Jak si lidé cení soukromí?

Marek Kumpošt, Václav Matyáš, FI MU

Článek se zabývá představením výsledků dvou experimentů, jejichž cílem bylo zjistit, jak si lidé cení svých soukromých informací.[1] Aby byly získané informace co možná nejméně ovlivněné tím, že se lidí přímo zeptáme na cenu, byly oba experimenty provedeny formou webového dotazníku, kdy skutečný záměr byl do určité míry skryt. V prvním experimentu byla zjišťována cena informací o aktuální poloze člověka – poloha zjištěna pomocí mobilního telefonu. V druhém případě jsme se zaměřili na cenu informací týkající se využití nástrojů pro online komunikaci (posílání e-mailů nebo použití instant messagingu) – informace o využití těchto typů online komunikace by byly zjišťovány pomocí námi vyvinutého specializovaného software. V obou případech jsme se účastníku ptali, jakou finanční kompenzaci by požadovali v případě, že by se zúčastnili navrženého experimentu. Navržený experiment byl ve skutečnosti pouze zástěrkou, právě z důvodu minimalizace zkreslení výsledků. Obě studie byly provedeny ve spolupráci s našimi zahraničními partnery (univerzitami) v rámci projektu FIDIS (Future of Identity in the Information Society).

1 Úvod

V současné době je ochrana soukromí stále aktuálnějším tématem a mnoho lidí si uvědomuje dopady v důsledku narušení soukromí v IT světě. Informační soukromí můžeme částečně vnímat důvěrnost dat nebo kontrolované poskytnutí osobních informací. Nicméně stále existují situace, kdy lidé ochotně sdělí své soukromé informace často za poměrně zanedbatelnou protihodnotu. Typickým příkladem mohou být různé věrnostní a slevové karty obchodních řetězců a specializovaných obchodů. Provozovatelé věrnostních karet pak mohou jednoduše propojit nákupy lidí a budovat strukturu zboží, o které má konkrétní zákazník zájem – například z důvodu cílené reklamy.

Zajistit ochranu informačního soukromí v informačních systémech není snadná. Lze například implementovat mechanizmy řízení přístupu v důvěryhodných systémech, ale jakmile jednou data získá někdo nepovolaný, je téměř nemožné jakkoliv dále kontrolovat jejich šíření. Existují dva základní přístupy pro řešení útoků na informační soukromí. Jednak právní nástroje a výše trestů těm, kdo neoprávněně získaná data zneužijí a jednak technické prostředky na ochranu systémů pro správu citlivých dat.

Příklad mobilní sítě a telefony – pro většinu lidí nepostradatelný společník, umožňuje sledování pohybu mobilního telefonu prostřednictvím BTS (Base Transceiver Stations). Pomocí triangulace je možné sledovat polohu telefonu v reálném čase a to s přesností na stovky metrů ve městech a jednotek kilometrů v méně pokrytých oblastech sítě.

Mohli bychom namítnout, že u GSM sítí je „sledování" mobilních telefonů potřeba z důvodů směrování (routing) telefonních hovorů. Informace o pozici mobilního telefonu může být operátorem uchovávána a mobilní operátor může tyto informace hypoteticky poskytnout k dalším službám – např. rodiče mohou sledovat své děti, zaměstnanec může sledovat pohyb svých zaměstnanců (resp. jejich služebných telefonů). Třetí generace GSM sítí nabídnou ještě přesnější určení polohy koncového zařízení.

Jiným příkladem může být využití nástrojů pro online komunikace jako e-mail nebo posílání krátkých zpráv v reálném čase – instant messaging. Síťový administrátor má možnost sledovat a analyzovat aktivitu uživatelů ve své síti. To vytváří potenciální riziko zneužití zmiňovaných informací a většina uživatelů takové riziko vůbec nevnímá.

Zjistit, jak si lidé cení soukromých informací, není tak snadné a pro potřeby našich experimentů jsme proto využili sadu dotazníků a cíle experimentů byly mírně zkreslené. To z toho důvodu, abychom minimalizovali „míru ovlivnění" účastníků právě s ohledem na cíle průzkumu. Experiment týkající se ceny lokačního soukromí

[1] Článek je částečně postaven na naší předchozí publikaci [9] a FIDIS (www.fidis.net) deliverable D13.12 (WP13) a byl publikován na konferenci IS2 (Information Security Summit) 2009.

můžeme vnímat jako zobecnění článku autorů Danezis, Lewise a Andersona [3]. Tito autoři provedli podobný průzkum v rámci jedné univerzity. Výsledky našeho experimentu v článku srovnáme s výsledky autorů publikace [3].

2 Návrh našich průzkumů

Z několika publikovaných studií [3, 4], zabývajících se tím, jak lidé přistupují k ochraně svého soukromí, je vidět, že pokud je člověk přímo tázán na cenu, kterou požaduje za své soukromé informace, má zpravidla tendenci navrhovat vysoké částky. V souladu s předchozí studií [3] jsme proto zvolili stejný postup získání informací o ceně – prostřednictvím aukce, kde lidé navrhnou požadovanou cenu za své soukromé informace. Částka, která bude účastníkům vyplacena, je stanovena jako nejnižší z navrhovaných, kterou navrhoval první již nepřijatý účastník. Důvod je zřejmý – přiblížení spodní i horní hranice co nejblíže k sobě. Spodní hranice je posouvána nahoru těmi účastníky, kteří chtějí získat maximální odměnu, zatímco horní hranice je tlačena dolů z důvodu setrvání v aukci a šanci na účast v experimentu.

Cenu soukromých informací v rámci studie také ovlivní povědomí účastníků o skutečné podstatě experimentu. Lidé mají tendenci přeceňovat hodnotu svých soukromých informací, pokud jsou tázáni přímo na cenu např. v rámci socilogického průzkumu [5]. Z tohoto důvodu jsme se rozhodli skutečnou podstatu experimentu skrýt a prezentovat ho jako studii o využití mobilních telefonů (první studie), která bude probíhat jeden měsíc a při které bude pravidelně sledována poloha mobilního telefonu. V druhém případě byla studie prezentována jako průzkum využitelnosti nástrojů online komunikace typu e-mail nebo instant messaging. Potenciálním účastníkům jsme též oznámili, že finanční prostředky na podporu experimentů jsou omezené a že výběr účastníků proběhne na základě aukce – tímto jsme se pokusili vytvořit takové prostředí, ve kterém účastníci přiřadí svým soukromým informacím skutečnou a nepřehnanou hodnotu. Skutečná podstata experimentu byla zveřejněna nějakou dobu po ukončení sběru odpovědí.

Obě studie byly provedeny v rámci (a s pomocí partnerů) projektu FIDIS[2]. V rámci tohoto prostředí a ve spolupráci s našimi partnerskými institucemi v Evropě se podařilo získat data od daleko většího množství respondentů.

Obě popisované studie byly implementovány formou webových formulářů s otázkami. Spuštění webové aplikace bylo oznámeno na všech spolupracujících institucích formou hromadných e-mailů. Zpráva o existenci experimentu v několika případech pronikla i na internetové stránky organizací, které se zajímají např. o mobilní technologie.

3 Implementace průzkumů

V této části si stručně popíšeme strukturu dotazníků průzkumů. Dotazníky byly implementovány jako webové aplikace, aby byla zaručena snadná přístupnost pro účastníky. V případě studie o lokačním soukromí byl dotazník autentizovaný, v případě využití nástrojů online komunikace byl dotazník přístupný bez nutnosti autentizace. V obou experimentech bylo možné explicitně odmítnout účast jednak v celém experimentu a nebo na úrovni jednotlivých scénářů.

3.1 První průzkum – lokační soukromí

Dotazník byl rozdělen do čtyř logických celků. V první části se účastník seznámil s úvodním textem pořádaného průzkumu (rozšířená verze textu, který byl šířen e-mailem). První otázkou pak bylo, zda se osoba chce zúčastnit průzkumu, či nikoliv. Účastníci, kteří souhlasili s účastí, byli požádáni o zadání e-mailové adresy na kterou jim byly zaslány přístupové údaje k dalším částem dotazníku. Po úspěšném přihlášení do autentizované části následovala další sada otázek s cílem např. zjistit, jak často účastník používá svůj mobilní telefon. V závěrečné otázce jsme se ptali na výší požadované finanční kompenzace za účast v našem experimentu. V dalších scénáři pak došlo ke změně zpracování získaných dat:

[2] FIDIS – "Future of Identity in the Information Society" is a 5-year Network of Excellence research grant scheme of the EU 6th Framework Program (www.fidis.net). Its objective is to research the changes that the concept of identity is undergoing in the developing European information society.

z akademického do komerčního prostředí a v posledním scénáři pak možnost prodloužení experimentu na jeden rok.

3.2 Druhý průzkum – využití nástrojů pro online komunikaci

V druhém experimentu byla struktura dotazníku podobná – nejprve volba jazykové mutace, dotaz na účast/neúčast v experimentu a série obecných otázek zejména pro podporu důvěryhodnosti experimentu.

Z pohledu experimentu byl nejdůležitější dotaz na požadovanou výši finanční kompenzace v případě sledování elektronické komunikace (bez sledování vlastního obsahu posílaných zpráv). Byly zde varianty pro elektronickou poštu, instant messaging a veškeré komunikační údaje.

Změna způsobu zpracování dat pak byla obdobná jako v případě prvního experimentu: akademické, komerční a (zcela hypoteticky) vládní prostředí. Účastníků jsme se dotazovali na výši finanční kompenzace v každém z těchto scénářů.

4 Výsledky první studie – lokační soukromí

4.1 Demografie

V této části stručně uvedeme získaná demografická data. Dotazník experimentu byl dostupný po dobu jednoho měsíce a nejvíce odpovědí jsme získali v průběhu prvních 48 hodin po odeslání hromadných e-mailů.

Okolo 1200 účastníků zodpovědělo první sadu otázek. Tito účastníci byli z pěti zemí: Belgie, Česká republika, Německo, Řecko a Slovenská republika. Rozdělení účastníků podle národnosti a také poměr mužů a žen je v tabulce 1. Množiny účastníků z České republiky, Německa a Slovenska jsou dostatečně velké pro detailní analýzu dat. Menší množiny účastníků z Belgie a Řecka jsou použity spíše jako „kontrolní data" pro potvrzení obecných výsledků.

4.2 Obezřetnost účastníků

První otázka na účastníky byla, zda se chtějí zúčastnit průzkumu či nikoliv. Ze tří nabízených možností můžeme zanedbat tu, že účastník nevlastní mobilní telefon – takových případů bylo jen několik. Máme tedy množinu 2582 lidí, z toho 239 vyjádřilo nesouhlas s účastí v experimentu. Z této množiny bylo 11 účastníků z Belgie, 85 z České republiky, 65 z Německa, 32 z Řecka a 46 ze Slovenska. Relativní výsledky jsou zajímavější, než absolutní čísla a jsou shrnuty v tabulce 2.

Stát	Celkem	Ženy
Belgium	37	3
Czech Republic	744	131
Germany	251	33
Greece	30	6
Slovak Republic	152	46

Tabulka 1: Počty účastníků podle jednotlivých států.

Stát	BE	CZ	DE	GR	SK
Počet	12 %	6 %	12 %	25 %	12 %

Tabulka 2: Počty lidí, které průzkum nezajímal.

Tabulka 3 shrnuje počty účastníků, kteří vyjádřili souhlas s účastí a poté, co zadali e-mailovou adresu, na kterou jim byly zaslány přístupové údaje, se do systému přihlásili. V tomto bodě je vhodné uvést, že někteří účastníci si účast rozmysleli v okamžiku, kdy byli požádání o zadání jejich e-mailové adresy.

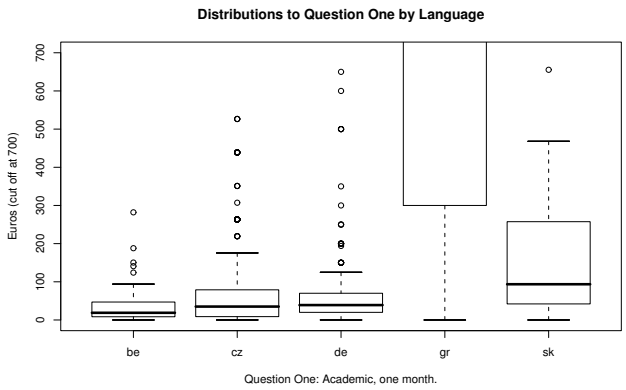
4.3 Hlavní výsledky

Dostáváme se k hlavním výsledkům průzkumu – ceně za soukromí. Data získaná od účastníků byla ze zemí s různými měnami, ale výsledné grafy a tabulky zobrazují cenu vždy v měně EURO. Ostatní měny byly přepočítány.

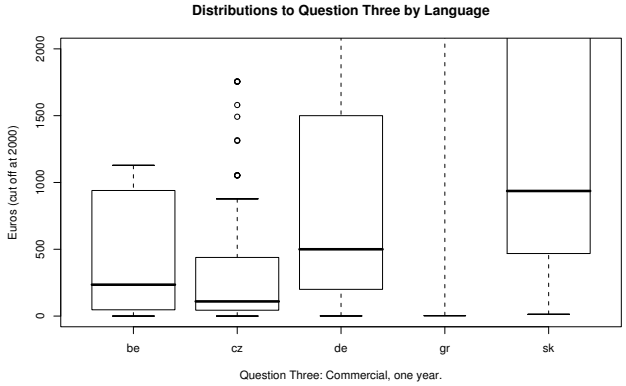
Získali jsme data ze tří aukcí (scénářů). První a druhý scénář bylo sledování polohy mobilního telefonu po dobu jednoho měsíce, přičemž v prvním případě pro akademické účely a ve druhém případě pro komerční využití. Ve třetím scénáři

Stát	BE	CZ	DE	GR	SK
Počet	44 %	56 %	52 %	32 %	42 %

Tabulka 3: Počty lidí, kteří měli zájem o experiment a minimálně se autentizovali do webové aplikace.

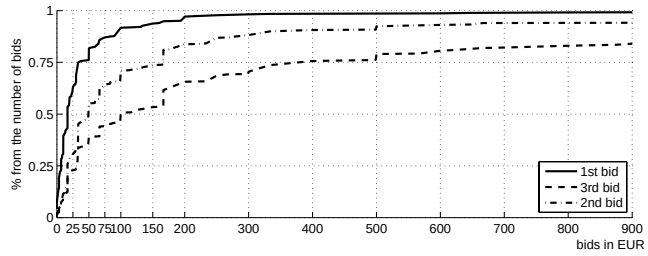


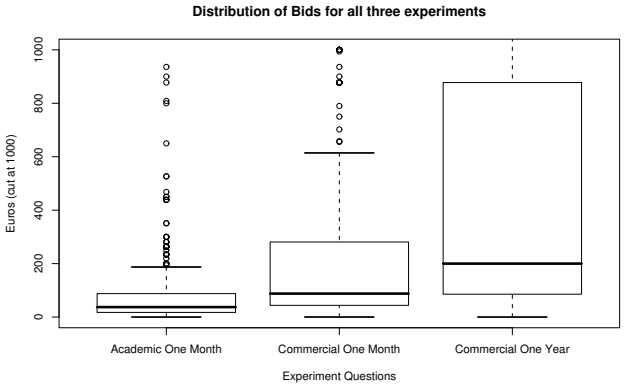
(a) Výše fin. kompenzace v prvním scénáři.



(b) Výše fin. kompenzace ve třetím scénáři.

Obrázek 1: Rozložení výše finanční kompenzace pro jednotlivé státy.





Obrázek 2: Rozložení výše fin. kompenzace pro všechny tři uvažované scénáře.

se jednalo o dlouhodobé (roční) sledování mobilního telefonu a data by byla poskytnuta ke komerčním účelům.

Rozdíly mezi státy. Rozložení první aukce zobrazuje graf 1(a). Je vidět, že Řekové opět potvrzují svoji citlivost na soukromí a ještě se s tímto trendem dále v textu setkáme. Samozřejmě jsou zde rozdíly i mezi ostatními státy, ale účastníci z Řecka jsou viditelně odlišní. Graf 1(b) zobrazuje situaci účastníků všech států v případě třetího scénáře. Účastníci z České republiky opět požadují nejnižší finanční kompenzaci a účastníci z Řecka už v grafu nejsou vůbec vidět. Problém u účastníků z Řecka je jejich malý počet pro dostatečné potvrzení tohoto trendu.

Vliv jednotlivých scénářů. Již jsme si ukázali jeden graf zobrazující situaci ve třetím scénáři. Je zajímavé sledovat změny výše finanční kompenzace ve všech třech uvažovaných aukcích. Grafy na obrázcích 2(a) a 2(b) zobrazují výsledky účastníků (ve dvou různých podobách), kteří zodpověděli všechny tři scénáře. Na levém obrázku zobrazuje osa x hodnotu finanční kompenzace v EUR a osa y podíl účastníků, jejichž požadavek byl alespoň do výše uvedené na ose x.

Z grafu je vidět, že medián nabídek se zhruba zdvojnásobil s přechodem od akademického ke komerčnímu zpracování dat. Rozšíření experimentu na celý rok vedlo opět pouze ke zdvojnásobení požadované finanční kompenzace. Tyto výsledky jasně ukazují, že účastníci jsou daleko citlivější na „účel" zpracování dat než na „dobu a objem" zpracovaných dat (sledované období bylo v našem případě rozšířeno z jednoho měsíce na dvanáct). Je také zajímavé, že účastníci různých států odlišně vnímají prodloužení experimentu na jeden rok. V případě účastníků z České republiky byl nárůst mediánu zhruba 20 %, 250 % nárůst v případě účastníků z Belgie a pětinásobek v případě Německa a Slovenska.

5 Výsledky druhé studie – využití nástrojů pro online komunikaci

V této části se zaměříme na nejzajímavější výsledky našeho druhého průzkumu. V tomto průzkumu jsme sledovali hodnotu informací o využití nástrojů pro online komunikace (e-mail a instant messaging). Pro potřeby uvedeného průzkumu by účastníci byli sledování pomocí speciálně vytvořeného software, který by v pravidelných intervalech odesílal souhrnné reporty na sběrný server.

5.1 Demografie

Úvodní text experimentu si otevřelo 1080 lidí. Úvodní text byl připraven v pěti jazykových mutacích: česká, slovenská, německá, anglická a vlámská. Po úvodním textu následovala otázka, zda se osoba chce zúčastnit experimentu či nikoliv.

Tabulka 4 obsahuje počty účastníků, kteří se rozhodli zúčastnit experimentu (bez ohledu zvolené zařízení). Celkový počet je 428 účastníků, což představuje 40 % z těch kteří viděli úvodní text. 26 % účastníků poskytlo odpovědi v prvním scénáři (akademické využití získaných dat). 80 % z těchto účastníků byli muži.

Následující tabulka 5 obsahuje počty účastníků, kteří na úvodní stránce dotazníku vyjádřili svůj explicitní nesouhlas s účastí v experimentu (čísla reprezentují zvolenou jazykovou variantu).

V druhém experimentu došlo k mírnému poklesu účastníků, kteří poskytli odpovědi v prvním scénáři – 40 % z těch co vidělo úvodní text. Pokud porovnáme situaci s naším prvním experimentem (cena lokačního soukromí), tak zde bylo toto číslo vyšší, konkrétně 48 %. Pokles počtu účastníků v druhém experimentu může být způsoben dvěma faktory: 1) účastníci byli vysoce citliví na tento typ osobních informací nebo 2) značná podobnost s naším předchozím experimentem (zaznamenali jsme několik takových odpovědí/důvodů v části proč se nechcete zúčastnit experimentu).

5.2 Hlavní výsledky

V této části si představíme hlavní výsledky průzkumu – cenu za sledování využití nástrojů online komunikace pomocí speciálně vytvořeného sledovacího software („spyware"). Data jsme získávali prostřednictvím dotazníků po dobu 14 dnů. Účastníkům jsme představili tři možné scénáře – získaní data budou použita pouze pro akademické účely; data budou poskytnuta komerčním subjektům; data budou poskytnutá národním vládám. V rámci každého scénáře jsme potom rozlišili způsob sledování: data o využití e-mailové komunikace; data o využití real-time komunikace – instant messaging; veškeré informace o online komunikaci. V každém z těchto případů by nebyl sledován obsah přenášených dat, ale pouze servisní informace.

Co se týče účastníků, kteří vyplnili alespoň první scénář, tak zde můžeme říci, že jsme nezaznamenali výrazný rozdíl mezi muži a ženami. 23 účastníků (9,871 %) explicitně vyjádřilo nesouhlas s účastí v rozšířené variantě experimentu – data budou poskytnuta komerčnímu partnerovi, se kterým máme obchodní vztah.

Tabulka 6 poskytuje přehled výsledků pro druhý scénář – data poskytnuta komerčnímu subjektu. V tomto případě můžeme sledovat i situaci v prvním scénáři pro porovnání, jak se vyvíjela výše požadované finanční kompenzace. V případě druhého scénáře lze pozorovat mírně vyšší požadavky u mužské části účastníků. Na druhou stranu je nutné zmínit, že množina žen byla velmi malá, abychom mohli výsledky považovat za směrodatné.

41 účastníků (18 %) explicitně vyjádřila nesouhlas s účastí v poslední navrhované variantě rozšíření experimentu – poskytnutí získaných dat národním vládám.

Podívejme se na poslední nabízený scénář využití získaných dat – poskytnutí dat národním vládám pro zlepšení technik detekce teroristické aktivity. Data v tabulce 7 ukazují situaci ve třetím scénáři a pro porovnání opět uvádíme i předchozí dva scénáře.

Jazyková mutace	BE	CZ	DE	SK	EN	Celkem
Počet	3 %	40,7 %	7 %	31,8 %	17,5 %	428

Tabulka 4: Počty účastníků, kteří se chtěli zúčastnit průzkumu.

Jazyková mutace	BE	CZ	DE	SK	EN	Celkem
Počet	3,5 %	33,8 %	15,8 %	36,8 %	10,5 %	57

Tabulka 5: Počty lidí, kteří explicitně vyjádřili nesouhlas s účastí.

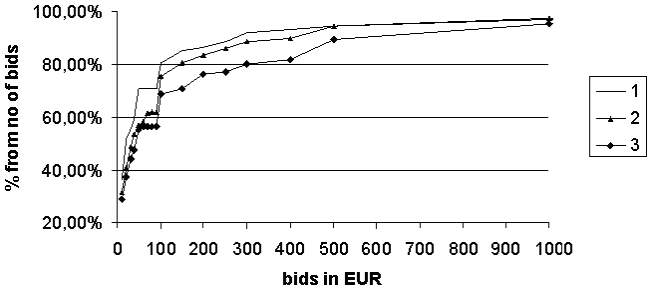
5.3 Histogramy požadovaných finančních kompenzací

V této části uvádíme histogramy požadovaných finančních kompenzací pro vybrané situace našeho experimentu. Histogramy v tomto případě dobře poslouží pro snadnou orientaci a porovnání výsledků v různých situacích. Rozhodli jsme se nerozdělovat data podle zvolených jazykových mutací, protože vzniklé množiny by byly v některých případech velice malé a výsledky by nemohly být považovány za průkazné.

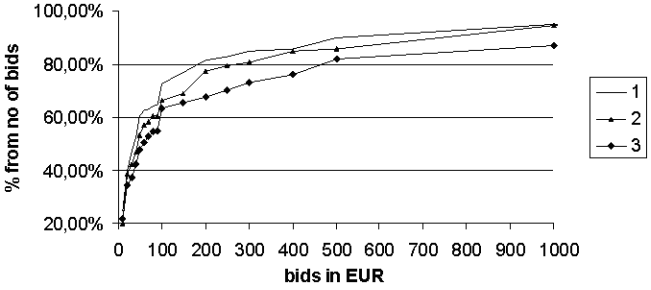
Obrázek 3 zobrazuje situaci pro variantu sledování využití e-mailové komunikace ve všech třech scénářích (akademické použití dat – čára 1; komerční využití dat – čára 2; vládní využití dat – čára 3) pro ty účastníky, kteří vyplnili všechny tři navrhované scénáře. Uvažujeme odpovědi těch účastníků, kteří nezvolili možnost vzdát se účasti ve druhém nebo třetím scénáři průzkumu. Z histogramu je patrný vzrůstající trend požadované finanční kompenzace se změnou využití získaných dat od akademického k vládnímu prostředí.

Histogram využití nástrojů pro komunikaci v reálném čase (instant messaging) je ve všech třech uvažovaných scénářích velmi podobný e-mailové komunikaci. Můžeme říci, že oba typy informací měly pro účastníky podobnou hodnotu. Výraznější posun jsme očekávali až v případě získávání veškerých komunikačních dat – zde jsme očekávali nejvyšší požadované finanční kompenzace. Situace za těchto podmínek je na obrázku 4.

Pokud provedeme srovnání histogramu na obrázcích 3 a 4, je vidět, že účastníci příliš nerozlišují mezi typy sledovaných služeb (rozdíly na začátcích histogramů jsou minimální). Výraznější



Obrázek 3: Histogram výše fin. kompenzace sledování e-mailové komunikace ve všech třech scénářích.



Obrázek 4: Histogram výše fin. kompenzace sledování veškeré online komunikace ve všech třech scénářích.

rozdíly jsou patrné až v druhé polovině účastníků.

6 Závěr

6.1 První studie – cena lokačního soukromí

V první části článku se zabýváme výsledky studie, která proběhla primárně mezi studenty univerzit. Prostřednictvím motivačního e-mailu jsme představili experiment a skryli jeho skutečnou podstatu za „výzkum topologie mobilních síti s ohledem na pohyb zákazníků". Skutečná

	První scénář			Druhý scénář		
Sledování	e-mail	messaging	vše	e-mail	messaging	vše
1. kvartil	10	8,3	10,4	10	10	15
2. kvartil	20	22,5	40	40	40	50
3. kvartil	100	80	150	100	100	200

Tabulka 6: Druhý scénář – komerční využití získaných dat.

	První scénář			Druhý scénář			Třetí scénář		
Sledování	e-mail	messaging	vše	e-mail	messaging	vše	e-mail	messaging	vše
1. kvartil	8,8	8,5	11,1	10	10	15	10	10	15
2. kvartil	20	25	40	40	40	50	50	50	60
3. kvartil	100	80	150	100	100	200	200	200	400

Tabulka 7: Třetí scénář – využití dat ve vládním prostředí.

podstata experimentu byla zveřejněna po ukončení sběru odpovědí a po prvním kole zpracování získaných dat.

Zhruba deset procent účastníků experimentu požadovalo výši finanční kompenzace za svoji účast pod jedno EURo. Myslíme, že to bylo způsobenou touhou účastníků zúčastnit se experimentu a spíše se zajímali o experiment jako takový a výše finanční kompenzace byla až druhotným faktorem. Po uveřejnění skutečné podstaty experimentu jsme obdrželi několik reakcí se zájmem o výsledky.

Jedním z podstatných zjištění našeho průzkumu může být vysoká citlivost účastníků z Řecka na možné narušení soukromí – nicméně výsledek bychom mohli považovat za průkazný v případě, že bychom měli více dat od účastníků z Řecka. Důvod takového výsledku (výše požadované finanční odměny) může být způsoben skandálem odposlechu mobilních telefonů, který se odehrál dva měsíce před naším experimentem [8]. Jednalo se o odposlechy vysoce postavených politiků po dobu jedenácti měsíců v průběhu olympijských her v roce 2004. Odposlechy byly potvrzeny začátkem února 2006.

Základní výsledky našeho průzkumu potvrzují výsledky průzkumu provedeného v Cambridge. Např. medián požadované finanční kompenzace je 20 GBP a 43 EUR (což odpovídá zhruba 28 GBP, přepočítáno kurzem ze srpna 2006) pro nekomerční využití získaných dat.

6.2 Druhá studie – využití nástrojů pro online komunikaci

Druhá část článku byla věnována experimentu, který byl proveden začátkem roku 2009 a jehož cílem bylo zjistit, jak si lidé cení informací o využití nástrojů pro online komunikaci. V průzkumu jsme získali cca 300 odpovědí z více než čtyř různých států pro první uvažovaný scénář (využití získaných dat v akademickém prostředí). Počet odpovědí je nižší, než jsme očekávali, nicméně stále použitelný pro podrobnou analýzu. Primárním cílem bylo zjistit výši požadované finanční kompenzace za účast v experimentu. Od účastníků bychom pomocí speciálně vyvinutého software získávali (v pravidelných intervalech) informace o využití různých forem online komunikace (e-mail, instant messaging). V článku jsme představili řadu základních výsledků a grafů.

Druhé kvartily výše finanční kompenzace můžeme považovat za hlavní výsledek našeho průzkumu (důvody pro použití kvartilů místo průměrů jsme uvedli v článku). Výše finanční kompenzace za sledování využití e-mailu je 30 EUR a stejná výše byla požadována i v případě sledování využití instant messagingu. Sledování všech komunikačních dat bylo „dražší" – konkrétně 50 EUR. V článku jsme provedli srovnání na úrovni ženy vs. muži, nicméně výsledky neukazují výrazné rozdíly mezi těmito skupinami účastníků.

Dále jsme vyhodnotili odpovědi těch účastníků, kteří poskytli informace i pro další uvažované scénáře zpracování získaných dat (využití dat

v komerčním prostředí a využití dat na vládní úrovni). Výsledky potvrdily naše předpoklady – výše požadované finanční kompenzace má vzestupnou tendenci tak, jak se mění způsob zpracování dat od akademického přes komerční až k vládnímu prostředí.

Z histogramů zobrazujících vývoj trendu požadované finanční kompenzace je vidět, že v některých momentech je instant messaging „dražší" než sledování e-mailů, nicméně sledování všech dat online komunikace je vždy „nejdražší".

Článek je částečně postaven na naší předchozí publikaci [9], FIDIS (www.fidis.net) deliverable D13.12 (WP13) a byl publikován na konferenci IS2 (Information Security Summit) 2009 [10]. Výsledky obou průzkumů budou též prezentovány v rámci informatického kolokvia FI MU dne 10. 11. 2009.

Literatura

[1] Boucher, P., Shostack, A., Goldberg, I.: *Freedom system 2.0 architecture.* whitepaper, Zero-Knowledge Systems, Inc. (2000)

[2] Law, G.: *Anonymity declines as zero-knowledge ends web service.* PC World (2001)

[3] Danezis, G., Lewis, S., Anderson, R.: *How much is location privacy worth?* In: Fourth Workshop on the Economics of Information Security. (2005)

[4] Hann, I.H., Hui, K.L., Lee, T.S., Png, I.: *The value of online information privacy: Evidence from the USA and Singapore.* In: International Conference on Information Systems. (2002)

[5] Acquisti, A., Grossklags, J.: *Privacy and rationality in individual decision making.* IEEE Security & Privacy **3**(1) (2005) 26–33

[6] Acquisti, A.: *Privacy in electronic commerce and the economics of immediate gratification.* In Breese, J.S., Feigenbaum, J., Seltzer, M.I., eds.: ACM Conference on Electronic Commerce, ACM (2004) 21–29

[7] Eagle, N.: *Machine Perception and Learning of Complex Social Systems.* PhD thesis, Massachusetts Institute of Technology (2005)

[8] Danezis, G.: *Government communication illegally wiretapped in Greece.* EDRI-gram http://www.edri.org/edrigram (2006)

[9] Cvrček, D., Kumpošt, M., Matyáš, V., Danezis, G.: *A study on the price of location privacy.* In WPES '06: Proceedings of the 5th ACM workshop on Privacy in electronic society, pages 109–118. ACM, 2006.

[10] Kumpošt, M., Matyáš, V.: *How much is privacy worth?* In 10th Information Security Summit, pages 139–151. Praha: Tate International, 2009. □