ÚVT MU
zpravodaj

Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě • říjen 2009 • roč. XX • č. 1

Bezpečnost bezdrátových technologií

Jan Krhovják, Václav Lorenc, FI MU a ÚVT

Používání bezdrátových technologií pro přenos informací se stalo během posledních 20 let doslova hitem. Asi každý z nás v dnešní době vlastní jedno či více zařízení, s nimiž lze na menší či větší vzdálenosti snadno a pohodlně komunikovat. V té nejjednodušší formě (jednosměrný přenos) se typicky jedná o pouhé zasílání příkazů takovému zařízení – ať již si zde představíme ovládání rádia, televizoru, počítače či některých dveřních a garážových systémů. Složitější forma komunikace (obousměrný přenos) pak zahrnuje vzájemnou komunikaci dvou a více zařízení najednou a pokrývá obousměrné přenosy dat nezbytných např. k realizaci složitějších komunikačních protokolů (jaké používají modernější systémy zabezpečení motorových vozidel či dokonce celých objektů).

K bezdrátovému přenosu signálů se typicky využívá některých částí elektromagnetického spektra neviditelných lidským okem. Různé části spektra ale mají různé vlastnosti, které mají samozřejmě také vliv na celkovou kvalitu komunikačního média a udávají, mimo jiné, i snadnost šíření signálu a jeho náchylnost k různým druhům rušení. Typickým příkladem budiž právě výše zmíněné běžné ovladače rádií, audio přehrávačů, či televizorů. Ty k přenosu informací využívají infračerveného záření, které se nešíří za pevné překážky, v některých případech vyžaduje relativně přesné zaměření a navíc je poměrně snadno ovlivňováno a rušeno nepříznivými vnějšími podmínkami (ať již slunečním zářením, deštěm, mlhou, prachem). To vše je samozřejmě z pohledu bezpečnosti poměrně pozitivní chování a (jednosměrná) komunikace mezi těmito typy zařízení proto mnohdy není nijak dodatečně zabezpečena. Tato zařízení pak lze (neautorizovaně) ovládat de facto libovolným programovatelným infračerveným vysílačem, např. i dostupným v mobilním telefonu.

Ostatní běžně využívané části elektromagnetického spektra již typicky tak příznivé vlastnosti nemají. Sílu vysílaného signálu (a tedy i okruh jeho šíření) lze sice v principu vždy regulovat zeslabením výkonu vysílače, ale i zdánlivě slabý signál (přijímaný z velké dálky) může být zachycen s využitím velmi citlivého přijímače. To je hlavním důvodem, proč by měly být veškeré bezdrátové komunikační spoje, které jsou určeny k přenosu citlivých informací, vždy vhodným způsobem zabezpečeny.

Ukázkovým příkladem, jak by zabezpečení bezdrátové komunikace nemělo vypadat, jsou některé ze soudobých bezšňůrových (z angl. cordless) klávesnic. Bezpečnost zde kromě omezeného výkonu vysílače „posiluje" i přítomnost více

(avšak typicky pouze dvou až čtyř) odlišných komunikačních kanálů reprezentovaných odlišnými nosnými frekvencemi. Asi netřeba detailně hluboce spekulovat nad tím, co vše se začne některým uživatelům objevovat jednoho dne na obrazovkách, vyskytne-li se v rámci jedné či více sousedních kanceláří (ne nutně stejné firmy či instituce) více kusů na tomto principu fungujících klávesnic a s nimi dodávaných přijímačů signálu. Nutno podotknout, že nemusí jít jen o zachycená jména a hesla, ale i např. o „přepisy" celých interních dokumentů velmi citlivé povahy.

Některé důmyslnější bezšňůrové klávesnice již sice využívají desítky tisíc odlišných komunikačních kanálů, čímž podobným situacím zamezují, bohužel cílený odposlech širšího komunikačního spektra (tj. všech komunikačních kanálů) je i nadále relativně snadno realizovatelný.

1 Což takhle kryptografie? A budeme vše šifrovat…

Nezbytnost zabezpečení citlivých dat (autentizace, důvěrnost, integrita) přenášených bezdrátovým médiem je tedy poměrně zřejmá a soudobé komunikační prostředky se již typicky snaží nějakým způsobem podporovat vhodné bezpečnostní mechanizmy. Zabezpečení dat však z jiného úhlu pohledu nemusí být pouze reakcí na ochranu citlivých informací, ale také mechanizmem, jak zavést např. zpoplatnění určité služby (accounting) či jiné zajímavé bezpečnostní vlastnosti (anonymita, nespojitelnost, nepopiratelnost). Ještě před srovnáním dalších používaných systémů/technologií, způsobů jejich zabezpečení a problémů, kterými tyto mechanizmy trpí, je proto nutno připomenout, že mnohé ze systémů vznikaly se značně odlišnými bezpečnostními požadavky, které se navíc postupem času dynamicky vyvíjely a měnily.

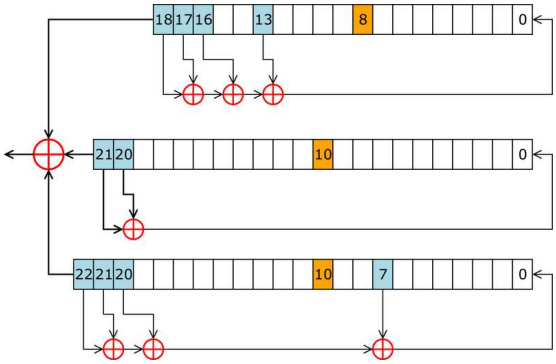
Pouze u prvních bezdrátových systémů nebyl, vyjma ojedinělých případů, žádný z výše uvedených bezpečnostních mechanizmů vyžadován. Dobrým příkladem budiž využití celosvětového družicového navigačního resp. polohového systému GPS (Global Positioning System) pro civilní sektor, kde jsou data z GPS satelitů vysílána nešifrovaná. Možnost ověření autenticity a integrity dat by však i zde byla vítaným vylepšením celého systému a nová generace systému GPS již počítá i se zajištěním důvěrnosti (z důvodu možného zpoplatnění služby, podobně jako v případě televizního satelitního vysílání). Poznamenejme, že i stávající systém GPS vysílá na odlišném kanálu mnohem přesnější informace (určené pro vojenské účely) a ty jsou již celkově lépe zabezpečeny (jedním z cílů je např. i zvýšená odolnost proti úmyslnému rušení či zmatení přijímače neautentizovaným signálem).

Plošné nasazení vhodných bezpečnostních mechanizmů ale komplikuje v tomto případě fakt, že satelitní vysílání jsou z pohledu běžných uživatelů typickým příkladem pouze jednosměrné komunikace. V současné době proto např. satelity vysílající televizní signál selektivně šifrují vysílaná data (rádia, televizní programy) různými šifrovacími klíči s omezenou časovou platností. V případě, že má uživatel nějakou službu (televizní program) předplacenu, tak od poskytovatele typicky obdrží kryptografickou čipovou kartu s odpovídajícími dešifrovacími klíči, které se periodicky obměňují na základě řídicích signálů pravidelně vysílaných z vysílajícího satelitu.

Dalším příkladem v Evropě asi nejpoužívanější bezdrátové technologie je GSM (Global System for Mobile Communication). Oproti svým analogovým předchůdcům již GSM podporuje digitální přenosy hlasu a dat (což je nezbytný předpoklad pro zavedení moderních bezpečnostních mechanizmů) a GSM telefon dnes v Evropě vlastní drtivá většina obyvatel. Bezdrátový signál je ve skutečnosti přenášen pouze mezi koncovými stanicemi (mobilní telefon) a základnovými stanicemi (BTS, Base Transceiving Station). Základnové stanice jsou pak připojeny do zbytku sítě metalickými spoji a pouze ve výjimečných případech i nákladnějším obousměrným satelitním spojem.

V době, kdy se GSM systém navrhoval, bylo základním požadavkem dosažení alespoň takové bezpečnosti, jakou poskytovaly tehdejší pevné linky – především se jednalo o zajištění autentizace (jednostranné ověření identity vlastníka telefonu a ochrana telefonu proti klonování), důvěrnosti (ochrana citlivých signalizačních a uživatelských dat) a anonymity (nemožnost vystopování polohy uživatele sledováním rádiové komunikační linky). GSM k tomuto účelu

využívá bezpečného prostředí kryptografické čipové karty (SIM, Subscriber Identity Module), dočasných identifikátorů, a několika typů proprietárních algoritmů (A3 pro autentizaci, A5 pro šifrování, A8 pro generování šifrovacích klíčů), jejichž princip fungování nebyl nikdy oficiální cestou publikován. Algoritmy A5/1 (viz obrázek 1) a A5/2 však byly v roce 1999 reverzním inženýrstvím odhaleny a následně zveřejněny [1].



Obrázek 1: Schéma šifrovacího algoritmu A5/1.

Mezi základní nedostatky celého GSM patří v dnešní době použití slabé 64bitové proudové šifry A5/1 či A5/2 (krom faktu, že je v obou případech šifra pouze 64bitová, byly v obou návrzích odhaleny i četné bezpečnostní slabiny), využití pouze jednosměrné autentizace (BTS se neautentizuje vůči mobilnímu zařízení a může být tedy nahrazena falešnou BTS, která mobilu navíc dokáže zakázat použití šifrování) a šifrování komunikace pouze v bezdrátové části sítě (na páteřní metalické síti či satelitním spoji jsou data typicky nešifrovaná).

2 Kryptografie znova a lépe. Šifrujeme, ale přestaneme utajovat!

Na přelomu tisíciletí se začaly bezdrátové technologie používat i k běžným přenosům mezi jednotlivými uživatelskými PC a tento trend byl o pár let později ještě umocněn masivním rozmachem používání přenosných počítačů (notebooky, PDA atp.). V této době vznikaly technologie jako Bluetooth a WiFi, které měly umožnit bezdrátové přenosy na relativně krátké vzdálenosti (desítky až stovky metrů). Se zabezpečením (autenticita, integrita, důvěrnost) přenášených dat se při návrhu počítalo, vědělo se o chybách existujících systémů, ale i přesto se v nových metodách zabezpečení objevilo několik zcela zásadních slabin (jak v návrhu, tak i v samotné implementaci). Otevřenost kryptografických algoritmů a jejich dostupnost širší veřejnosti však pomohla v relativně krátké době (jednotky let) řady z těchto nedostatků detekovat a odstranit (a to jak v reálných zařízeních, tak i v novějších verzích specifikací).

Bluetooth zařízení používají k vytvoření šifrovacího klíče proceduru tzv. párování, kdy je klíč vytvořen na základě krátkého hesla či PINu. Samotná procedura párování se však ukázala jako zranitelná a konstrukcí vhodné zprávy umožňuje útočníkovi párování i bez znalosti PINu. V mnoha jednodušších zařízeních je navíc PIN přednastaven (typicky s hodnotou 0000), což činí útok ještě snadnější. Se získaným šifrovacím klíčem již lze pak snadno pasivně odposlouchávat probíhající komunikaci (s tzv. Bluetooth puškou i na více než 1,5 km). Poznamenejme dále, že slabiny obsahuje i použitý šifrovací algoritmus E0, na jehož prolomení a získání 128bitového klíče je se znalostí dostatečného množství otevřeného textu potřeba jen 2^{38} operací (oproti očekávaným 2^{128}), což odpovídá cca 19 hodinám (na sběr dostatečného množství dat je potřeba 37 hodin). Více informací lze nalézt v [2, 3].

Bezdrátové sítě založené na standardu IEEE 802.11 (označované a certifikované jako Wi-Fi kompatibilní) a jejich zabezpečení prošly v uplynulých letech také poměrně drastickými změnami. Nejstarším podporovaným kryptografickým bezpečnostním mechanizmem je WEP (Wired Equivalent Privacy), zamýšlený zejména pro zajištění důvěrnosti (ale používaný i pro autentizaci). Existuje několik variant jeho implementací, které jsou vždy založené na proudové šifře RC4, a rozdíl mezi nimi je pouze v podporované délce šifrovacího klíče (64, 128 či někdy i 256 bitů). Na WEP existuje v současné době celá řada pasivních i aktivních útoků – jak na nevhodný autentizační mechanizmus (všichni uživatelé sdílejí stejné klíče, protokol typu výzva-odpověď využívá proudovou šifru, stanice si samy volí tzv. inicializační vektor), tak na samotný šifrovací mechanizmus využívající nevhodně navržený management klíčů (s využitím statistických

metod může útočník v řádech minut nepozorovaně odvodit statický tajný klíč). Podrobnosti lze nalézt například v [4, 5].

Novějším bezpečnostním mechanizmem, který řeší mnohé z výše uvedených nedostatků, je WPA (Wi-Fi Protected Access). Ten v principu zachovává použití WEP, ale pouze v rámci protokolu TKIP (Temporal Key Integrity Protocol). Pro šifrování každého paketu je zde již vygenerován zcela nový (dočasný) šifrovací klíč, zdvojnásbila se délka požadovaných inicializačních vektorů a k zajištění integrity zprávy se kromě nekryptografického CRC-32 (detekční a opravný kód) používá i kryptografický MIC (Message Integrity Code) označovaný jako Michael. Na WPA se až teprve nyní začínají objevovat první úspěšné útoky – jeden např. umožňuje zaslat po 12–15 minutách do šifrované sítě 5–7 vlastních rámců [6].

Posledním bezpečnostním mechanizmem je WPA2 (někdy označován jako RSN, Robust Security Network). WPA2 je standardizován v IEEE 802.11i a přidává podporu 128bitového algoritmu AES-CCMP (AES Counter Mode with Cipher Block Chaining Message Authentication Code), který slouží pro zajištění důvěrnosti i integrity. V současné době nejsou známy žádné praktické útoky na tento mechanizmus. Podpora AES však již vyžaduje i výměnu hardware (přechod z WEP na WPA vyžadoval pouze upgrade firmware) a některé starší operační systémy jej nepodporují.

Odlišné mechanizmy zabezpečení, jejichž základní principy jsou ale do jisté míry velmi podobné mechanizmům použitým v Bluetooth či Wi-Fi, pak využívají i modernější sítě typu ZigBee, WiMAX a mnohé další…

3 Jednočipová kryptografická zařízení. Utajujeme za každých okolností...

Během popisu bezpečnostní architektury některých systémů jsme také několikrát zmiňovali využití kontaktních kryptografických čipových karet (karty pro předplacené televizní vysílání, SIM karty v telefonech). Čipové karty jsou ale často využívány např. i jako platební či identifikační a přístupové karty. Tyto karty pak běžně slouží jako tzv. bezpečné nosiče dat, které navíc disponují určitým (i když značně omezeným) výpočetním výkonem. Jejich hlavním účelem je chránit citlivá data jejich vydavatelů (např. operátor mobilní telefonní sítě či banka) a musí proto být schopny zajistit těmto datům bezpečnost i v potenciálně nepřátelském prostředí (tj. v rukou uživatelů).

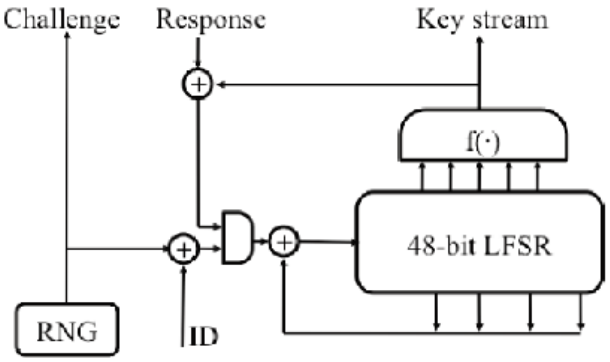
Kontaktní rozhraní, jehož prostřednictvím je po zasunutí do čtečky čip napájen, je ale z praktického hlediska poměrně omezující (vložení karty do čtečky zabere čas). Tento problém byl odstraněn až zavedením bezkontaktních čipových karet resp. obecně RFID čipů (často též označovaných jako RFID tagů). Existuje poměrně široká škála produktů založených na RFID, které se liší ať již metodami napájení (aktivní RFID obsahují vlastní zdroj napájení, pasivní RFID využívají k napájení elektromagnetické indukce), komunikační frekvencí, komunikačními protokoly atp. V současnosti je tato technologie využívána jednak k označení a identifikaci zboží (náhrada za čárové kódy), v bezdrátových čipových kartách (určeno zejména k identifikaci osob, umožnění přístupu do budovy/místnosti, k provádění mikroplateb) či ve státem vydávaných elektronických identifikačních dokumentech (elektronické pasy).

Starší systémy využívající bezkontaktní karty či jiné tagy typicky nemají žádné bezpečnostní mechanizmy implementovány – čip pak pouze v blízkosti přijímače vysílá nějaký identifikační kód, a na jeho základě systém rozpozná o jaký produkt/osobu se jedná. Udávaná vzdálenost vysílání pasivních tagů je totiž mnohdy limitována na několik centimetrů a odposlech z větší vzdálenosti (zejména od tagu ke čtečce) není tak snadný, protože přenos signálových prvků využívá tzv. zátěžové modulace. Zkopírování takovéhoto dostatečně blízkého (či nepozorovaně vypůjčeného) tagu ale není příliš obtížné a zabere jen jednotky sekund.

Základními bezpečnostními požadavky moderních čipů (ať již s kontaktním či bezkontaktním rozhraním) jsou u kryptografických čipových karet odolnost proti neautorizovanému přečtení uchovávaných dat a s tím související obtížnost padělání. U výrobců (nejen těchto) jednoči-

pových zařízení stále přetrvává pro snazší „splnění" těchto požadavků zcela utajený návrh daného čipu, a mnohdy i vytváření proprietárních protokolů či šifrovacích algoritmů. Ukázkovým příkladem produktu se zcela utajeným návrhem (jež se z bezpečnostního hlediska ukázal jako zcela nedostatečný) je bezkontaktní čipová karta MIFARE Classic.

Tuto bezkontaktní kartu využívají mnohé instituce pro identifikační účely, systémy podnikové docházky či mikroplatby (např. za služby hromadné dopravy některých měst nebo celých zemí). Na konferenci Chaos Communication Camp (CCC) 2007 odhalili pánové Nohl, Evans a Plötz první schémata čipu MIFARE Classic. Jejich metoda reverzního inženýrství spočívala v rozřezání a nasnímání jednotlivých vrstev čipu. Následným poloautomatickým zpracováním získaných snímků po rozpoznání jednotlivých hradel vlastně zjistili, jak čip funguje. Odhalili jednak princip proprietárního algoritmu Crypto-1 (viz obrázek 2) a jeho slabiny (včetně možného útoku hrubou silou pod 50 minut).



Obrázek 2: Schéma šifrovacího algoritmu Crypto1.

Dále odhalili také zcela zásadní chybu v návrhu generátoru (pseudo)náhodných čísel, spočívající v možnosti využití konstantního semínka, závislého pouze na počtu hodinových cyklů, jež uběhly od přivedení energie do čipu. Pseudonáhodná čísla generovaná pomoci registru s lineární zpětnou vazbou (LFSR) jsou navíc pouze 16bitová, což je v dnešní době zcela nedostatečné. Prezentovaná metoda snímání a automatické rekonstrukce funkcionality čipu je zcela jasným signálem, že bezpečnosti založené na utajování algoritmu již skutečně odzvonilo. V témže roce se na MIFARE Classic objevilo i několik dalších (nezávislých) útoků, demonstrujících jak chyby v komunikačním protokolu vedoucí až k získání části tajných informací uložených v čipu, tak také přítomnost nejrůznějších postranních kanálů [7, 8].

V posledních letech se v souvislosti s bojem proti terorizmu poměrně razantně prosadily a stále prosazují nejrůznější elektronické identifikační dokumenty (pasy, identifikační karty, řidičská oprávnění). V České republice se v současné době můžeme setkat zejména s elektronickými pasy. Součástí těchto pasů je kryptografická čipová karta s bezkontaktním komunikačním rozhraním. Uvnitř této karty jsou nahrány veškeré informace, které jsou v tištěné formě viditelné v pasu, ale také dodatečné tzv. biometrické údaje (např. fotografie, otisk prstu) sloužící k přesnější identifikaci předkladatele pasu. Tato data již zcela evidentně nejsou vlastnictvím vydavatele daného dokumentu (tj. státu), ale jedná se o osobní údaje držitelů pasů. Ochrana a mechanizmy zabezpečení těchto dat jsou proto v popředí zájmu nemalé části potenciálních držitelů pasu (nejen z akademických kruhů).

I v případě elektronických pasů se však začaly objevovat určité nedostatky. Mechanizmy sloužící proti padělání pasu (tzv. pasivní a aktivní autentizace) jsou do značné míry podobné s mechanizmy použitými u kontaktních čipových platebních karet kompatibilních se specifikací EMV (tzv. statická a dynamická autentizace dat). Problematickým místem je ale řízení přístupu, které je v první verzi navrženo tak, že k autentizaci využívá dat snímaných ze strojově čitelné zóny pasu (MRZ, Machine Readable Zone). Původním předpokladem (pro zamezení neoprávněného, neautorizovaného a nepozorovaného kopírování pasu) bylo, že přístup k čipu získá jen ten, kdo pas fyzicky vlastní (a má tedy přístup k MRZ). Ukázalo se však, že data v MRZ obsahují jen málo entropie – namísto teoretických 58/74 bitů obsahují data jen 32 bitů (tj. jsou snadněji předvídatelná). To umožňuje bezkontaktní a nepozorovaný přístup k citlivým informacím mnohem většímu okruhu útočníků.

Tento problém je vyřešen až rozšířeným řízením přístupu, které je založeno na důmyslnějších metodách symetrické a asymetrické kryptografie. Celý mechanizmus je navržen tak, aby jednotlivé státy mohly ovlivnit, které ostatní státy budou mít přístup k citlivým osobním (zejména biometrickým) údajům jejich občanů a držitelů pasů. Více informací lze nalézt v [9].

4 I kryptologové mohou jezdit v drahých autech. Nebo se do nich alespoň dostat...

Dalším z velmi často používaných bezkontaktních zařízení je i tak běžná a nenápadná věc, jako dálkové uzamykání a odemykání auta či garáže.

První klíče se u aut objevily v roce 1919, jako obrana před krádeží. Nešlo o klíče bránící přístup do automobilu, ostatně mnohá z aut neměla ani střechu, ale o klasické startovací klíčky. Teprve od konce dvacátých let minulého století se u aut se střechou bránilo přístupu do vozu právě zámkem na dveřích.

Snaha výrobců aut a garážových systémů poskytnout řidičům co nejvíce pohodlí při běžných činnostech vedla k tomu, že se v padesátých letech objevil systém vzdáleného přístupu do garáží bez klíče (RKE, Remote Keyless Entry), který byl od roku 1983 zaveden i pro automobily. Vlastník vozidla dostal s klíčkem od startéru i bezdrátový vysílač, jenž umožňoval ovládat zámky u dveří auta.

Původní myšlenka jistě šikovná, systémy dodávané do devadesátých let však trpěly nepříjemným problémem – vhodně vybavený útočník mohl kód (libovolně dlouhý a komplikovaný) posílaný bezdrátovým klíčem nahrát a kdykoliv zopakovat tak, aby si vyhlédnuté auto či garáž znovu otevřel. Frekvence dodávaných systémů byly veřejně známé (315 MHz v Severní Americe a Japonsku, 433.92 MHz v Evropě) a sestrojit podobný přístroj nebylo technicky neřešitelné. Řečeno odborně – systém nebyl chráněný proti útokům přehráním.

V průběhu devadesátých let minulého století se tak začala postupně užívat zařízení firmy Microchips, která v sobě obsahovala algoritmus KeeLoq, který už tomuto jednoduchému útoku byl schopen odolat. Ostatně posuďte sami – jeden z přístupů, tzv. „rolling codes" spočívá v tom, že zámek i fyzický klíč mají synchronizovaný čítač, který s každým dalším zmáčknutím fyzického klíče obě strany zvýší. Toto číslo je navíc pouze vstupem do speciální funkce, jejímž výsledkem je špatně predikovatelná posloupnost bitů posílaná směrem k zámku. Odposlechnutí tedy možné je, ale prosté zopakování již poslané sekvence útočníka k úspěšné krádeži nedovede.

Čistě teoreticky vzato bylo tedy zabezpečení systému KeeLoq zvoleno tak, aby odolávalo útokům. Nebo v to alespoň většina zúčastněných věřila.

Vývoj těchto vzdálených (ne)klíčů se nezastavil a pokračuje úspěšně dál, představena byla další zařízení od různých výrobců, která v sobě kombinují krom klíčů i platební karty a ještě více usnadňují život uživatelům automobilů. My se však zastavíme u zmiňovaného systému KeeLoq, který se v průběhu let dočkal masivního nasazení po celém světě (a používají jej automobilky jako Fiat, Chrysler, Daewoo, VW, Honda, Jaguar a další).

4.1 Postranní kanály, odběrová analýza

Aby bylo možno pokračovat ve výkladu slabin kryptografických zařízení, provedeme drobnou odbočku a vysvětlíme termín analýzy postranních kanálů, konkrétně oblast odběrové analýzy. Tento nápad se zrodil kolem roku 1998 v laboratořích Cryptographic Research, Inc., a to v hlavě Paula Kochera a jeho týmu během snahy o vyčítání tajných dat z kryptografických čipových karet [10].

Během práce libovolných počítačových čipů, tvořených milióny tranzistorů, nejsou jednotlivé bloky čipu vytěžovány stejnou měrou. Tento fakt sám o sobě nijak převratný není, právě tato vlastnost čipů je jejich návrhářům známa již od počátku. Co přišlo v roce 1998, byla úvaha, že zpracovává-li kryptografický čip tajná data a provádí tedy nějaký algoritmus, pak jednotlivé části takového algoritmu, kupříkladu blokové šifry, se na procesoru projeví v různý okamžik jinak velkým odběrem. Pro ilustraci – násobení a umocňování jsou dvě různě náročné operace, při kterých se zapojí jiné množství tranzistorů daného obvodu. Pečlivým sledováním odběru je tedy možné, bez dalších znalostí čipu či konkrétního

prováděného algoritmu, tyto operace identifikovat. Tento přístup je znám pod názvem jednoduchá odběrová analýza (SPA, Simple Power Analysis).

Při využití statistických metod a násobného měření (prováděného i na různých vstupních datech) je možné odhalit pomocí diferenciální odběrové analýzy (DPA, Differential Power Analysis) nejen samotné operace, ale i jednotlivé bity tajných dat, které do procesu šifrování také vstupují (viz obrázek 3). Tedy krom získání informace, že právě probíhá operace násobení, zjistí útočník například i to, že čip s vysokou pravděpodobností násobí čísla lichá. Zdá se vám to málo? Věřte, že postupným odhalováním dalších a dalších vlastností operací a jejich operandů je možné se postupně dobrat až k celému tajnému klíči.

Hodila by se vám analogie? Vlastníci notebooků se dozajista potkali se situací, kdy je procesor vytížený natolik, že se větráčky chladící celý systém točí jako splašené. Tímto způsobem je tedy možné alespoň určit, a to bez jakéhokoliv dalšího zkoumání notebooku a jeho softwarového vybavení, že je jádro procesoru zatíženo nějakou náročnou operací. Právě jste úspěšně provedli pozorování postranního kanálu!

U speciálních kryptografických čipů, jejichž hlavním cílem je udržet v sobě tajný klíč, který se nikdy nesmí dostat do světa, jde o závažný problém, který od té doby neustále motivuje další a další výzkumníky a vývojáře kryptografického hardware, a to jak z pohledu útočníků, tak i obránců.

A samozřejmě – proti těmto i dalším útokům existují i obranné mechanizmy. Stejně jako existují nové a stále účinnější útoky.

4.2 Útoky na KeeLoq

Vraťme se k zabezpečení automobilů. Více než dvacet let vydrželo firmě MicroChips tvrzení, že jejich systém je dokonalým zabezpečením draze pořízených automobilů.

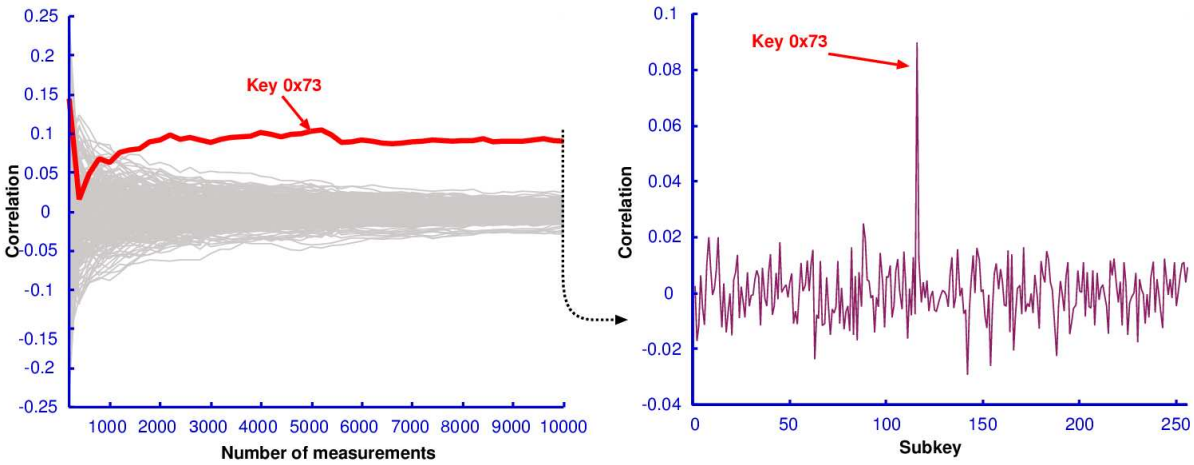
To se však zásadně změnilo roku 2006, když se do světa dostala část zodpovědná za kryptografickou stránku systému KeeLoq a vědci se rozhodli přijít na kloub celému procesu. Mezi tvrzením, že je systém bezpečný, a bezpečným systémem jako takovým, je totiž propastný rozdíl.

Uvnitř KeeLoqu se skrývá algoritmus generování přístupových kódů, který využívá principu tzv. posuvných registrů s nelineární zpětnou vazbou, NLFSR, (Non-Linear Feedback Shift Registers). Jednoduše přiblíženo – funkce dostává na vstupu sadu bitů a na základě svého předchozího stavu a vstupu vygeneruje nejen výsledek, ale i stav pro další výpočet. Tyto funkce se často používají jako základ pro generátory pseudonáhodných čísel, a v KeeLoqu měly za úkol zabránit možnosti odposlechu a následného přehrání kódu pro manipulaci se zámky.

Andrey Bogdanov [11] a Nicolas Courtois se tedy pokusili v roce 2006 zaútočit za pomoci algebraických postupů a lineárních transformací na část zodpovědnou za generování kódů. Jednalo se však pouze o první krůčky – ve skutečnosti byla celá řada zámků mnohem více náchylná na útoky hrubou silou, kdy útočníci s kvalitním vybavením (zařízením založeným na tzv. programovatelných hradlových polích) byli schopni během několika týdnů odhalit klíč používaný konkrétním majitelem auta.

Týdny času a náročné zařízení však pořád představovaly poměrně velké překážky pro běžné útoky, a pro výrobce KeeLoqu to celé byla spíše nepříjemnost, než konkrétní problém. V roce 2007 skupina studentů a výzkumníků z univerzity v Leuvenu ve spolupráci s dalšími týmy nalezla další útok [12]. Ukázalo se, že pokud by se jim podařilo odhalit klíč pro konkrétního výrobce zařízení založených na KeeLoqu, stačilo by jim k úspěšnému útoku jen odposlechnout komunikaci mezi zámkem a klíčem. Teoretický pokrok značný, ale z praktického hlediska to stále nebylo ono – zjištění oněch tajných klíčů výrobců byla netriviální překážka.

Nicméně důležitý poznatek byl, že KeeLoq předpokládá, že vysílač v daném systému vlastní unikátní tajemství, kterým šifruje sekvence posílané směrem k přijímači, zatímco přijímač obsahuje tzv. hlavní klíč (z angl. master key) – bez znalosti konkrétního tajemství vysílače je tak schopen ověřit, že komunikace, která s ním probíhá, pochází od „správného” výrobce.



Obrázek 3: Naměřené odběry během kryptooperací.

A v tuto chvíli nastupuje na scénu poslední příspěvek z řad akademické obce. 31. března roku 2008 přišel tým z univerzity v Bochumi s kompletním postupem, který v důsledku umožňuje útočníkovi opravdu odposlechnout pouze dvě zprávy vyměněné mezi klíčem a automobilem či garážovými vraty, aby z toho následně bylo možné zrekonstruovat původní klíč[13]. Klíčovou se ukázala právě analýza postranních kanálů, která umožnila vyčtení výše zmiňovaných tajných klíčů výrobců z přijímačů zabudovaných v garážových vratech. Neb se tyto hlavní klíče nemění, stačí si pořídit dostatečnou zásobu zařízení pro vzdálené odemykání a klíče si např. přes Internet vyměnit s ostatními útočníky. Výroba padělku klíče od vašeho automobilu, a to i na vzdálenosti stovek metrů, je následně záležitostí pár vteřin.

Naštěstí to však neznamená, že by útočník mohl s autem odjet. V dalším pokračování úspěšného útoku mu brání imobilizér a startér, často používající odlišné mechanizmy nebo alespoň způsoby odvozování klíčů. Jen první úroveň obrany již padla.

Je poměrně zajímavé, že slabina není ani tak vázaná na samotnou funkci použitou uvnitř KeeLoqu, stejně dobře by bylo možné napadnout i další symetrické šifry (včetně AES) použité na jejím místě. Dalším zajímavým faktem je i skutečnost, že autoři KeeLoqu nabízeli od konce devadesátých let i systémy s větší délkou klíče, které by v mnohém ztížily celou analýzu a v podstatě eliminovaly útoky hrubou silou – ty se však v reálné výrobě jaksi neobjevily.

5 Závěr

Jak plyne z předchozích odstavců, bezkontaktní či bezdrátové technologie představují nelehkou technologickou oblast, alespoň co se zabezpečení týče. Jejich odposlech je často technicky realizovatelný i s menšími prostředky a všechny důležité věci kolem zajištění autentizace, integrity či důvěrnosti je tedy třeba řešit na úrovni kryptografických operací. A to je i místo, kdy přichází do hry tzv. Kerckhoffův princip, nabádající k tomu, že je mnohem snazší utajit pouze privátní klíče než celý algoritmus. V některých oblastech (bezdrátové sítě, přístupové karty, elektronické pasy) tento přístup již funguje, v jiných je utajení algoritmů stále základní součástí zabezpečení.

V posledních letech se navíc ukazuje, že softwarová a hardwarová stránka kryptografických zařízení spolu velmi těsně souvisí, a chyba na jedné nebo druhé straně může vést k dalekosáhlým důsledkům a nemalým investicím na záchranu nezabezpečených systémů. V době značných technologických pokroků a rychlých komunikačních sítí, je i termín tzv. výpočetní bezpečnosti podrobován neustálým zkouškám. Objevují se proto i nové, neotřelé přístupy s cílem lépe bránit tajné klíče a bránit jejich kopírování do jiných zařízení rovnou na fyzické úrovni (PUF, Physical Unclonable Functions).

Bezpečí je velmi křehký stav a je nutné o něj neustále pečovat. Pro začátek přinejmenším informováním o existujících problémech a možnostech jejich náprav.

A co systémy fungující denně kolem vás? Důvěřujete jejich bezpečnosti? Nezapomeňte, že každý systém je pouze tak bezpečný, jak je bezpečný jeho nejslabší článek...

Literatura

[1] M. Briceno, I. Goldberg, and D. Wagner. *A pedagogical implementation of A5/1*. 1999. Dostupné na: http://www.scard.org/gsm/a51.html.

[2] A. Becker. *Bluetooth Security & Hacks*. 2007. Dostupné na: http://gsyc.es/~anto/ubicuos2/bluetooth_security_and_hacks.pdf.

[3] Y. Lu, and S. Vaudenay. *Faster Correlation Attack on Bluetooth Keystream Generator E0*. 2004. Dostupné na: http://lasecwww.epfl.ch/pub/lasec/doc/YV04a.pdf.

[4] N. Borisov, I. Goldberg, D. Wagner. *Intercepting Mobile Communications: The Insecurity of 802.11*. 2001. Dostupné na: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.

[5] E. Tews, A. Pychkine, and R.-P. Weinmann. Breaking 104 bit WEP in less than 60 seconds. 2007. Dostupné na: http://eprint.iacr.org/2007/120.pdf.

[6] M. Beck, and E. Tews. *Practical attacks against WEP and WPA*. Prosinec, 2008. Dostupné na: http://dl.aircrack-ng.org/breakingwepandwpa.pdf.

[7] F. D. Garcia et al. *Dismantling MIFARE Classic*. 2008. Dostupné na: http://www.cs.ru.nl/~flaviog/publications/Dismantling.Mifare.pdf.

[8] F. D. Garcia et al. *Wirelessly Pickpocketing a Mifare Classic Card*. 2009 Dostupné na: http://www.cs.ru.nl/~flaviog/publications/Pickpocketing.Mifare.pdf.

[9] Z. Říha, P. Švenda, V. Matyáš. *Bezpečnost elektronických pasů (část II)*. Crypto-World 1/2007. Dostupné na: http://crypto-world.info/casop9/crypto01_07.pdf.

[10] P. Kocher, J. Jaffe, B. Jun. *Differential Power Analysis*. 1999. Dostupné na: http://www.cryptography.com/resources/whitepapers/DPA.pdf

[11] A. Bogdanov. *Cryptanalysis of the KeeLoq block cipher*. Cryptology ePrint Archive: Report 2007/055. Dostupné na: http://eprint.iacr.org/2007/055

[12] E. Biham, O. Dunkelman, S. Indesteege, N. Keller, B. Preneel. *How To Steal Cars – A Practical Attack on KeeLoq*. 2007. Dostupné na: http://www.cosic.esat.kuleuven.be/keeloq/

[13] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar et al. *Physical Cryptanalysis of KeeLoq Code Hopping Applications*. Cryptology ePrint Archive: Report 2008/058. Dostupné na: http://www.crypto.rub.de/keeloq/

□

Session Riding

Jaromír Dobiáš, Zdeněk Říha, FI MU

Pojem „Session Riding" [2] označuje skupinu zranitelností a útoků typu Cross Site Request Forgery (CSRF) [3], [4]. Session Riding bývá často ztotožňován se samotným CSRF, avšak, jak již napovídá název, Session Riding je možno považovat za podtřídu, která se týká uživatelova otevřeného a již autentizovaného sezení (tzv. session). Útoky typu Session Riding je možné realizovat díky důvěře zranitelné služby v to, že dotazy, které služba přijímá prostřednictvím protokolu HTTP z prohlížeče uživatele, jsou platnými požadavky zadanými z iniciativy uživatele. Přestože počátky odhalování a dokumentování zranitelností založených na tomto principu je možno datovat do roku 2001 a některé zdroje hovoří dokonce o dobách dřívějších, počet webových služeb a aplikací, které je dnes stále možné napadnout prostřednictvím bezpečnostní zranitelnosti typu Session Riding, je alarmující.

Pro praktické ověření tohoto tvrzení jsme se rozhodli provést test nejmenovaného webového systému z prostředí českého Internetu poskytujícího mimo jiné e-mailové účty svým uživatelům.

V průběhu testu se nám podařilo využitím kombinace zranitelnosti XSS (Cross Site Scripting, viz např. [5]) a Session Riding docílit toho, že zprávy určené příjemci byly automaticky přeposílány i na náš e-mailový účet a to pouze tím, že jsme uživateli zaslali speciálně upravený e-mail a počkali, až se přihlásí do systému. Žádná další aktivita příjemce nebyla nutná. K provedení útoku stačilo pouhé přihlášení oběti do systému.

1 Princip útoku

Útoky využívající zranitelnost typu Session Riding používají ke svému provedení relaci uživatele přihlášeného ke zranitelné službě. Jednoduchý útok může být realizován například tak, že útočníkem podstrčený URL odkaz vyvolá v prohlížeči nic netušícího přihlášeného uživatele akci, kterou daný uživatel nezamýšlel provést. Tato akce je provedena v kontextu autentizovaného spojení mezi daným uživatelem a zranitelnou webovou aplikací. Příkladem takové akce by mohl být v případě zranitelné aplikace elektronického bankovnictví například převod peněz z účtu podvedeného uživatele na účet útočníka:

```
http://zranitelnaBanka.com/
prevod.php?prevadenaCastka=
1000000&naUcet=IDutocnik
```

Pokud by bankovní webová aplikace akceptovala dotaz v uvedeném formátu bez kontroly dalších prvků, útočníkovi by stačilo vytvořit dostatečně důvěryhodný e-mail, který by přiměl uživatele kliknout na daný odkaz. K provedení převodu by však došlo pouze tehdy, pokud by byl uživatel v jiném okně případně v některé záložce daného prohlížeče přihlášen ke zranitelné aplikaci elektronického bankovnictví.

Útoky tohoto typu lze provádět především proto, že řada služeb verifikuje po úspěšném přihlášení uživatele pouze jeho identitu. Nekontroluje však, že požadavek, který pod danou identitou server obdržel, je skutečně zamýšleným požadavkem daného uživatele. Identita je v případě webových aplikací obvykle ověřována na základě identifikátoru session ID, který prohlížeč zasílá automaticky prostřednictvím HTTP metody GET, POST nebo nejčastěji v Cookie. Tím, že se identifikátor posílá při komunikaci automaticky, nemá uživatel prakticky žádnou možnost kontroly nad akcemi, které jsou vyvolávány z jeho prohlížeče. Pokud akce směřují do autentizované oblasti, zranitelná aplikace nedokáže rozeznat, zdali přicházejí skutečně od uživatele nebo z jiného zdroje využívajícího jeho prohlížeč. Vůči zranitelnosti typu Session Riding jsou náchylné také webové systémy, které používají k autentizaci uživatele metodu „Basic Authentication" podporovanou nativně protokolem HTTP. Při použití tohoto autentizačního mechanizmu jsou totiž autentizační údaje zasílány rovněž automaticky.

Jakmile se uživatel přihlásí do autentizované sekce zranitelné webové služby, mají veškeré následné dotazy odeslané z prohlížeče přihlášeného uživatele také možnost ovlivňovat stav uvnitř autentizované oblasti. Tato možnost existuje až do okamžiku, kdy se uživatel odhlásí nebo dojde k vypršení platnosti relace. V praxi to znamená, že pokud uživatel v době svého aktivního přihlášení obdrží podvržený hypertextový odkaz, který směřuje do autentizované sekce, provede zranitelná webová aplikace akci podstrčenou útočníkem pod identitou přihlášeného uživatele. Útočník k tomu obvykle využívá sociálního inženýrství a snaží se nalákat uživatele na aktivaci nevinně vypadajícího hypertextového odkazu. Typicky se k propagaci podvrženého hypertextového odkazu využívá e-mail, chat nebo webové fórum.

Útočník však má také silnější zbraň, která mu umožňuje aktivovat podvržený odkaz v prohlížeči uživatele bez nutnosti jeho přímé spolupráce. Útočník například vyláká oběť na svoji stránku, která obsahuje HTML kód pro načítání externích objektů (např. HTML element IMG pro načítání obrázků). Kód za normálních okolností odkazuje na zdroj externího objektu (např. obrázku, souboru definic kaskádových stylů nebo JavaScriptu), odkud je jeho obsah načítán, avšak trik útočníka spočívá v tom, že místo původního obsahu vyvolává hypertextový odkaz požadovanou akci v autentizované sekci zranitelné webové aplikace. To sice může způsobit podezřelé anomálie v načítané stránce (například ikonku chybějícího obrázku), avšak prohlížeč ve snaze o

načtení externího objektu voláním podstrčeného odkazu způsobí vykonání útočníkem zamýšlené akce, a to v kontextu aktuální relace uživatele! Byl-li například uživatel již přihlášen ke zranitelnému e-shopu, lze takto podvrhnout objednávku bez jakýchkoliv viditelných stop indikujících, že něco není v pořádku. K rozšíření těchto lstivých „objektů" mohou sloužit například různá webová fóra či blogy, kde je povoleno přímé načítání externích objektů.

Útoky vedené prostřednictvím zranitelnosti typu Session Riding bývají často přirovnávány k útokům krádeže relace a následné impersonaci, kdy útočník převezme plnou kontrolu nad napadeným účtem. Zranitelnost Session Riding však lze považovat v tomto směru za nebezpečnější, neboť její efekt může být v podstatě stejný, při vynaložení menšího úsilí a zanedbatelné možnosti detekce útoku. Při zneužití prohlížeče oběti se totiž podvržený požadavek útočníka jeví navenek jako právoplatný požadavek oběti, nevykazující atypický projev, jakým je například podezřelá změna IP adresy požadavku v případě útoku krádeže relace (tzv. session hijacking).

2 Příklady zranitelností

Původem zranitelnosti je samotná aplikace poskytující patřičnou funkčnost autentizovaným uživatelům. Obecně lze říci, že čím důležitější je webová aplikace, která je náchylná vůči útokům typu Session Riding, tím závažnější důsledky má útok využívající zranitelnosti v této aplikaci. Kromě zmiňovaného výskytu zranitelnosti v aplikacích elektronického bankovnictví patří mezi další rizikové potenciální zdroje například sociální sítě, aukční portály, portály pro nákup a prodej akcií a cenných papírů, webová rozhraní správy/administrace nejrůznějších systémů, nebo aplikace, které na základě jediného přihlášení poskytují přístup k širokému spektru webových služeb (tzv. Single Sign-On).

Session Riding ohrožuje především uživatele zranitelné služby, samotná webová služba je jen zprostředkovatelem útoku. To také může být důvodem pro značné rozšíření tohoto problému a malý zájem ze strany administrátorů a webových návrhářů a programátorů.

Ve světě se již objevily případy zranitelnosti tohoto typu ve službách elektronického bankovnictví renomovaných bankovních institucí. Známým se stal případ nalezení této zranitelnosti na portálu ING Direct.com týmem bezpečnostních výzkumníků z Princetonské Univerzity [6]. Jejich odhalení šokovalo veřejnost tím, že pomocí existující zranitelnosti bylo jednoduše možné provést převod peněz z účtu oběti na účet útočníka a to i přesto, že relace byla zabezpečena šifrovaným spojením SSL [1].

Jiným příkladem z praxe muže být například zranitelnost, která byla odhalena ve firmware verze 4.30.9 bezdrátového přístupového bodu Linksys WRT54GL [7]. S využitím této zranitelnosti bylo možné provést neautorizované změny v konfiguraci tohoto přístupového bodu. Bylo tedy možné například návštěvou určité stránky způsobit deaktivaci firewallu tohoto zařízení.

3 Jak se bránit?

Existuje celá řada více či méně úspěšných mechanismů, které bývají v boji proti zranitelnosti typu Session Riding používány. Ve snaze zabránit jejímu výskytu bývá jako obranný mechanismus často nasazována kontrola HTTP parametru „Referer" (URL předchozí stránky z níž jsme se dostali na aktuální stránku). Tímto způsobem se inkriminovaná aplikace snaží hlídat, zda požadavek na provedení autentizované akce pochází z očekávaného umístění rozhraní (obvykle z lokace, kde je webový formulář způsobující nastavení hodnot). Tato metoda není zcela vhodným řešením, jelikož nemalé množství uživatelů si parametr Referer blokuje. Tento mechanismus navíc není schopen zabránit útokům, které z očekávaného umístění pocházejí. Jiným obranným mechanismem, který bývá často nasazován jako protiopatření vůči zmiňované zranitelnosti, bývá nahrazení HTTP metody GET metodou POST při přenosu řídících parametrů. Tento mechanismus eliminuje kupříkladu možnost použití načítání externího objektu jako prostředku provedení útoku. Útočník však může obejít i tento mechanismus, zejména v případě výskytu zranitelnosti XSS, a docílit tak vykonání akce v kontextu uživatelského účtu oběti (např. využitím neviditelného rámce IFRAME obsahujícího podvrženou

stránku). Útok je sice pracnější a méně efektivní než v případě nastavení hodnot prostřednictví URL, nicméně pokud dokáže útočník zkonstruovat dostatečně přesvědčivý scénář, pak s využitím technik sociálního inženýrství může být dopad útoku srovnatelný.

Často používanou obranou proti zranitelnostem webových služeb je použití potvrzovacích dialogů. Tato metoda je však v drtivé většině případů pouze na obtíž uživatele, navíc je útočník většinou schopen obejít i tento mechanismus, a to tak, že postupnou návštěvou patřičných hypertextový odkazů, které odpovídají akci potvrzení, simuluje kroky uživatele. I v případě, že je aplikace ošetřená sofistikovanější logikou potvrzovacích dialogů je schopen útočník simulovat akce uživatele například i vložením umělého zpoždění mezi jednotlivé dotazy v případě možnosti vyvolání kontextu JavaScriptu (nejčastěji prostřednictvím zranitelnosti XSS).

Vhodným přístupem, který řeší popisovaný bezpečnostní problém, je validace požadavků uživatele ve třech krocích. V prvním kroku se ověří, že uživatel je držitelem patřičných autentizačních údajů. V druhém kroku se ověří, zdali jsou v dotazu přítomny veškeré požadované argumenty. Ve třetím kroku se ověří, zdali uživatel opravdu použil patřičné webové rozhraní pro vytvoření a odeslání daného požadavku. K ověření požadavku je vhodné použít sdíleného tajemství mezi rozhraním na straně uživatele a aplikací na straně serveru. Toto tajemství je vhodné generovat pseudonáhodně na straně serveru v době, kdy uživatel úspěšně ověří svou identitu vůči němu. Tajemství není možné ukládat do cookie uživatele, jelikož cookie se zasílá serveru automaticky. Běžnou praxí je přidávat tento parametr do skrytého pole formuláře, který je proti útokům typu Session Riding ochráněn. Uvedený mechanismus zabraňuje útočníkovi zasílat validní dotazy prostřednictvím přihlášeného uživatele, neboť konstrukce platného dotazu vyžaduje znalost časově proměnného tajemství. Pokud by bylo možné tajemství automatizovaně zjišťovat jiným způsobem (například pomocí útoku XSS), byl by útok přece jen proveditelný, v každém případě se však použitím popsaného obranného mechanismu výrazně zvyšuje náročnost provedení úspěšného útoku.

4 Závěr

Se zranitelnostmi a útoky typu Cross Site Request Forgery se setkáváme již řadu let. Kategorie útoků „Session Riding", která se týká spojení zachovávajících stav mezi jednotlivými dotazy, je nebezpečná v tom, že zneužívá důvěru webové aplikace v platnost požadavků pocházejících z prohlížeče autentizovaného uživatele. Se službami zranitelnými vůči tomuto typu útoku se setkáváme relativně často. Existují sice metody, jak se webové služby mohou bránit, jejich implementace však nemusí být vždy snadná.

Článek je krácenou a upravenou verzí článku [8].

Literatura

[1] K. J. Higgins. *CSRF Flaws Found on Major Websites*. DarkReading, 2008. http://www.darkreading.com/security/appsecurity/showArticle.jhtml?articleID=211201247

[2] Thomas Schreiber. *SESSION RIDING: A Widespread Vulnerability in Today's Web Applications*. SecureNet whitepaper. prosinec 2004. http://www.securenet.de/papers/Session_Riding.pdf

[3] *OWASP Testing Guide: Testing for CSRF*. http://www.owasp.org/index.php/Testing_for_CSRF

[4] D. Stuttard, M. Pinto. *The Web Application Hacker's Handbook – Discovering and Exploiting Security Flaws*. ISBN: 0470170778

[5] Wikipedia. *Cross-site scripting*. http://en.wikipedia.org/wiki/Cross-site_scripting

[6] W. Keller, E. W. Celtem. *Cross-Site Request Forgeries: Exploitation and Prevention*. září 2008. http://www.freedom-to-tinker.com/sites/default/files/csrf.pdf

[7] T. Bratusa. *Linksys WRT54 GL Session Riding (CSRF)* http://www.securiteam.com/securitynews/5TP0320N5U.html

[8] J. Dobiáš, Z. Říha. *Session Riding*. DSM, Praha: Tate International, s.r.o., XIII, 1, s. 40–42. ISSN 1211-8737. 2009 □

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.

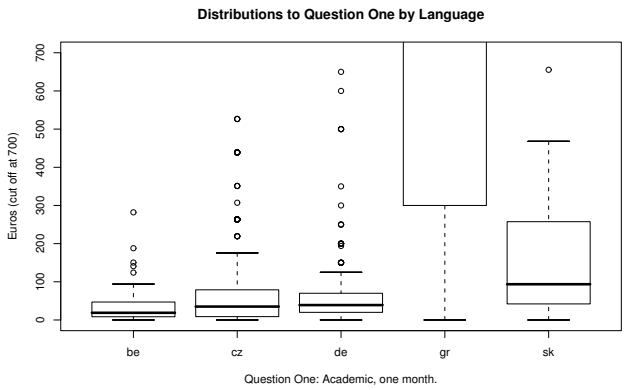
4.3 Hlavní výsledky

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.

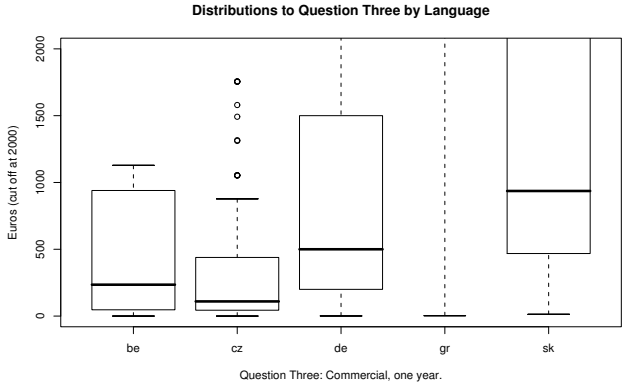
Získali jsme data ze tří aukcí (scénářů). První a druhý scénář bylo sledování polohy mobilního telefonu po dobu jednoho měsíce, přičemž v prvním případě pro akademické účely a ve druhém případě pro komerční využití. Ve třetím scénáři

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.

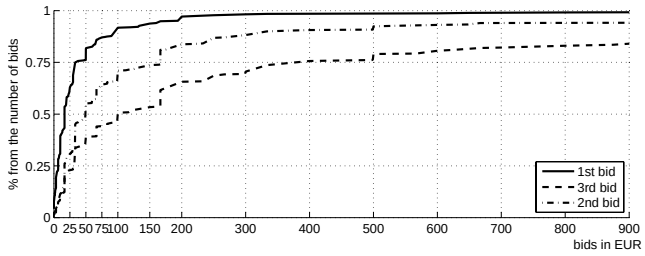


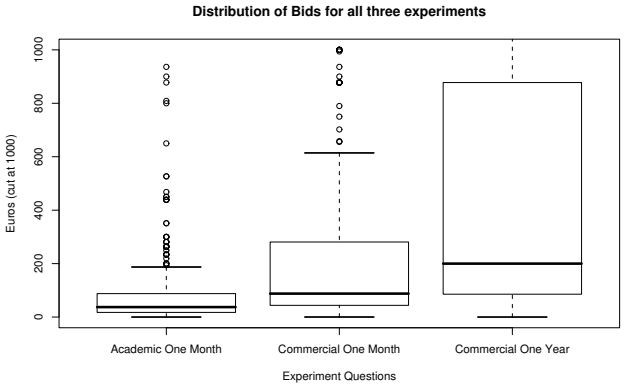
(a) Výše fin. kompenzace v prvním scénáři.



(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.

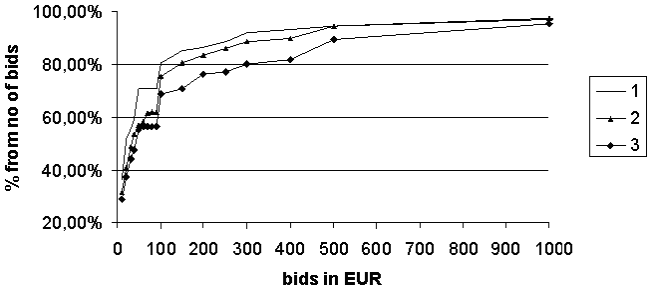
5.3 Histogramy požadovaných finančních kompenzací

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.

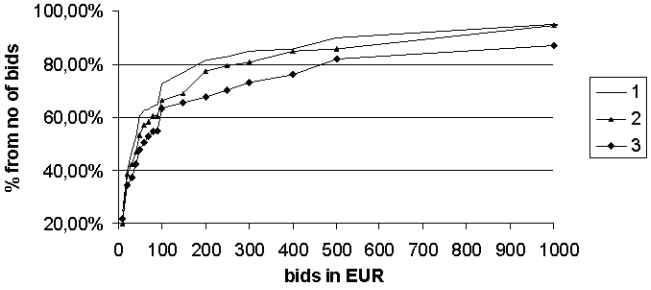
Obrázek 3 zobrazuje situaci pro variantu sledování využití e-mailové komunikace ve všech třech scénářích (akademické použití dat – čára 1; komerční využití dat – čára 2; vládní využití dat – čára 3) pro ty účastníky, kteří vyplnili všechny tři navrhované scénáře. Uvažujeme odpovědi těch účastníků, kteří 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. □

Nástroje Google. 6. Google Docs

Tomáš Pitner, FI MU

1 Co jsou Google Docs

Google Docs (zkráceně *GDocs* nebo česky „Dokumenty Google") jsou vedle známého *GMailu* asi nejvýraznějším představitelem rodiny webových aplikací Google. Slouží k individuálnímu, ale především kolektivnímu editování textových dokumentů, souborů tabulkového kalkulátoru, prezentací a dotazníkových formulářů.

Používat je může zdarma každý registrovaný uživatel služeb Google, aniž by na svém lokálním počítači musel cokoli instalovat; stačí mu k tomu téměř jakýkoli webový prohlížeč s povoleným JavaScriptem. Google Docs najdeme na `http://docs.google.com` a jsou také přímo přístupné kliknutím z horní lišty ostatních aplikací Google.

Nad konkurenci, rovněž nabízející kancelářské balíky jako webové aplikace, je vyvyšuje především dobrá integrace s ostatními službami (GMail, Blogger), slušné možnosti importu a exportu z nejfrekventovanějších formátů kancelářských balíků, některé pokročilé funkce a široká komunita uživatelů, kteří nejen dodávají volně použitelné šablony, ale především s nimiž lze dokumenty sdílet a pracovat na nich v týmu. Nejprve si přiblížíme základní funkcionalitu spojenou s vytvořením dokumentu a jeho úpravami.

2 Práce s dokumenty

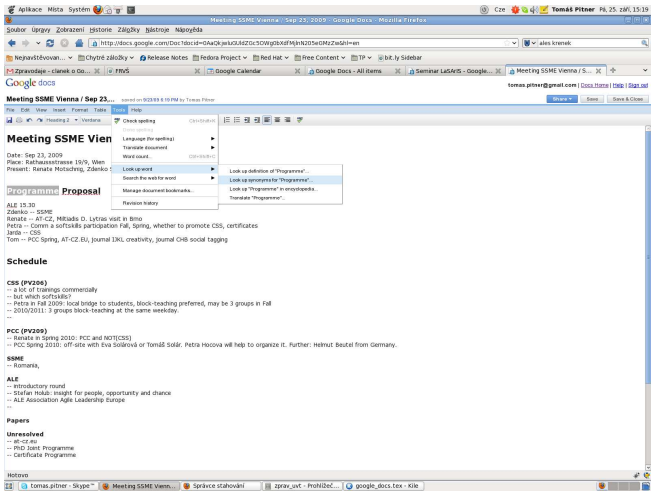
Jak bylo uvedeno, k použití GDocs postačí prohlížeč, do nějž zadáme adresu aplikace, a jsme-li již registrováni, můžeme se přihlásit. Ani registrace není obtížná a stále více aplikací je lokalizováno i do češtiny. Po přihlášení uvidíme složky pro soubory a nahoře se objeví podobná nabídka jako u jiných editorů. Začneme vytvořením nového dokumentu či jeho importem z existujícího souboru nebo přímo z přílohy mailu doručeného do služby GMail. Zajímavou možností je také založit nový dokument pouhým odesláním na speciální adresu přidělenou individuálně každému uživateli služby GDocs – vypadá asi jako `Tomas+Pitner-HJgtsg5567@prod.writely.com`. Pak můžeme pokračovat jeho úpravou. Budeme se zde věnovat podrobněji práci s textovým dokumentem; tabulkové kalkulace, prezentace v podobě slidů, jakož i dotazníkové formuláře si zaslouží popis v dalších dílech tohoto seriálu. Dále popisované vlastnosti, možnosti týmové práce, publikování atd. pro ně platí také.

3 Editace textů

Pro editaci textů je k dispozici běžná paleta formátovacích operací zahrnujících vizuální stylování (nadpisy, zvýraznění, volba velikostí a řezu písma, jakož i fontu), běžné operace s textem (vyjmutí, kopie, vrácení operace), vkládání obrázků a tvorba jednoduchých tabulek. Ovládání se děje buď to běžnými klávesovými zkratkami (např. CTRL-X pro vyříznutí, CTRL-B pro volbu tučného písma atd.) nebo výběrem myší z nabídek. Při práci občas zbytečně zabírají místo nabídkové lišty prohlížeče i samotných GDocs; obou se zbavíme příslušnými klávesovými povely nebo výběrem z menu a dosáhneme tak stavu, kdy obrazovku pokrývá skutečně jen editovaný dokument.

4 Formátovací omezení

Možnosti úpravy vizuálního stylu jsou do značné míry omezené a víceméně vycházejí z formátování HTML dokumentů, čemuž odpovídá např. repertoár stylů písma, odstavce (např. nadpisy



Obrázek 1: Formátování dokumentu

H1...H6, styl odstavce P) a tvorba tabulek. Chudoba formátovacích možností se negativně projeví i při importu z běžných desktopových editorů disponujících bohatými vizuálními prvky – vložené obrázky, složité tabulky a především jejich přesné rozmístění na stránku, které s výjimkou vynuceného zalomení stránky nedokážeme snadno zajistit. Jsme-li ovšem odborníci na webovou tvorbu, máme výsledný styl v rukou daleko pevněji; GDocs umožňují přímou úpravu HTML a CSS kódu dokumentu. GDocs ale i tak zůstávají především aplikací k pořízení obsahu, který je např. pro kvalitní tisk třeba doformátovat jinde, mimo webové prostředí, nebo aspoň použít export do PDF a tento tisknout. Pokud má ovšem výsledek skončit na webu k běžnému prohlížení nebo publikování do blogu, možnosti plně postačí. GDocs sídlí na webu, je proto přirozené, že při práci nad dokumentem máme přístup k dalším webovým službám, jako je vyhledávání slov v encyklopediích, kontrola pravopisu, slovník synonym a dokonce překladač do jiných jazyků, viz obr. 1.

Tisk z GDocs je trochu těžkopádný – z dokumentu se podle nastavení vzhledu stránky vygeneruje PDF, které je připraveno ke stažení na náš počítač a následnému vytištění.

5 Týmová práce

Sdílení dokumentů a skutečně souběžná práce více uživatelů na jednom dokumentu jsou vůbec nejpádnějším argumentem pro použití webo-

vých aplikací podobného typu. Možnosti GDocs jsou v těchto směrech široké – jeden uživatel dokument vytvoří a může ho nasdílet ostatním vyjmenovaným členům týmu, pokud tito mají účet na službách Google. GDocs si při sdílení dokážou ověřit, že zadaný účet skutečně existuje a že nejde o překlep. Je dokonce možné předat vlastnictví, tj. plnou kontrolu nad určitým dokumentem. Pozor: není pravda, že kolegové, s nimiž sdílíme, musejí mít e-mailovou adresu *jmeno*`@gmail.com` – Google dovoluje registrovat i uživatele nepoužívajícího GMail. Společná práce např. nad jedním textem může být skutečně souběžná; dokument může být otevřen a editován více lidmi současně a změny se dynamicky promítají do pohledu všech současně pracujících.

6 Správa revizí

Samozřejmostí je i správa verzí (revizí), tzn. lze si dřívější revize v poměrně zdařilém barevném zvýraznění prohlížet nebo se k nim vrátit a pozdější změny zrušit („undo"). Vizuální správa změn staví GDocs nad použití nízkoúrovňových prostředků správy verzí, jako je např. CVS nebo Subversion, které jsou bez nadstavby – např. v editoru zdrojových kódů, který změny vizualizuje sám – zcela závislé na ručně zadávaných metadatech (slovních popisech změn) a nejsou tedy praktické ani pro běžné texty, natož třeba tabulky typu Excel. Lze vytvořit i kopii dokumentu a vývoj dokumentu větvit; kopie se však sama nezařadí do stejné složky/složek jako originál ani nepřevezme práva sdílení.

7 Vazba na GMail

Google Docs je možné bez potíží používat samostatně, specifické výhody však přináší jejich integrace a souběžné využívání spolu s dalším službami, jmenovitě zmíněným GMail a *vyhledáváním*. Integrace dovoluje snadné převzetí dokumentu došlého jako příloha do schránky u GMail v podporovaném formátu (MS Word vč. `.docx`, MS Excel, RTF, OpenDocument Format, StarOffice, MS PowerPoint, PDF, HTML a čistý text) přímo do úložiště GDocs a jeho otevření pro editaci[1] v tomto prostředí. Důvodů je několik: Google si je vědom toho, že oběh dokumentů založený na neustálém připojování příloh k e-mailům a ručním řízení verzí je nejen nepohodlný, náročný na správu a náchylný k chybám, ale také citelně zahlcuje schránky uživatelů vč. těch na serverech Google.

Uživatelé komerčních služeb *Google Apps* mohou připojovat dokumenty z GDocs i k položkám kalendáře *Google Calendar*, což umožňuje efektně zpřístupnit třeba podklady a prezentace k plánované schůzce.

8 Zveřejnění a prezentace

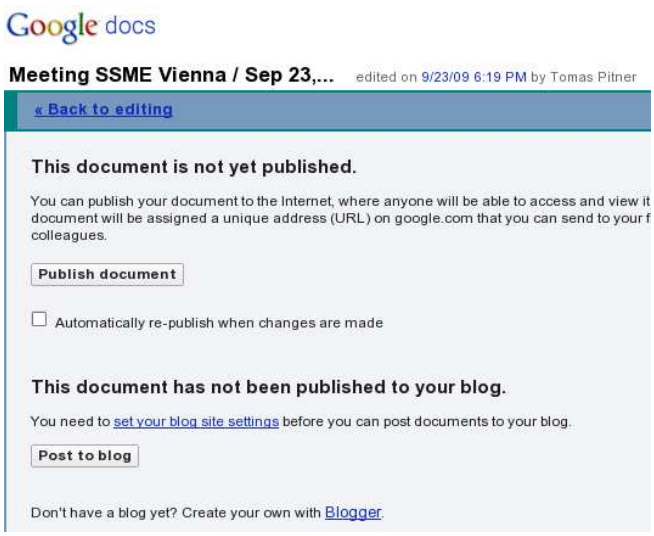
Šikovnou vlastností je možnost rychlého publikování výsledného dokumentu na webu nebo na blogu. Při zveřejnění na webu dokument jednoduše dostane URL, pod kterým bude vidět odkudkoli ze světa, aniž bychom jej museli ručně vkládat do vlastního webového prostoru nebo systému správy dokumentů, viz obr. 2. Podobně triviální je i vložení dokumentu jako záznamu do blogu (webového zápisníku) založeného na další službě Google Blogger, `http://www.blogger.com`. Pro prezentace („slidy") je zde specifická možnost je přímo rychle promítnout z prostředí GDocs, zobrazené na plnou plochu obrazovky stejně, jako by to dokázal např. PowerPoint.

Řada uživatelů Google, vč. autora tohoto článku, využívá k webové prezentaci službu *Google Sites*, která si jako taková zaslouží podrobnější komentář někdy příště. Zde pouze zmiňme, že do webové stránky na Sites je možné několika kliknutími přímo vložit dokument napsaný v GDocs, přičemž originál lze i nadále editovat a změny se po znovunačtení promítnou do webové stránky na Sites. Výsledek je velice působivý a při omezených nárocích nahradí i rozsáhlé systémy správy dokumentů.

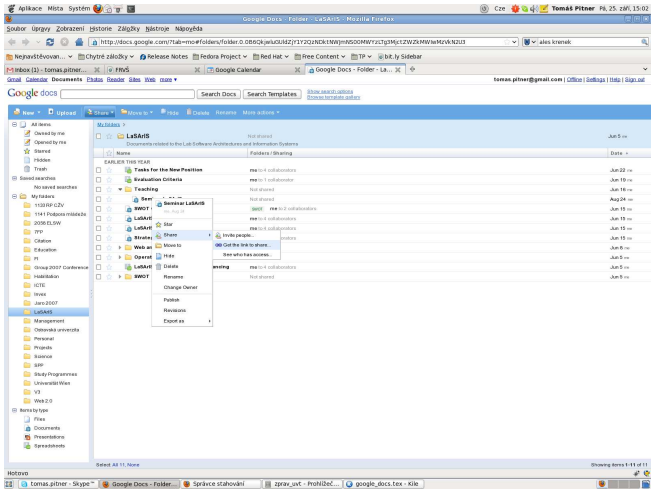
9 Organizace dokumentů

Přestože koncepce organizace dokumentů v úložišti Docs je relativně letitá a používaná od počátku v téměř nezměněné podobě, v určitých prvcích konkurenci stále převyšuje. Netypická je zejména možnost zařazovat – podobně jako v unixovém systému souborů – jeden soubor do

[1] Výjimkou jsou PDF soubory, které se uloží a lze je pak i bez Acrobat Readeru prohlížet či sdílet, ale ne editovat.

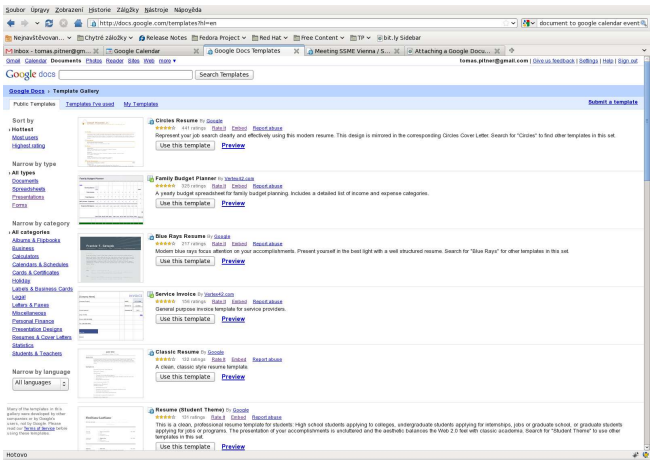


Obrázek 2: Publikování na web a do blogu



Obrázek 3: Organizace do složek

více složek, které mohou být hierarchicky vnořené. Tato představa je sice na počítačích přirozená, v aplikacích Webu 2.0 bývá však většinou nahrazená tzv. *štítkováním* (tagging, labelling). Jeden zdroj (dokument, odkaz, obrázek,...) může mít v aplikacích přiřazen jeden či více štítků, což jsou podle možností příslušného systému slova nebo slovní spojení charakterizující daný zdroj. Takto konstruované štítky ale nenahrazují hierarchické systémy souborů, protože mezi štítky jako takovými nemůžeme vnoření (hierarchie) definovat. Google Docs vlastnosti obou kombinuje: složky hierarchické jsou, a přesto lze mít jeden dokument ve více z nich, viz obr. 3.



Obrázek 4: Komunitou vytvořené šablony dokumentů

Nevýhodou systému složek GDocs je nezávislost na štítcích (label) aplikace GMail: není tedy možné mít společnou složku na poštu i dokumenty. Rovněž vyhledávání ve vlastních zprávách, dokumentech či událostech kalendáře je dosud oddělené a není možné jedním dotazem hledat v mailech, textech a popisech událostí.

10 Šablony

V základních instalacích balíků typu „office" – a to jak komerčních tak volných – zpravidla nemáme, pokud jde o předpřipravené vizuální styly dokumentů, mnoho na výběr. GDocs naproti tomu nabízejí rozsáhlou paletu komunitou vytvářených šablon (template) pro texty, tabulky, prezentace i dotazníkové formuláře, viz obr. 4.

11 Problémy

Stejně jako jiné podobné aplikace, jsou i GDocs choulostivé na kvalitu internetového připojení a při nedostatečné rychlosti či pomalé odezvě jsou nepoužitelné. Rovněž samotná výpočetní infrastruktura Google, tj. mohutný cluster komoditních počítačů s unikátním middlewarem, sice dostačuje službám, kde je akceptovatelný i neúplný výsledek (např. při vyhledávání se nenajde všechno a s tím, co se najde, „jsme v podstatě spokojeni"), ale jako podnikové kolaborativní prostředí vyhovovat nemusí – podobně jako GMail s jeho občasnými několikahodinovými výpadky.

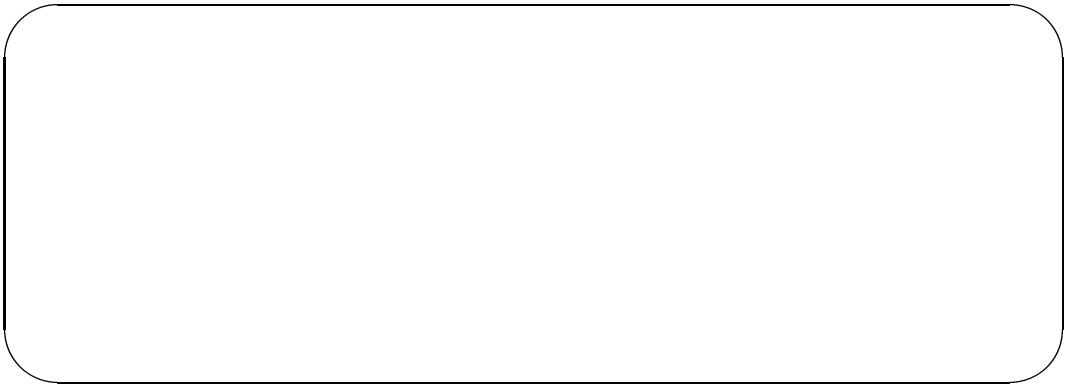
12 Praktické zkušenosti

Díky rostoucím možnostem se Google Docs a podobné aplikace stávají schůdnou alternativou k desktopovým editorům textu, tabulek a prezentací tam, kde to dovoluje rychlost internetového připojení i PC a kde se obejdeme bez pokročilejší práce s grafikou, vkládání objektů apod. Malý výřez funkcionality je v současnosti reálně dostupný i prostřednictvím mobilního zařízení – např. nahlédnutí do textového dokumentu bez editace není problémem ani v tak minimalistickém prostředí, jaké nabízí javový prohlížeč Opera Mini běžící dnes téměř na jakémkoli mobilním zařízení. Velmi se hodí pro práci na dynamicky se vyvíjejích pracovních verzích, kde přesná vizuální podoba není podstatná. V pozdějších fázích bývá lepší dokument stáhnout a vizuální úpravy provádět v plnohodnotné desktopové aplikaci.

Praktická zkušenost však ukazuje, že poté na GDocs málokdy najdeme finální verzi takto zpracovávaného dokumentu – ta jednoduše zůstane v systému souborů posledního autora, příp. po odeslání v elektronické poště, a do GDocs ji už nikdo nevystaví. Má to i praktické důvody – zpětný převod z finálního formátu (typicky MS Word) do dokumentů Google není bezeztrátový. GDocs tedy nelze použít jako archív, není to funkční ekvivalent sdíleného systému souborů. Naproti tomu jsou GDocs ideální pro operativní práci s dokumenty, které primárně pocházejí z různých „světů". Zbaví nás starostí s různými platformami, kódování textů, formáty dokumentů atp. Užitečnou vlastností je podpora PDF (import/export), která je jinak např. v MS Office možná pouze s placeným rozšiřujícím modulem produktu Adobe Acrobat.

GDocs se reálně osvědčily v prostředí heterogenních a distribuovaných týmů majících přístup k internetu, přičemž stačí i rozumné WiFi připojení a středně výkonný netbook. Vyhneme se starostem s údržbou datového úložiště dokumentů i se synchronizací dokumentů pořízených někde na notebooku během cest do centrálního systému souborů. □

Obsah



Editor: Miroslav Bartošek • Vydavatel: Masarykova univerzita • Žerotínovo náměstí 9, 601 77 Brno, CZ
tel.: 549 492 100 • e-mail: zpravodaj@muni.cz • WWW: http://www.ics.muni.cz/zpravodaj/
Sazba systémem LaTeX 2ε písmem LucidaBright • Tisk: Tribun EU s. r. o. • *Neprodejné* • ISSN: 1212–0901