlavním principem není technologie, ani přenos dat, ale interakce s reálným světem. Embedded SW je vytvořen s cílem být implementován do elektroniky u aut, hraček, telefonů, robotů, bezpečnostních systémů, kardiostimulátorů, televizí a jiných nejen zábavních technologií. Tento SW se stává stále významnějším při vytváření designu aplikací pro letadla, rakety, zdravotní technologie atd.[37]

Embedded SW vytváří hrozby pro soukromí díky novým programovacím paradigmatům. Těmito jazyky jsou např. Java, JavaScript, XML a Active X. Povolují vzdáleným serverům spouštět aplikace na klientském počítači. Tyto jazyky mohou být zneužívány v komerčním sektoru, aby povolily elektronickému obchodu získat přístup k zákazníkově osobnímu prostředí a datům. Tato rizika stále více nabývají na významu, protože se internet stává rozšířeným kanálem především pro zábavní průmysl.

[37] LEE, Edward A. Embedded Software. In: *Advances in Computers* [online]. London: Academic Press, 2001 [cit. 2012-04-04]. Vol. 56. Dostupné z: http://ptolemy.eecs.berkeley.edu/publications/papers/02/embsoft/embsoftwre.pdf

2.3.Definice PET

Až dosud jsem hovořila o řadě nejen legislativních doporučení na používání PET a o hrozbách, které jsou z pohledu PET považovány za nejvýznamnější. V této části práce předchozí myšlenky rozvedu a přidám samotný základní popis PET ve smyslu technologií, uvedu příklady jejich použití a představím jejich architekturu.

Rozvoj ICT vede k tomu, že je daleko jednodušší než kdykoli předtím sbírat, ukládat, zpracovávat a poskytovat osobní data. Potenciální hrozby číhají na uživatele s mnohem větší intenzitou. Ty samé technologie, které soukromí ohrožují, mohou být použity k tomu, aby soukromí chránily, a nabízejí řešení v podobě „agentů", kteří uživateli dokáží dostatečnou ochranu poskytnout. Tyto technologie jsou známy jako Privacy Enhancing Technologies (PET). Cílem této práce je zaměřit se na pozitivní stránku PET a na to, jak mohou uživateli zabezpečit jeho soukromé informace a soukromí obecně.[38] Vycházet budu z poznatků PISA konsorcia.[39]

PET bývají charakterizovány jako schopnost a/nebo právo na ochranu našich osobních tajemství, nebo schopnost/právo zamezit napadání našeho osobního prostoru.[40] Jedná se o jednotný systém v rámci ICT zajišťující ochranu informačního soukromí tím, že vylučuje nebo minimalizuje osobní data anebo zamezuje zbytečnému a nechtěnému zpracování osobních dat, a to vše bez ztráty funkčnosti informačního systému.[41]

[38] PISA CONSORTIUM. *Handbook of Privacy and Privacy-Enhancing Technologies*: *The case of Intelligent Software Agents*. [online]. Haag: TNO-FEL, 2003. ISBN 90-74087-33-7. [cit. 2012-04-03]. Dostupné z: http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf
[39] PISA CONSORTIUM, ref. 38.
[40] SENIČAR, Vanja, Borka JERMAN-BLAŽIČ a Tomaš KLOBUČAR. Privacy-Enhancing Technologies : approaches and development. *Computer Standards* [online]. 2003, roč. 25, č. 2, s. 148 [cit. 2012-04-03]. ISSN 09205489. DOI: 10.1016/S0920-5489(03)00003-5. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0920548903000035
[41] PISA CONSORTIUM, ref. 38, s. [33].

Podle projektu PISA „[…] může využívání PET pomoci při navrhování informačních a komunikačních systémů a služeb tím, že minimalizuje sběr a využívání osobních údajů a usnadňuje dodržování pravidel na ochranu údajů“[42]. Komise ve své první zprávě o provádění směrnice o ochraně osobních údajů zastává názor, že „[…] využití vhodných technických opatření je nezbytným doplňkem právních prostředků a mělo by být nedílnou součástí při veškerém úsilí o dosažení dostatečné úrovně ochrany soukromí. Využívání PET by mělo vést k tomu, že porušování určitých pravidel na ochranu údajů se stane obtížnější a/nebo pomůže při jeho odhalování.“[43]

2.4. Historie a technické pozadí

Podle van Blarkoma, Borkinga a Olka[44] se poprvé o PET hovořilo v souvislosti s uveřejněním studie s názvem *Privacy-Enhancing Technologies – A Path to Anonymity* v roce 1995. Tato zpráva ukázala, že technologie mohou být použity jako prostředky ochrany jednotlivců proti zneužití jejich osobních dat tím, že redukují zpracovávání těchto osobních dat. Těmito technologiemi byly zamýšleny právě PET. Tím vešly PET do širšího povědomí a svět se o ně začal více zajímat. Teoretický model nebyl publikován až do roku 1997, kdy byl implementován poprvé jako komerční aplikace. ICL[45] v Holandsku navrhlo IS založený na pseudoidentitách v nemocničním informačním systému. Princip spočíval v tom, že každý pacient byl identifikován unikátní pseudoidentitou v rámci jedné domény, přičemž druhá doména byla vytvořena s cílem střežit identitu pacienta určeného unikátním identifikátorem. Pouze uživatelé s přístupovými právy mohli přistupovat k tzv. identity protectoru, který dosahoval vyššího stupně ochrany, tj. během jeho činnosti byl použit šifrovací protokol. Pseudoidentita byla odlišná pro každou pseudoidentity doménu, jednoduché autorizační schéma pouze umožňovalo přístup k těm doménám, které uživatel

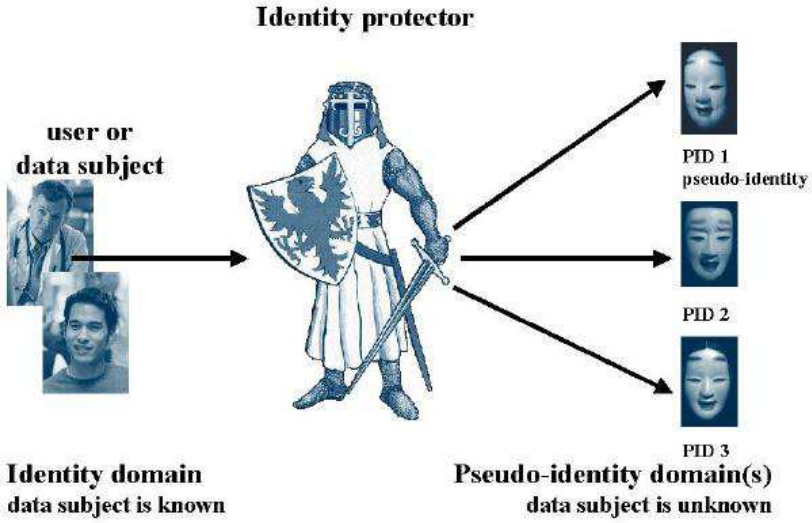
[42] Evropská unie. Sdělení Komise Evropskému parlamentu a Radě o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PETs). [online]. Brusel, 2007, s. 3. [cit. 2012-04-03]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:CS:PDF

[43] Sdělení Komise Evropskému parlamentu a Radě o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PETs), ref. 42.

[44] PISA CONSORTIUM, ref. 38, s. 33-50.

[45] ICL (International Computers Limited) byla velká britská společnost zabývající se počítačovým hardwarem, softwarem a počítačovými službami. Fungovala od r. 1968 do r. 2002, kdy byla převzata společností Fujitsu.

opravdu potřeboval na základě role, která mu byla přidělena díky jeho **user identity**. Přeměnu identity uživatele na jeho **pseudoidentitu** prostřednictvím tzv. **identity protectoru** naznačuje obrázek:



Obrázek 4 Činnost identity protectoru[46]

Autoři příručky[47] tyto prvky dále specifikují. Základním prvkem PET systému je tzv. **„identity protector“**, který slouží k implementaci věcí po stránce technické, s cílem konvertovat identitu datového subjektu, který je součástí jedné nebo více pseudoidentit. Identity protector poskytuje nejméně dvě různé domény uvnitř datového systému. Jedna doména, kde je zahrnutá identita známá - **identity domain**, a jedna, kde je tomu naopak - **pseudoidentity domain**. Cílem pseudoidentity je zaručit osobám, že nemohou být identifikovány. Identity protector v IS může mít několik forem, např.: samostatnou funkci implementovanou v systému, samostatný systém spravovaný uživatelem (např. smart card v případě biometrické identifikace) a datový systém spravovaný stranou pověřenou poskytovatelem služeb a zákazníkem (Trusted Third Party - TTP).

Použití identity protectoru umožňuje preventivně zasáhnout uvnitř datového systému s cílem skrýt identity zúčastněné osoby. Dalšími řešeními jsou také digitální podpis,

[46] PISA CONSORTIUM, [obrázek], ref. 38, s. 37.
[47] PISA CONSORTIUM, ref. 38, s. 33-50.

digitální pseudonym, digitální certifikáty a MIX nodes (tj. procesor, který pro zpracování vezme jistý počet zpráv, které modifikuje a provádí jejich výstup v náhodném pořadí).

Jedním z nejdůležitějších principů ochrany soukromí je, že už více dat nemusí být sbíráno nebo zpracováváno, než je nezbytně nutné pro daný účel. Existuje samozřejmě více možností, jak zajistit ochranu dat, ale technická řešení jsou velmi efektivní právě proto, že se jim nelze vyhnout. Volba technických řešení v podobě PET je závislá na stupni ochrany, který je vyžadován podle toho, jaká rizika se vyskytují. Projekt PISA využívá PET k ochraně osobních dat s tradičními PET součástmi, jako jsou právě identity protector a vytvoření anonymní domény nebo pseudoidentitní domény.

Poté, co bylo dosaženo implementace PET, ICT průmysl se začal velmi zajímat o možnosti PET. Bylo ustanoveno 7 principů PET[48]:

1. **Omezení sběru osobních dat** – sběr dat musí být přiměřený, relevantní a ne nadměrný ve vztahu k účelu, pro který jsou data sbírána, a/nebo zpracovávána.

2. **Identifikace/ověření/oprávnění** – uživatel informačního systému zpracovávajícího osobní data musí zpracovávat pouze osobní data z důvodné potřeby v nezbytně nutném rozsahu („need-to-know basis“).

3. **Standardní technologie použité pro ochranu soukromí** – např. anonymizační nástroje, které zaručují, že uživatel smí využít službu bez toho, aniž by odhalil svá osobní data. Tyto nástroje nejsou primárně určeny k tomu, aby zcela skryly uživatelovu identitu, ale spíše aby zajistily, že data, která jsou nějakým způsobem zpracovávána, nebudou skladována déle než na nezbytně dlouhou dobu. Např.: není nutné znát přesnou profesi uživatele, zcela postačuje znát oblast, v níž uživatel pracuje.

4. **Pseudoidentita** – patří mezi základní principy PET.

[48] PISA CONSORTIUM, ref. 38, s. 37-42.

5. **Šifrování** – je typickým příkladem technologií, které mohou pomoci chránit data. Jedná se o hlavní způsob, jak zajistit důvěrnost a zabezpečit „tajný“ charakter dat. Za všech okolností, kde je důvěra nejdůležitějším tématem, je šifrování možným řešením zabezpečení její ochrany. Příklady použití šifrování: bezpečné skladování dat, autorizace subjektu v systému, přístup k datům a zveřejnění dat, přenos dat aj.

6. **Biometrika** – jedná se o velkou příležitost i hrozbu zároveň. Je dalším příkladem technologie, která může fungovat jako PET. Vedle klasických zabezpečení při autorizaci, jako je např. heslo k přístupu, lze využít i biometrické údaje, které přesně identifikují subjekt bez toho, aby je bylo možné zneužít jednoduchým způsobem. Heslo lze snadno zapomenout, ztratit nebo nechat ležet vedle klávesnice, přičemž jsou osobní data vystavena velkému riziku. Heslo nezaručuje správnou identitu uživatele. Ten, kdo heslo použil, nemusí být ten, kdo má mít k datům přístup. Biometrické údaje jsou jednoznačné a „nosíme“ je stále s sebou, patří mezi ně např. otisky prstů, sken sítnice, tvar ucha aj.

7. **Schopnost kontroly** – PET jsou ideálním nástrojem pro kontrolu a správu ze strany kontrolorů, kterými mohou být různé správní agentury, vlády či organizace zajišťující ochranu soukromí po stránce technické i teoretické. Zajímají se především o popis systémů, které jsou použity při zpracování osobních údajů, a monitoring subjektů, které zpracovávají osobní data. Užitečné, ale v nepovolaných rukou z hlediska právního i etického velmi nebezpečné.

Těchto sedm principů bylo ustanoveno mmj. proto, aby vedly designery informačních systémů k dalším návrhům systémů s implementovanými PET. Design PET systému je nekončící proces. Vždy je třeba jej zdokonalovat a posouvat kupředu. V této souvislosti se hovoří i o designu soukromí („privacy by design“), kdy se uvažuje nad tím, jak navrhnout technická zabezpečení s ohledem k soukromí subjektů. Při návrhu designu se klade důraz na převod zákonů, doporučení a směrnic do technických specifikací a do strojově čitelných kódů. Bylo definováno 9 oblastí[49] pro design PET, které je při návrhu PET nutné zohlednit:

[49] PISA CONSORTIUM, ref. 38, s. 49-50.

1. Záměr a uvědomění *(Intention and notification)*

2. Průhlednost *(Transparency)*

3. Definitivní pravidla *(Finality principle)*

4. Zákonný podklad pro zpracovávání *(Legitimate grounds of processing)*

5. Kvalita *(Quality)*

6. Práva subjektu údajů *(Data subject's rights)*

7. Bezpečnost *(Security)*

8. Zpracovávání procesorem *(Processing by a processor)*

9. Přenos osobních dat mimo EU *(Transfer of personal data outside the EU)*

Některé části jsou pro implementaci do systému jednodušší, např. „Security", ale některé jsou naopak velkým oříškem. Tím je právě oblast „Data subject's rights", která se řeší spíše po stránce legislativní.

PET se týkají i dva doplňující přístupy integrace. Prvním je přístup, který předpokládá plnou integraci PET do existujících informačních systémů. Druhý přístup předpokládá rozvoj prostředků, které mohou být použity subjekty v momentě, kdy pracují s informacemi. V tomto případě může být funkcionalita PET „vypnuta" v rámci defaultního nastavení a v případě, kdy jsou PET vyžadovány pro podporu určité činnosti, tak mohou být zase „zapnuty". Do těchto dvou skupin lze zařadit tyto PET[50]:

Integrated PET - PET mohou být integrovány do několika částí IS. Vhodným způsobem, jak toho dosáhnout, je brát v úvahu PET již ve fázi vytváření designu IS.

ICT Networks - v ICT sítích se hovoří o dvou aplikacích PET: **MIX Routes** a **Onion Routers**. Tyto dvě aplikace umožňují uživatelům komunikovat spolu navzájem bez toho, aniž by tuto komunikaci odposlouchával někdo jiný. Obě aplikace jsou založeny na síťových routerech (směrovačích). Routery se v sítích starají o odesílání datových paketů. Datové pakety vznikají a jsou doručovány do počítačů v rámci sítě. Směrování je založeno na adresách, díky nimž router ví, kam má datové pakety poslat. Každému počítači je přidělena unikátní síťová adresa. Mezi příchozími a odchozími pakety je fixní vztah. To

[50] PISA CONSORTIUM, ref. 38, s. 51-52.

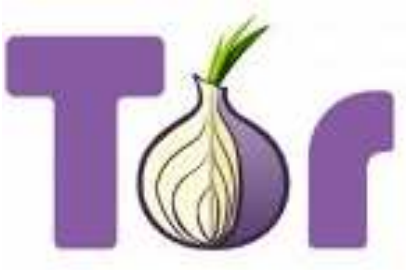
umožňuje analyzovat komunikační pohyb skrze routery a tak určovat, který počítač zrovna komunikuje. MIX Routes a Onion koncept staví překážky mezi příchozí a odchozí datové pakety, čímž zamezují nebo znesnadňují analýzu komunikačního pohybu a navazují vztah mezi přijímacími a odesílajícími počítači.

Information Systems - jedná se o systémy a aplikace, které zabraňují podvodnému užití osobních dat, která jsou uchovávána v databázích. Osobní data jsou často skladována v databázích s odkazem na unikátní klíč, jako např. identifikační číslo pacienta. Osoby s přístupem do databáze mohou získat všechna data spojená s tímto klíčem, dokonce i když data nejsou osobou požadována. Podvodnému užití osobních dat může být zabráněno implementací silného přístupového kontrolního mechanismu založeného na uživatelských skupinách kombinovaných s mechanismem, který rozpojuje skupiny osobních dat od sebe. Rozpojení je dosaženo použitím pseudoidentit. Spojení mezi identitami a pseudoidentitami je uchováváno na přístupovém kontrolním seznamu a je přiřazováno k přístupovým právům založeným na účelu přístupu dané osoby do databáze.

Anonymisers - anonymizér je pomůcka určená k využívání služeb v rámci ICT sítí anonymně. Jedná se o SW program, jež filtruje identifikovatelná osobní data z dat, která jsou vyžadována k navázání kontaktu v síti. Jedná se především o data typu: síťová adresa, typ operačního systému, informace o používaném SW aj. Anonymizační program nahrazuje informace informacemi, které neumožňují dohledání uživatele.

Příkladem anonymizačního nástroje je služba TOR[51], která umožňuje např. rodinám chránit své děti při práci na internetu, média využívají TOR k ochraně svých zdrojů, aktivisté za lidská práva díky němu mohou podávat zprávy z nebezpečných zón po celém světě, armáda prostřednictvím TORu zabezpečuje svou komunikaci atd.

[51] THE TOR PROJECT. *Tor*: *Anonymity Online* [online]. [2012] [cit. 2012-04-17]. Dostupné z: https://www.torproject.org/index.html.en



Obrázek 5 Logo TOR projektu[52]

Profile Managers - profile managers umožňují uživateli vytvořit několik profilů, které mohou být považovány za pseudoidentity. Různé profily mohou být spravovány různými způsoby, čímž lze zvýšit bezpečí uživatelova soukromí.[53]

2.5.Architektura – příklady PET

Příkladů a typů PET je poměrně velké množství. Jejich typologie se liší. Mohou to být nezávislé nástroje, které vyžadují pozitivní akci na straně spotřebitelů (kteří si je musí koupit a instalovat do svých PC), anebo mohou být zabudovány do samotné architektury informačních systémů. Lze uvést několik příkladů PET:

- „Automatická **anonymizace** údajů po uplynutí určité doby podporuje zásadu, že zpracovávané údaje by měly být uchovávány ve formě, která umožňuje identifikaci subjektů údajů pouze na dobu, která je pro účely, na které se údaje původně sbíraly, nezbytná.
- **Kódovací nástroje** zabraňující neoprávněnému přístupu při přenosu informací přes internet umožňují správci údajů splnit jeho povinnost přijmout vhodná opatření na ochranu osobních údajů proti neoprávněnému zpracování.

[52] THE TOR PROJECT. *Tor*: *Anonymity Online* [logo online]. [2012] [cit. 2012-04-17]. Dostupné z: https://www.torproject.org/index.html.en
[53] PISA CONSORTIUM. *Handbook of Privacy and Privacy-Enhancing Technologies*: *The case of Intelligent Software Agents*. [online]. Haag: TNO-FEL, 2003. ISBN 90-74087-33-7. [cit. 2012-04-03]. Dostupné z: http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf

- **Nástroje blokující cookies** umístěné na uživatelově PC za účelem vykonávání určitých pokynů bez příkazu uživatele podporují dodržování zásady, že údaje se musí zpracovávat spravedlivě a zákonně a že subjekt údajů musí být o probíhajícím zpracování informován.
- **Platforma P3P** (The Platform for Privacy Preference) umožňující uživatelům internetu analyzovat metody internetových stránek, pokud jde o ochranu soukromí, a porovnávat je s preferencemi uživatele, pokud jde o informace, které si přejí zveřejnit, a napomáhá zabezpečit, aby subjekty údajů poskytovaly souhlas se zpracováním svých údajů na základě jim sdělených dostatečných informací.“[54]

Z výzkumu Rolfa Oppligera[55] vyplývá, že PET mohou být použity k poskytnutí anonymity, anonymizačních služeb na webu, pro anonymní surfování i publikování. Ačkoli se zdá být brouzdání na internetu anonymní, tak tomu je přesně naopak. Libovolný webový server obvykle zaznamená každý HTTP požadavek, to samé platí pro HTTP proxy servery, které jsou lokalizovatelné díky cestě, kterou putují nejrůznější zprávy. Podobně i publikování na webu vždy vyžaduje odhalení URL, přičemž částí tohoto URL je i IP adresa nebo host name serveru, který hostí požadované zdroje.

Otázky zní: jak může uživatel zůstat anonymní, zatímco brouzdá po internetu? Jak mohou entity zůstat anonymní při publikování na internetu? Řešením se zdá být PET, i když i ty s sebou nesou určité problémy. Např. jejich zneužití kriminálními živly, aby se vyhnuly monitorování své činnosti ze strany vymáhání práva a národních bezpečnostních složek. Také při publikování je problém v tom, že PET mohou být zneužity pro prodej drog, dětskou pornografii a pro šíření propagandistických materiálů od extremistů.

Z průzkumu vzešlo několik příkladů PET, které mohou určit a řešit problém anonymního surfování. Strukturovány jsou dle toho, zda náleží do oblasti anonymního surfování nebo publikování na internetu.

---

[54] Evropská unie. Sdělení Komise Evropskému parlamentu a Radě o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PETs). [online]. Brusel, 2007, s. 3-4. [cit. 2012-04-03]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:CS:PDF

[55] OPPLIGER, Rolf. Privacy-enhancing technologies for the world wide web: Short Survey. *Science Direct* [online]. 2005[cit. 2012-04-03]. Dostupné z: http://www.sciencedirect.com/science/article/pii/S0140366405000691

A. Anonymní surfování

a. ANONYMIZING HTTP PROXY SERVER (AHPS[56])

Jedná se o nejjednodušší způsob, jak anonymně surfovat. AHPS mohou skrýt IP adresu prohlížeče. Webový server totiž nepotřebuje znát nic o klientově platformě a prohlížeči, který používá, proto tyto kousky informací mohou být odstraněny z odpovídajících HTTP požadavků. Mnoho AHPS zvládá tzv. „nested URL“, což je URL, ve kterém dokumentová část URL odkazuje k jinému URL.

Např.: *http://proxy.service.com/http://www.esecurity.ch*

Při obdržení „nested URL“ se prohlížeč nejprve spojí s HTTP proxy serverem běžícím na *proxy.service.com* a toto proxy se poté spojí s *www.esecurity.ch*. Podobně jako anonymní remailery, i použití AHPS může být vázané, přičemž může být použita spousta odpovídajících serverů (místo jediného HTTP proxy serveru).

Pokud není použit AHPS vázaný (tj. URL je vždy vyžadováno skrze jeden AHPS), pak může být použit tzv. SSL protokol (Secure Sockets Layer) nebo TLS protokol (Transport Layer Security) pro další zvýšení ochrany, jelikož v SSL/TLS chráněné datové výměně je celý datový provoz zašifrovaný.

Je mnoho společností a organizací, které spravují AHPS a poskytují korespondenční anonymní služby pro webové uživatele, např. anonymizer.com.

b. CROWDS

Další alternativa vedle výše zmíněné byla vyvinuta v 90. letech v rámci systému jménem CROWDS. Systém je založen na myšlence, že lidé mohou být anonymní, když se přimísí do davu. Proto každý člen davu musí pracovat s anonymním HTTP proxy serverem, který také musí být použit ostatními členy davu. Tato myšlenka je všudypřítomná v P2P tak, jak ji známe dnes. Oproti tradičním P2P konceptům ale CROWDS také přicházejí s nápadem pravděpodobnostního postupu. Tzn., že každý HTTP

[56] Zkráceno pro vlastní potřebu, nejedná se o oficiálně používanou zkratku.

požadavek na zprávu je pravděpodobnostně směrován k náhodně vybranému číslu náhodně vybraných členů davu předtím, než je odeslán do cílové destinace. Cílová destinace požadované zprávy přišla od člena davu, neříká ovšem od koho.

B. Anonymní publikování

a. REWEBBERS

Jedná se o službu, která vychází z německého výzkumu a rozvojového projektu JANUS[57]. Poskytuje anonymní služby pro prohlížeče i nakladatele. K poskytování anonymních služeb pro prohlížeče se rewebber chová jako AHPS podporující SSL/TLS protokol. K poskytnutí anonymních služeb pro webové publikování rewebber servis používá zakódovaná URL, která jsou součástí „nested URL“.

Rewebbery poskytují jednoduchý, ale účinný způsob podpory pro anonymní publikování na webu. Existuje tu ale několik omezení, na která se nesmí zapomínat, když se uvažuje nad širokým uplatněním rewebberů:

- Poskytovatel rewebberů musí být důvěryhodný, nesmí odhalovat nezašifrovaná nebo dekódovaná URL.
- Ti, co publikují, musí zpřístupnit zakódovaná URL.
- Uživatel musí zadat zašifrovaná URL.

b. ETERNITY služby

V 90. letech byla poprvé publikována myšlenka o věčných službách. Tato idea spočívá v tom, že se implementuje médium založené na skladovacím serveru, které je odolné vůči útokům na služby a destrukci zúčastněných serverů. Uživatel, který si přeje publikovat dokument, předloží jej do „Eternity“ služby. Eternity server pak zkopíruje dokument na náhodnou podmnožinu Eternity serverů. Jednou takto předaný dokument nemůže být z Eternity serveru vymazán. Proto autor nemůže být nucený smazat dokument

[57] Projekt Janus je zaměřen na tvorbu a vývoj multiagentních aplikací.
Více na: http://www.janus-project.org/Home

publikovaný v této službě. První implementace Eternity služeb se objevila v r. 1997. Od té doby byla tato idea dále zpřesňována v mnoha výzkumech a rozvojových projektech.

Př.:

FREENET[58] používá decentralizovanou P2P architekturu, v ní každý uživatel musí poskytnout úložný prostor. Každý soubor je skladován a kopírován na více serverů. Pokud někdo požaduje soubor, požadavek je vyslán, dokud není dosaženo serveru, který skladuje soubor. Tento soubor je pak poslán zpět uživateli. Soubory jsou zakódovány a náležitý dekódovací klíč je k dispozici pouze legitimním příjemcům souboru.

FREE HAVEN[59] podobně jako Freenet používá decentralizovanou P2P architekturu k implementaci Eternity-like služeb k ukládání dat. Cílem projektu je zavést systém pro distribuované, anonymní, trvalé ukládání dat, které je odolné vůči pokusům silných protivníků najít a zničit všechna uložená data.

Existuje mnoho druhů PET, které se liší svojí architekturou, činností, účelem apod. Pro účely této práce jsem proto vybrala ty, které jsou dle literatury k tomuto tématu považovány za významné a rozšířené, popř. k tomu směřují. Pro bližší seznámení s tematikou PET ale také uvádím další zdroje, v nichž se čtenář může s PET seznámit podrobněji.

[58] https://freenetproject.org/
[59] http://www.freehaven.net/

2.6.Bližší informace o tématu

PET se neustále vyvíjejí a jsou na ně kladeny stále větší nároky. Proto lze i v zahraničních zdrojích ve větší míře nalézat nové informace o PET.

Základním pilířem se v tomto ohledu staly výstupy z Mezinárodního sympózia PET[60] konaného každý rok s cílem představit nové skutečnosti, design či technologie PET. V roce 2012 se koná již 12. setkání. Dosud ke každému ročníku vyšla i sbírka článků, které shrnují probíraná témata. Od prvotního definování a vymezování PET vývoj pokročil k velmi sofistikovaným možnostem, které se sympózium vždy snaží zachytit a představit veřejnosti. Výstupy z tohoto sympózia považuji za komplexní přehled o problematice PET.

Roger Clarke[61] na svých webových stránkách zasvěcuje uživatele do základů PET. Kromě toho ale také vymezuje „protiklad" PET, kterými jsou dle něj tzv. PITs (Privacy Invasive Technologies), tj. technologie, které soukromí nějakým způsobem narušují. Jako příklad uvádí skladování dat či biometrických údajů.

White Paper for Decision-Makers[62] také přibližuje problematiku soukromí a PET, ale tentokrát z pozice designu těchto technologií. PET jsou tu pojímány jako atraktivní, dosažitelné a zcela nezbytné prostředky na ochranu soukromí na internetu. Odpovídá se tu na otázky, co mohu od PET očekávat? Proč používat právě PET? Jednou z možných odpovědí je tu přitom tato: PET zvyšují hygienu informačního systému. Tento zdroj je psán populárnější formou a nabízí na PET různé úhly pohledu.

---

[60] O zatím posledním konaném ročníku:
11. sympózium: FISCHER-HÜBNER, Simone a Nicholas HOPPER. *Privacy Enhancing Technologies : 11th International Symposium, PETS 2011 Waterloo, ON, Canada, July 27-29, 2011 Proceedings* [online]. ? : Springer, 2011 [cit. 2011-03-26]. Dostupné z WWW: <http://dl.dropbox.com/u/17936902/Privacy%20enhancing%20technologies.pdf>. ISBN 978-3-642-22262-7.

[61] CLARKE, Roger. Introducing PITs and PETs: Technologies Affecting Privacy. In *Roger Clarke's Web-Site* [online]. Chapman, Australia : Xamax Consultancy Pty, 2001, 2003 [cit. 2011-11-26]. Dostupné z WWW: <http://www.rogerclarke.com/DV/PITsPETs.html#GPETs>.

[62] KOORN, Ronald (ed.). *Privacy Enhancing Technologies : White Paper for Decision-Makers* [online]. 1. Nizozemí : Ministry of the Interior and Kingdom Relations, 2004 [cit. 2012-04-16]. Dostupné z WWW: <http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf>.

Výzkum EU *Study on the economic benefits of privacy enhancing technologies (PET's)*[63], se zaměřil na ekonomické benefity PET pro organizace a instituce, které používají osobní data, nebo je zpracovávají. Do výzkumného vzorku byla zahrnuta i Česká republika. Teoretická část výzkumu dává dohromady různé definice a názory na PET, jedná se tedy o komplexnější pohled na problematiku PET.

Stále více informací o soukromí, PET a jejich legislativnímu pokrytí lze najít na webových stránkách amerického Bílého domu[64], kde jsou k dispozici aktuální rozhodnutí, listiny, návrhy zákonů i zákony týkající se této problematiky. USA je totiž stejně jako EU velmi přísným arbitrem, co se týče požadavků na zabezpečení soukromí svých obyvatel.

Další příklady využití PET uvádí CIS PET wiki databáze[65]. CIS (The Center for Internet and Society at Stanford Law School)[66] je škola, kterou založil Lawrence Lessig a která se zabývá právem a politikou spjatými s internetem. Pokud se někdo zabývá novými technologiemi, aplikacemi, službami, internetem a mnohým dalším po stránce legislativní, pak je to právě CIS, který v komplexním přehledu uvádí a analyzuje aktuální trendy, hrozby či možnosti. CIS wiki databáze PET technologií a aplikací uvádí jejich ucelený přehled s odkazy a popisem. Uživatel má tak možnost vyzkoušet si např. nějaký anonymizační nástroj v praxi.

[63] Promoting Data Protection by Privacy Enhancing Technologies (PETs). *Europa.eu* [online]. 2007, [cit. 2011-11-28]. Dostupný z WWW: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/598&format=HTML&aged=0&language=EN&guiLanguage=en>
[64] http://www.whitehouse.gov/
[65] The Center for Internet and Society. *PET* [wiki databáze online]. Stanford, 2011 [cit. 05. 04. 2012]. Dostupné z: http://cyberlaw.stanford.edu/wiki/index.php/PET
[66] http://cyberlaw.stanford.edu/

3. ISA

„Agent je softwarová věc, která ví, jak dělat jiné věci,
které byste pravděpodobně dělali, kdybyste měli čas.“[67]
(Ted Selker, IBM)

Příkladem situace, kdy je užití PET více než vhodné, je oblast zahrnující tzv. „intelligent software agents“ (ISA, agenti, knowbot, taskbot, userbot, robot, personal assistant, transport agent, cyber agent, search agent, role agent, management agent, search agent aj.). ISA může být na jedné straně hodný a velice užitečný sluha, ale na straně druhé poměrně nebezpečný pán.

Kapitoly, které následují, definují inteligentní agenty a jejich činnost a přibližují vztah mezi agenty, soukromím a PET. Agenti jsou totiž považováni za významný příklad užití PET v praxi. Dále se budu zabývat jejich představením.

3.1. Definice

Rozmach internetu s sebou přináší mmj. jeden aspekt, se kterým se uživatelé musí vyrovnat. Jedná se o nadbytek informací („information overload“, informační přetížení) různého charakteru, v jejichž záplavě se často ztrácíme a hledáme způsob, jak z toho co nejlépe „vybruslit“, v tomto případě s informací, kterou jsme hledali. Je pro nás totiž stále těžší takové informace najít, navíc tím ztrácíme spoustu času.

Jakými způsoby lze k informaci dojít? Klasickým řešením je sednout si za počítač a hledat v dostupných zdrojích, co zrovna potřebujeme. Alternativním řešením je použít

[67] *„An agent is a software thing that knows how to do things that you could probably do yourself if you had the time.“* [vlastní překlad]
JANCA, Peter. *Pragmatic Application of Information Agents*. Norwell, United States: BIS Strategic Decisions, 1995. Podle: PISA CONSORTIUM. *Handbook of Privacy and Privacy-Enhancing Technologies*: *The case of Intelligent Software Agents*. [online]. Haag: TNO-FEL, 2003, s. 56. ISBN 90-74087-33-7. [cit. 2012-04-03].
Dostupné z: http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf

inteligentní agenty, kteří tuto práci vykonají za nás. Jedná se totiž o software, který vykonává úlohy s minimálním úsilím uživatele. Agent pracuje na počítači uživatele, ale může se také pohybovat na internetu nebo v jiných síťových infrastrukturách. Agent pomáhá uživateli zbavit se rutinních úkolů. Uživatel má pak více času na to, co je opravdu důležité.

Definice agentů není přesně daná. Jedná se totiž o součást umělé inteligence („artificial intelligence, AI“) , při jejímž definování se odborníci také rozcházejí. S AI mají agenti společné to, že jsou schopni se učit a uvažovat.[68]

Václav Matoušek ve své prezentaci[69] charakterizuje ISA na základě čtyř charakteristik, z nichž je patrné, jak agenti ve své podstatě fungují:

- **Autonomní působnost** = agent je schopný provádět úkoly bez interakce s uživatelem. Uživateli stačí, aby agentovi specifikoval činnost, kterou má vykonávat, kdy a na jakém místě. Agent plní úkol ve chvíli, kdy nastanou dané podmínky.
- **Přizpůsobivé chování =** agent se učí z jednotlivých kroků, které uživatel učiní při provádění úlohy. Agent je tak schopný zapamatovat si uživatelovy reakce na různé situace a podle toho příště sám rozhodovat.
- **Mobilnost** = „schopnost volně procházet počítačovými sítěmi a vykonávat úlohy na vzdálených místech. Agenti jsou většinou tvořeni přeložitelným skriptem, který napomáhá bezproblémovému pohybu přes různé architektury sítí. Např. komunikačně orientovaný skript jako Telescript může ulehčit vzájemnou komunikaci mezi jinými agenty, které jsou uloženy na odlišných procesorech“[70].
- **Kooperativní chování** = „schopnost dvousměrné komunikace mezi agenty. Např. pan X pošle panu Y elektronický dopis, který musí být neprodleně doručen. Agent nesoucí dopis od pana X se spojí s agentem pana Y a ten mu

[68] PISA CONSORTIUM. *Handbook of Privacy and Privacy-Enhancing Technologies*: *The case of Intelligent Software Agents*. [online]. Haag: TNO-FEL, 2003, s. [55]-58. ISBN 90-74087-33-7. [cit. 2012-04-03]. Dostupné z: http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf
[69] MATOUŠEK, Václav. *Inteligentní agenti* [prezentace online]. 2011 [cit. 2012-04-05]. Dostupné z: http://www.kiv.zcu.cz/studies/predmety/uir/predn/P8/Folie_IntAg.pdf
[70] MATOUŠEK, Václav, ref. 69.

sdělí, že pan Y je na dovolené, tudíž je lepší zprávu odfaxovat sekretářce pana Y“ [71].

3.2. Druhy agentů

Agenti mohou být rovněž klasifikováni podle činností, které vykonávají. Typů agentů je celá řada, mezi jedny z nejvýznamnějších patří dle *Handbook of Privacy and Privacy-Enhancing Technologies*[72] mmj. tyto:

Interface agents (IA)

- IA poskytují personalizovaná uživatelská rozhraní pro sdílení informací osvojených z různých pozorování. IA se přizpůsobují uživatelským preferencím tím, že uživatele imitují díky sledování jeho instrukcí nebo skrze „Pavlovův efekt“ (učením se z pozitivních nebo negativních odpovědí uživatele);
- mezi známé příklady užití IA patří tzv. „news filtering agents“ (např. PointCast) nebo UrbanYenta, což je agent, který dává dohromady lidi se stejnými zájmy („Love is personal. At UrbanYenta, we make finding love personal too“[73]), nebo Ringo či Firefly, což jsou systémy založené na doporučování hudby založené na sociálním filtrování, což je technika podobná ústnímu doporučování.

Information agents

- tito agenti obcházejí model „tonutí v datech, zatímco prahneme po informacích“ a tím se snaží řešit problém s aktuálním nadbytkem dat. Za nejznámější příklad je považován prohlížeč Netscape, Alta Vista nebo Yahoo!

[71] MATOUŠEK, Václav, ref. 69.
[72] PISA CONSORTIUM. *Handbook of Privacy and Privacy-Enhancing Technologies*: *The case of Intelligent Software Agents*. [online]. Haag: TNO-FEL, 2003, s. 62-63. ISBN 90-74087-33-7. [cit. 2012-04-03]. Dostupné z: http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf
[73] Finding Love is personal with UrbanYenta. *UrbanYenta* [online]. [?] [cit. 2012-04-05]. Dostupné z: http://urbanyenta.com/

Stephen Haag[74] dělí agenty do 4 základních skupin:

Buyer agents or shopping bots („nakupovací agenti“)

- pomáhají uživateli vyhledat zboží nebo službu;
- putují internetem a vyhledávají to, co by mohlo uživatele zaujmout.

User or personal agents („osobní agenti“)

- vykonávají činnost místo uživatele, např.:
  - kontrolují emaily, řadí je dle preferencí, upozorňují na důležité zprávy;
  - hrají počítačové hry jako uživatelům protihráč;
  - umožňují „customizovat“, tj. přizpůsobovat zprávy dle preferencí, jak je tomu např. u CNN;
  - automaticky vyplňují za uživatele formuláře a dotazníky;
  - v textu vyhledávají nejdůležitější informace;
  - usnadňují vyhledávání pracovních pozic tím, že procházejí nabídky práce a rozesílají životopisy a žádosti o práci dle stanovených kritérií.

Monitoring-and-surveillance or predictive agents („dohlížející nebo předpovídající agenti“)

- sledují a podávají zprávy o činnosti, nejčastěji počítačového systému;
- př.: zvláštní organizace agentů použitá k napodobování procesů během taktických operací (oblast tzv. „human decision making“). Agenti monitorují stav majetku (střelivo, dostupné zbraně, atd.) a obdržují příkazy či cíle mise od vyšších stupňů agentů.

[74] [HAAG, Stephen]. *Decision Support and Artificial Inteligence*: *Brainpower for Your Business* [prezentace online]. The McGraw-Hill Companies, 2004 [cit. 20. 4. 2012]. Dostupné z: http://www.csupomona.edu/~vllucas/courses/cis310/chap004a.pdf
Prezentace vychází z článku:
HAAG, Stephen, Maeve CUMMINGS a Donald J MCCUBBREY. Decision Support and Artificial Inteligence: Brainpower for Your Business. *In: Management information systems for the information age*. 4th ed. Boston: McGraw-Hill, 2004. ISBN 0-07-281947-2.

Data-mining agents („agenti pro dolování dat“)

- pracují v datových skladištích, prochází různé zdroje a vyhledávají informace, které jsou vyžadovány;
- např.: agent může odhalit úpadek v ekonomickém průmyslu, díky této informaci jsou společnosti schopné učinit vhodná opatření a rozhodnutí týkající se zaměstnanců nebo nákupů/prodejů atd.

3.3.Soukromí a ISA

Inteligentní agenti se velice úzce dotýkají soukromí uživatele, neboť mohou sbírat, zpracovávat, skladovat a zprostředkovávat data. Tato data mohou být i osobního a velmi citlivého obsahu.

K pověření agenta nějakým úkolem uživatel zároveň poskytuje agentům díky svému profilu osobní data, jako je např. emailová adresa, zvyky či preference. Potenciální hrozba soukromí nastává v okamžiku, kdy agent pracuje s těmito daty a zároveň komunikuje s vnějším prostředím nebo s ním data vyměňuje.

3.4.ISA a PET

V předchozí kapitole bylo naznačeno, v jakém vztahu jsou agenti a soukromí uživatele. K tomu, aby byla data dostatečně chráněna, přicházejí PET jako nástroj, který tuto ochranu dokáže zabezpečit. PET se snaží vyrovnat s hrozbami, kterým agenti čelí. Mezi tyto hrozby patří např. to, že agenti mohou mezi sebou navzájem sdílet uživatelská data, agenty může spravovat nedůvěryhodný poskytovatel, agent může zprostředkovávat osobní data uživatele okolnímu prostředí nebo se může „nabourat“ do uživatelova účtu a zcizit libovolné informace. Stejně tak je schopný ukrást osobní data uživatele od jiného agenta a jeho uživatele.

Tyto hrozby lze zobecnit do dvou skupin na:

- hrozby způsobené agenty, kteří jednají jménem uživatele

(díky odhalení uživatelových osobních informací)

- a hrozby způsobené cizími agenty, kteří jednají jménem jiných uživatelů (skrze monitoring dopravního toku informací, data miningu a dokonce prostřednictvím skrytých útoků s cílem získat informace přímo od uživatelova agenta)[75].

Existuje několik způsobů použití PET k ochraně osob v prostředí založeném na činnosti agentů:

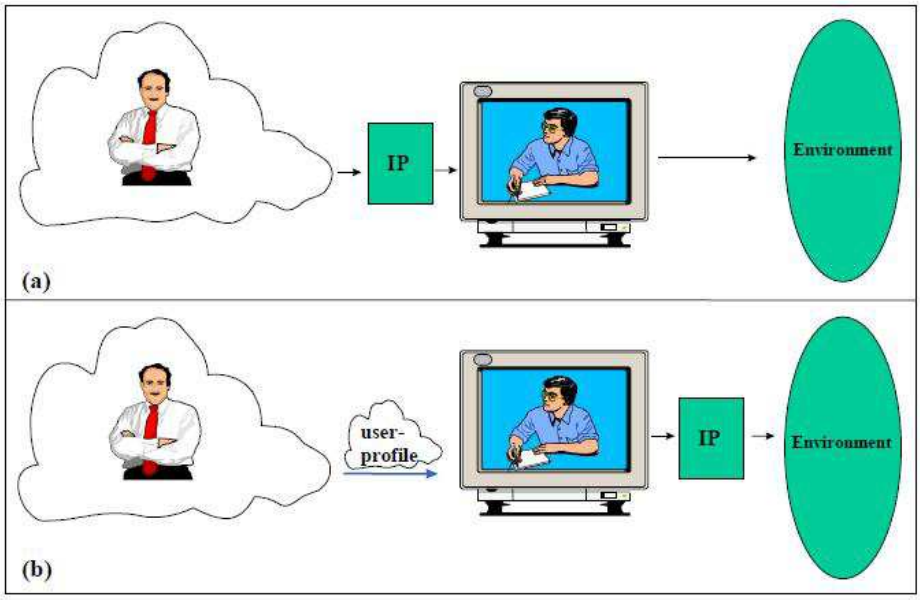
- „obalení“ PET kolem uživatelova agenta (obdobné jako když je umístěn identity protector mezi agenta a vnější prostředí - viz níže),
- integrace PET do uživatelova agenta nebo
- kombinace obou předchozích.[76]

Aktivity agentů mohou být řízeny **identity protectorem (IP)**, který je implementován právě pomocí PET. IP kontroluje výměnu uživatelovy identity v rámci informačního systému. V prostředí založeném na agentních systémech může být IP použit dvěma různými způsoby:

- mezi uživatelem a agentem,
- mezi agentem a vnějším prostředím (jak naznačuje následující grafika):

[75] *Handbook of Privacy and Privacy-Enhancing Technologies*: *The case of Intelligent Software Agents*, ref. 68, s. 68-69.
[76] *Handbook of Privacy and Privacy-Enhancing Technologies*: *The case of Intelligent Software Agents*, ref. 68, s. 77-78.

Obrázek 6 Vztah mezi agenty a vnějším prostředím[77]



The Identity Protector (IP) placed in an agent-based environment: (a) the IP placed between the user and the agent; (b) the IP placed between the agent and the external environment.

Příručka dále říká, že nemůže dojít k výměně osobních dat mezi uživatelem a agentem bez souhlasu IP a uživatele, pokud je IP umístěn mezi uživatelem a agentem. Uživatel tak může kontrolovat množství osobních dat, která jsou zaznamenána agentem. Této možnosti může být využito v případě ochrany uživatele před ohrožením soukromí způsobeným správci agentů.

Je třeba poznamenat, že ochrana soukromí pořád leží v rukou uživatele jako jeho vlastní volba a na vlastní zodpovědnost. To samé platí o použití PET - uživatel se smí rozhodnout, zda použije PET k ochraně svého agenta, popř. proti cizím agentům. Pokud se rozhodne pro ochranu, musí zvolit rozsah této ochrany. To záleží i na tom, v jakém vztahu s okolním prostředím se uživatel nachází. Tento vztah se skládá z politické, sociální, veřejné nebo jiné interakce.

[77] *Handbook of Privacy and Privacy-Enhancing Technologies*: *The case of Intelligent Software Agents*, [obrázek], ref. 68, s. 69.

PET spolu s agenty, kteří plní uživatelovy požadavky, mají velký potenciál stát se významným nástrojem pro ochranu soukromí. Cílem organizací, které vyvíjejí bezpečnostní nástroje nebo agenty, by se měl stát rozvoj PET. Mezi tyto nástroje patří i identity protector, který pomáhá subjektům chránit jejich soukromí. Každý uživatel by měl být do budoucna schopný propojit své soukromí s jeho aktivní ochranou a s agenty a to v závislosti na uživatelově specifických nárocích na soukromí.

3.5. Bližší informace o tématu

O ISA lze nalézt množství článků, které se zabývají především technologickým popisem a designem, programovacími schématy a implementací do systémů. V mnohém jsou si podobné. Většinou se autoři snaží v úvodu definovat, co to ISA je, jaké mají vlastnosti a specifikace.

Ráda bych upozornila především na článek *Intelligent software agents for library applications*[78], který je zvláštní tím, že vymezuje ISA z knihovnického pohledu, přičemž se tu uvádí seznam příkladů užití agentů právě v knihovnách. Užití agentů v knihovnách se dle tohoto článku předpokládá v oblasti elektronických informačních služeb, sbírek a akvizice, klasifikace a organizace knihovního materiálu, indexace, referenčních služeb aj. Agent může také pomoci uživateli při vyhledávání informací v databázích. V tomto případě by užití agentů v knihovnách bylo jistě vítanou pomocí, jelikož by mohli převzít řadu rutinních činností spojených s knihovnickou praxí a ušetřit spoustu času i energie na další potřebné aktivity.

[78] LOHANI, Minoo a V.K.J. JEEVAN. Intelligent software agents for library applications. *Library Management*. 2007, roč. 28, č. 3, s. 139-151. ISSN 0143-5124. DOI: 10.1108/01435120710727983. Dostupné z: http://www.emeraldinsight.com/10.1108/01435120710727983

ZÁVĚR

Je zřejmé, že naše soukromí s nástupem internetu překročilo práh našich domovů a stává se z něj „běžné zboží“. Situace se dle dostupné literatury a každodenních zpráv zdá být poměrně vyhrocená. Jako bychom z fáze, kdy si své soukromí střežíme za zdmi domu, přešli rovnou do fáze, kdy soukromí neexistuje, kdy je prakticky mrtvé. Jako uživatelé se stáváme méně ostražitými a více důvěřivými vůči technologiím, které nám v mnohém ulehčují pracovní i osobní život, za cenu narušení jednoho ze základních lidských práv, kterým je právo na soukromí.

Domnívám de, že naše soukromí je spíše zmatené, než-li mrtvé. Vytváří se kolem něj prostředí chaosu, kde se jej snažíme ochraňovat všemi dostupnými prostředky, ale zároveň jej v různých situacích různě odhalujeme. Dokud se nezmění přístup v myšlení lidí-uživatelů k této problematice, tak veškeré legislativní a technologické snahy budou zbytečné. To, že se o soukromí začíná mluvit stále častěji a že vznikají nástroje na jeho ochranu ale svědčí o tom, že s tím lze stále něco udělat.

Předkládaná práce upozornila na tento fenomén a nabídla možnosti na ochranu soukromí v podobě nástrojů PET. Na PET začíná být kladen velký důraz i po stránce legislativní, kdy jednotlivá doporučení a zákony počítají do budoucna s rozvojem a rychlou implementací těchto nástrojů do informačních systémů. Vznikají projekty a směrnice, jejichž cílem je ochrana uživatelova soukromí před vnějšími hrozbami, ale i před jeho vlastní neopatrností.

Má práce nabídla pohled na PET jako na moderní technologie, které byly navrženy s dobrým úmyslem a ve snaze ochránit naše soukromí. Na PET lze ale také pohlížet z odvrácené strany, a to jako na nástroj moci, který v nepovolaných rukou může ve výsledku přinést více škody než užitku. Ačkoli to nebylo tématem mé práce, je více než patrné, že PET se velmi těsně dotýkají i etických aspektů. I když ve zpracované literatuře k této práci nepadl žádný striktně odmítavý hlas vůči PET, vyvstává u nich řada otázek, které etiku použití PET řeší.

Sběr dat, jejich zpracování, ukládání, poskytování třetím stranám, popř. obchodování s informacemi je velké etické téma; kdo, co, proč a jakým způsobem má zájem o naše data? Pokud začneme využívat PET k ochraně soukromí, nebude to jen další, mnohem sofistikovanější nástroj kontroly a moci, něco jako „velký bratr 2.0“? Nestane se z ISA

agentů armáda všudypřítomných „špehů“, kteří budou kontrolovat každý náš krok a v případě, že se jim to nebude líbit, tak zasáhnou, udělají to jinak a ještě o tom podají zprávu někomu dalšímu? Nebude to jen další pokus o dohled či cenzuru? Domnívám se, že do návrhu designu PET a ISA by měla být velice důkladně vsazena legislativní, etická a morální zabezpečení, která zaručí, že výše položené otázky nenajdou své opodstatnění.

I přesto na základě všech zjištěných poznatků o PET, ISA a soukromí na internetu považuji PET za nástroj budoucnosti, co se týče ochrany soukromí, a ISA agenty za inteligentní aplikace, které se v blízké budoucnosti stanou nedílnou součástí života a každodenních činností každého z nás. Věřím, že tyto technologie mohou ochránit naše soukromí a že tak budou činit zcela nezištně a naprosto profesionálně.

Cílem mé práce bylo nabídnout čtenáři základní ucelený pohled na oblast PET, ISA a soukromí na internetu tak, aby zjistil, proč by se měl věnovat svému soukromí, čím je ohroženo a především jakými prostředky jej lze v současné době, ale i v budoucnu ochraňovat.

SEZNAM ZKRATEK

AI	Artificial Intelligence
AHPS	Anonymizing HTTP Proxy Server
apod.	a podobně
atd.	a tak dále
atp.	a tak podobně
CIS	The Center for Internet and Society
CNN	Cable News Network
ČR	Česká republika
DDoS	distributed denial-of-service *attack*
ENISA	European Network and Information Security Agency
EU	Evropská unie
GPS	Global Positioning System
HTTP	HyperText Transfer Protocol
ICL	International Computers Limited
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IP	Identity Protector
IP (adresa)	Internet Protocol
IS	informační systém
ISA	Intelligent Software Agent
IT	information technology
mmj.	mimo jiné
např.	například
OECD	Organisation for Economic Co-operation and Development
OP	občanský průkaz
P2P	peer to peer
P3P	Platform for Privacy Preferences Project
PC	personal computer
PET	Privacy Enhancing Technologies

PII	Personally Identifiable Information
PISA	Programme for International Student Assessment
PIT	Privacy Invasive Technologies
popř.	popřípadě
PRIME	Privacy and Identity Management for Europe
r.	rok
RFID	Radio Frequency Identification
SSL	Secure Sockets Layer
SW	software
tj.	to jest
TLS	Transport Layer Security
TTP	Trusted Third Party
tzv.	tak zvaně
UBE/UCE	Unsolicited Bulk/Commercial Email
URL	Uniform Resource Locators
USA	United States of America
VPN	virtual private network
Wi-Fi	Wireless Fidelity
WWW	World Wide Web

SEZNAM OBRÁZKŮ

POUŽITÉ ZDROJE

About PRIME. *PRIME* [online]. 2004-2012 [cit. 2012-04-03]. Dostupné z: https://www.prime-project.eu/about/

'Action needed' to meet UK's cookie tracking deadline. In: *Www.bbc.com* [online]. 18. 4. 2012 [cit. 2012-04-21]. Dostupné z: http://www.bbc.com/news/technology-17745938

CLARKE, Roger. Introducing PITs and PET: Technologies Affecting Privacy . In *Roger Clarke's Web-Site* [online]. Chapman, Australia : Xamax Consultancy Pty, 2001, 2003 [cit. 2011-11-26]. Dostupné z WWW <http://www.rogerclarke.com/DV/PITsPET.html#GPET>.

Co je to phishing?. *Www.hoax.cz* [online]. 2010-2012 [cit. 2012-04-02]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

Česká republika. Zákon č. 101/2000 Sb.: o ochraně osobních údajů. In: *Zákony ČR online*. 2011. [cit. 2012-04-02]. Dostupné z: http://www.zakonycr.cz/seznamy/101-2000-Sb-zakon-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu.html

ENISA: European Network and Information Security Agency. *Enisa* [online]. 2005-2012 [cit. 2012-04-03]. Dostupné z: http://www.enisa.europa.eu/

Evropská unie. Článek 8: Ochrana osobních údajů. In: *Listina základních práv Evropské unie*. 2007. Dostupné z: http://eur-lex.europa.eu/cs/treaties/dat/32007X1214/htm/C2007303CS.01000101.htm

Evropská unie. Sdělení Komise Evropskému parlamentu a Radě o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PET). [online]. Brusel, 2007. [cit. 2012-04-03]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:CS:PDF

Evropská unie. Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací: Směrnice o soukromí a elektronických komunikacích. In: *Úřední věstník L 201*. 2002. [online]. [cit. 2012-04-03]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:CS:HTML

Fair Information Practice Principles. *FEDERAL TRADE COMMISSION* [online]. [?], 2007 [cit. 2012-04-02]. Dostupné z: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

FEDERAL TRADE COMMISSION. *Privacy online: fair information practices in the electronic marketplace*: *a report to Congress* [online]. 2000 [cit. 2012-04-02]. Dostupné z: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

Finding Love is personal with UrbanYenta. *UrbanYenta* [online]. [?] [cit. 2012-04-05]. Dostupné z: http://urbanyenta.com/

FISCHER-HÜBNER, Simone a Nicholas HOPPER. *Privacy Enhancing Technologies : 11th International Symposium, PET2011 Waterloo, ON, Canada, July 27-29, 2011 Proceedings* [online]. ? : Springer, 2011 [cit. 2011-03-26]. Dostupné z WWW: <http://dl.dropbox.com/u/17936902/Privacy%20enhancing%20technologies.pdf>. ISBN 978-3-642-22262-7.

Guidance on the rules on use of cookies and similar technologies. INFORMATION COMMISSIONER'S OFFICE. *Http://www.ico.gov.uk/* [online]. 2. vyd. 13. 12. 2011 [cit. 2012-04-21]. Dostupné z: http://www.ico.gov.uk/global/search.aspx?allwords=Guidance%20on%20the%20rules%20on%20use%20of%20cookies%20and%20similar%20technologies&collection=ico&start=0

Guide to Data Mining: What is Data Mining?. *Data-Mining-Guide.net* [online]. 2005 [cit. 2012-04-05]. Dostupné z: http://www.data-mining-guide.net/

HAAG, Stephen, Maeve CUMMINGS a Donald J MCCUBBREY. Decision Support and Artificial Inteligence *Brainpower for Your Business. In: Management information systems for the information age*. 4th ed. Boston: McGraw-Hill, 2004. ISBN 0-07-281947-2.

JANCA, Peter. Pragmatic Application of Information Agents. Norwell, United States: BIS Strategic Decisions, 1995. Podle: PISA CONSORTIUM. Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents. [online]. Haag: TNO-FEL, 2003, s. 56. ISBN 90-74087-33-7. [cit. 2012-04-03]. Dostupné z WWW: http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf

KOORN, Ronald (ed.). *Privacy Enhancing Technologies : White Paper for Decision-Makers* [online]. 1. Nizozemí : Ministry of the Interior and Kingdom Relations, 2004 [cit. 2012-04-16]. Dostupné z WWW: <http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf>.

LEE, Edward A. Embedded Software. In: *Advances in Computers* [online]. London: Academic Press, 2001 [cit. 2012-04-04]. Vol. 56. Dostupné z: http://ptolemy.eecs.berkeley.edu/publications/papers/02/embsoft/embsoftwre.pdf

LOHANI, Minoo a V.K.J. JEEVAN. Intelligent software agents for library applications. *Library Management*. 2007, roč. 28, č. 3, s. 139-151. ISSN 0143-5124. DOI: 10.1108/01435120710727983. Dostupné z: http://www.emeraldinsight.com/10.1108/01435120710727983

MATOUŠEK, Václav. *Inteligentní agenti* [prezentace online]. 2011 [cit. 2012-04-05]. Dostupné z: http://www.kiv.zcu.cz/studies/predmety/uir/predn/P8/Folie_IntAg.pdf

MCCALLISTER, Erika, Tim GRANCE a Karen SCARFONE. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology.* [online] National Institute of Standards and Technology: Computer Security Dicision. 2010, s. 2.1 – 2.2. [cit. 2012-04-02]. Dostupné z: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Me, Myself and I! Manage your identities safely. *PRIME – Privacy and Identity Management for Europe* [online]. [?] [cit. 2012-04-03]. Dostupné z: https://www.prime-project.eu/press_room/leaflets/Prime-Primer-2pager.pdf

NISSENBAUM, Helen Fay. *Privacy in context*: *technology, policy, and the integrity of social life*. Stanford, Calif.: Stanford University Press, 2010, 288 s., [cit. 2011-11-26]. Dostupné z WWW: <http://dl.dropbox.com/u/17936902/NISSENBAUM%20-%20Privacy%20in%20Context.pdf>. ISBN 978-0-8047-5237-4.

NYKODÝMOVÁ, Helena. Bojíte se krádeže své identity?. *Lupa.cz* [online]. 16. 8. 2006 6:30 [cit. 2012-04-24]. Dostupné z: http://www.lupa.cz/clanky/bojite-se-kradeze-sve-identity/

OpenTC. *Www.opentc.net* [online]. [?] [cit. 2012-04-02]. Dostupné z: http://www.opentc.net/index.php?option=com_content&task=view&id=29&Itemid=45

OPPLIGER, Rolf. Privacy-enhancing technologies for the world wide web: Short Survey. *Science Direct* [online]. 2005[cit. 2012-04-03]. Dostupné z: http://www.sciencedirect.com/science/article/pii/S0140366405000691

PISA CONSORTIUM. *Handbook of Privacy and Privacy-Enhancing Technologies*: *The case of Intelligent Software Agents*. [online]. Haag: TNO-FEL, 2003. ISBN 90-74087-33-7. [cit. 2012-04-03]. Dostupné z: http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf

Phishing a Pharming. *Www.bezpecnyinternet.cz* [online]. [?] [cit. 2012-04-02]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

PRIME PROJECT. *Privacy and Identity Management for Europe* [online]. 2004-2012 [cit. 2012-04-03]. Dostupné z: https://www.prime-project.eu/

Promoting Data Protection by Privacy Enhancing Technologies (PET). *Europa.eu* [online]. 2007, [cit. 2011-11-28]. Dostupný z WWW: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/598&format=HTML&aged=0&language=EN&guiLanguage=en>

Protect your privacy. GET SAFE ONLINE. *Get Safe Online*: *Free expert advice* [online]. 2012 [cit. 2012-04-02]. Dostupné z: http://www.getsafeonline.org/nqcontent.cfm?a_id=1132

SENIČAR, Vanja, JERMAN-BLAŽIČ, Borka, KLOBUČAR, Tomaš. Privacy-Enhancing Technologies : approaches and development. *Computer Standards* [online]. 2003, roč. 25, č. 2, s. 147-158 [cit. 2012-04-03]. ISSN 09205489. DOI: 10.1016/S0920-5489(03)00003-5. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/S0920548903000035

SHILTON, Katherine Carol . *Building Values into the Design of Pervasive Mobile Technologies* [online]. Los Angeles : University of California, 2011 [cit. 2011-04-04]. [online]. Dostupné z WWW: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1866783>.

Spam. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 15. 3. 2012 [cit. 2012-04-02]. Dostupné z: http://cs.wikipedia.org/wiki/Spam

THE CENTER FOR INTERNET AND SOCIETY. *PET* [wiki databáze online]. Stanford, 2011 [cit. 05. 04. 2012]. Dostupné z: http://cyberlaw.stanford.edu/wiki/index.php/PET

THE TOR PROJECT. *Tor*: *Anonymity Online* [online]. [2012] [cit. 2012-04-17]. Dostupné z: https://www.torproject.org/index.html.en

USA. Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promting Innovation in the Global Digital Economy. In: *The Consumer Privacy Bill of Rights*. Washington: The White House, 2012. Dostupné z: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

WEITZNER, Danny. We Can't Wait: Obama Administration Calls for A Consumer Privacy Bill of Rights for the Digital Age. In: *The White House Blog* [online]. Washington, D.C., 23. 2. 2012 [cit. 2012-04-04]. Dostupné z: http://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age

What is botnet?. *Www.microsoft.com* [online]. 2012 [cit. 2012-04-02]. Dostupné z: http://www.microsoft.com/security/resources/botnet-whatis.aspx

ZADRAŽILOVÁ, Iva. *Nebezpečí zneužití osobních informací v době globálního monitoringu s přihlédnutím k možnostem ochrany soukromí*. Brno: Masarykova univerzita, Filozofická fakulta, Ústav české literatury a knihovnictví, 2009. 143 s. Vedoucí bakalářské práce PhDr. Michal Lorenz.