Co dělat po PRISM?

Honza Šípek

17. července 2013

Před měsícem prozradil whistleblower Edward Snowden veřejnosti existenci amerického systému Prism. Americká vojenská tajná služba NSA nejen že se snaží odposlouchávat a uchovávat veškerou internetovou a telefonní komunikaci, ale podle Snowdena jí naše data poskytují přímo velké IT společnosti, miláčkové Silicon Valley, mezi nimiž nechybí Microsoft, Yahoo!, Google, Apple, Skype ani Facebook.

Dotčené společnosti nejprve jakoukoliv spolupráci vyvrátily a zdálo se, že se obvinění nepodaří prokázat. [1] Když ale systém začal obhajovat i prezident Obama [2], ve Velké Británii byl odhalen spolupracující sledovací systém Tempora [3] a opozice se začala ptát, proč výzvědné systémy míří proti vlastním občanům, začalo být pravděpodobné, že systém Prism skutečně existuje. K čemu získaná data tajným službám mohou být? A jaká se proti masivnímu sledování formuje obrana?

K čemu PRISM může být?

Sociální síť Facebook by byla pokladem pro sociology. Její uživatelé zcela dobrovolně a mimoděk mapují a zaznamenávají svoje každodenní životy. Popisují velmi detailně sociální síť, v níž se pohybují. Víme přesně, kdo jsou jejich přátelé, kdo jsou jejich příbuzní, koho ignorují, s kým by se radši neviděli, s kým soukromě komunikují mimo dohled „zdí“ a co si píšou. Síť také ví, kdo jsou sociometrické hvězdy, „opinion leadeři“, zkrátka aktivní lidé s velkým potenciálem hýbat společností. A nikdy nebylo pochyb o tom, že tajné služby budou o tyto data dřív nebo později stát.

Vzpomeňme si na nyní historiky popisovanou zpravodajskou síť StB. Nohavica se nejprve hájil, že na Kryla ani Kohouta nic podstatného neřekl. [4] S kým se stýká? O čem se baví? Co ho trápí? Co má rád? Co je jeho slabůstka? Zdánlivě nepodstatné informace měly za cíl profilovat „zájmové osoby“ a najít způsob, jak na ně. Dobová mašinérie musela získané informace pracně zpracovávat na psacích strojích s průklepovým papírem, zavést důsledný kartotéční a archivní systém a udržovat a platit rozsáhlou síť agentů. Na podobné masové zpracování sociálních sítí za pomoci počítačů se psaly diplomky už před deseti lety a Facebook sběr podobných dat provádí v globálním měřítku.

Nedávno se na Facebooku vyskytla chyba, která některým uživatelům dala přístup k jejich „stínovým profilům“. Přišlo se na to, že kromě obyčejného profilu Facebook uchovává profil další, s informacemi, o nichž ani nevíme, že je má. Byly to například adresy a telefonní čísla z adresářů či emailových schránek, která si od nás Facebook vycucl při „hledání přátel“. [5]

Twitter, další sociální síť, která se zaměřuje pouze na rychlé a virální šíření informací, je ideálním prostředkem pro „sentiment analýzu“ a „detekci vynořujících se zpráv“. [6] To, co se dříve projevovalo jako „drb“, případně žhavá novinka, která šla od ucha k uchu, nebo jako „dobrá pověst“, je nyní dokonale zmapovaným jevem. U zprávy, která se sítí šíří, je jednoduché detekovat, u koho se zrodila, kdo byli její šiřitelé a jaké lidi zaujala. Příkladem je Arabské jaro, facilitované a eskalované právě Twitterem, u nějž je možné analyzovat všechny aktéry a průběh revoluce. V pesimističtější variantě pak takové revoluce moderovat. [7]

Největším jackpotem je ovšem Google. Má v držení nejen soukromou korespondenci několika desítek milionů osob i organizací (mimo jiné i několik verzí tohoto textu dávno předtím, než vyšel, neboť strana redakce používala Gmail), ale i dotazy do vyhledávače z celého světa, zaměřené s přesností na jeden počítač. Dále informace o tom, kdo prohlížel jaké stránky (na stránkách, které nemá pod kontrolou, používá svoje Google Analytics a reklamní systém AdSense). Navíc provozuje úložiště, cloud, do nějž uživatelé nahrávají („zálohují“) „neveřejná“ data ze svých počítačů a může tak do nich nahlížet a vyhledávat v nich. K tomu má pod kontrolou mobilní telefony s operačním systémem Android.

Česká policie si stěžuje na problémy s omezenou možností odposlechu telefonů, zvlášť když se telefonní hovory čím dál častěji uskutečňují přes Internet. Je logické chtít mít k těmto datům přístup. Skype, nyní patřící Microsoftu je logickým cílem. Aplikace běžící na počítači, které jsme přidělili volný přístup k vestavěnému mikrofonu a kameře a která beztak neustále komunikuje se světem, je bezpečnostní riziko, které popisoval už Orwell. Orwellovská Obrazovka nás ale chytře nepoučuje o ideologii, nenutí nám obsah, který nechceme, jen si tiše vrní na pozadí, jako by tu ani nebyla.

Kontrola nad mobilními operačními systémy by mohla být i důvodem spolupráce s Applem. iPhone, marketingový miláček 21. století, se zabydlel v kapsách 250 miliónů lidí po celém světě. [8] Kromě běžných telefonních dat, jaká známe z klasických odposlechů, přes něj proudí i provoz Internetu a zhusta též sociálních sítí, dále poskytuje informace o své přesné poloze za pomoci systému GPS. Co přesně iPhone sděluje a komu není jasné, protože operační systém je uzavřený a tedy nepodléhá veřejné kontrole. Průšvihů, při nichž se zjistilo, že iPhone říká více, než by měl, bylo několik. Například v dubnu 2011 se zjistilo, že iPhone neustále zaznamenal svoji polohu a dvakrát denně data odesílal mateřské firmě. [8] Apple provozuje též cloud pro uživatele svých počítačů, iCloud, který se nabízí k aktivaci hned po instalaci operačního systému MacOS X i iOS.

Snowden a před ním

Snowden však není první, kdo o masivním sledování ze strany NSA promluvil.

Už loni v březnu popsal americký časopis Wired ohromné datové centrum NSA, budované v Bluffdale v Utahu. Celé věže serverů mají běžet na 2323 čtverečních metrech. Kapacita je odhadovaná v řádech zettabytů [17] nebo dokonce yottabytů [10]. Jsou to jednotky, které zatím příliš neslýcháme. Zettabyte je tisíc exabytů, tedy milión terabytů. Yottabyte je ještě tisíckrát tolik. Pro srovnání: loňský provoz celého Internetu je odhadován na 528 exabytů [13][12], na rok 2015 se předpokládá 966 exabytů ročně. [11] Už jen plánovaná spotřeba elektřiny výpočetního supercentra je 65 megawattů, tedy pro srovnání více než polovina výkonu elektrárny Hodonín. Dokončení areálu je údajně plánováno na letošní září. [10]

Další výpočetní centrum (s trafostanicí projektovanou na 150 MW) má stát ve Fort Meade, sídle NSA, svá centra vybudovali i subdodavatelé armády jako *General Dynamics* či *Boeing*. Firma *Booz Allen Hamilton*, která zaměstnávala právě Snowdena, měla podle časopisu Wired obstarávat propojení právě mezi těmito výpočetními centry. Dalším ze subdodavatelů má být firma *Endgame Systems*, která se snaží udržovat celosvětovou databázi všech zařízení připojených k Internetu včetně jejich fyzického umístění, běžícího softwaru a seznamu potenciálních bezpečnostních děr. [15]

Bývalí zaměstnanci NSA, William Binney, Thomas Drake a J. Kirk Wiebe na podezřelé praktiky upozornili už v roce 2002. [18] Kryptograf Binney paradoxně vystoupil hlavně proto, že systém dodávaný do NSA považoval za předražený, odfláknutý a tedy i korupční. Drake proto, že systém, který měl sledovat „zahraniční cíle“, protiústavně sledoval občany vlastního státu. Všichni tři měli vážné problémy, byli zadrženi, stanuli před soudem (Drake dokonce za špionáž), nakonec našli zastání u organizace na podporu whistleblowerů a nakonec byli očištěni. [17] Rozdíl oproti Snowdenovi je v tom, že se na média obrátili až v okamžiku, kdy vyčerpali všechny možnosti domoci se nápravy u svých nadřízených. Přesto jim světová média věnovala minimální pozornost a ve srovnání s ohlasem, kterého se dostalo Snowdenovi (například Česká televize zmínila Drakea teprve před několika dny [16] v „exkluzivním rozhovoru“), považují sami sebe za neúspěšné. [18] Způsob, jakým NSA odposlouchává internetový provoz, popsali Drake a Binney například loni v prosinci na hackerské konferenci 29c3 v Berlíně. [17] Masivní odposlech komunikace tedy není nic nového (například systém Echelon vybudovaly Spojené státy a jejich spojenci již během studené války), Snowden však poprvé promluvil o tom, že v této hře spolupracují s tajnými službami i internetové a telekomunikační firmy.

Celý cirkus kolem „disidenta Snowdena“, datacentra popsaná „zdroji“ Wiredu i vystoupení předchozích whistleblowerů můžou být samozřejmě zpravodajskou hrou. Logická je ale touha mocných po kontrole nad elektronickými komunikacemi, a bylo by s podivem, kdyby neprobíhala. Navíc, recepty, jak se sledování bránit, můžou mít příjemné vedlejší účinky: kromě

ochrany před běžným špiclováním ze strany konkurence nebo policie, větší odolnosti proti spywaru a virům, to je i větší decentralizace informací. A ta se může hodit i v případě průšvihu jiného druhu, třeba masivního blackoutu nebo kybernetického útoku.

Obrana

Po odhalení projektu PRISM se česká média věnovala hlavně bizarnímu příběhu „viníka úniku“. Internet i odborná společnost mezitím začaly hledat nápady, jak se vyhnout sledování. Český technologický blogger „Franta“ již loni popsal svoje zkušenosti s experimentem „Týden bez Googlu“. *„Nejde primárně o to, zda je Google ‚hodný‘ nebo ‚zlý‘ – problém vidím už v tom, že se příliš mnoho moci koncentruje v rukou jednoho subjektu (který, i kdyby byl sám o sobě desektrát svatý, může být ovládnut někým zlým). Internet by měl být podle mého co nejvíce decentralizovaný a systémy by měly fungovat co nejvíc autonomně a nezávisle na svém okolí,*“ popisuje svoji motivaci. [9] Experiment, který si málokdo z nás dovede představit (už při psaní tohoto textu autor vyslal Googlu několik desítek dotazů), dopadl konstatováním „přežil jsem to v pohodě“ a radami, jak se službám Googlu vyhnout. [19]

S nápady na decentralizovanější využívání Internetu přišla i Nadace elektronického pohraničí (EFF). Na jednoduché a přehledné stránce PrismBreak.org zveřejnila možné náhrady za produkty ohrožené sledováním nebo se na sledování podílejícím. Windows a MacOS – které s „domovskou stájí“ Microsoft nebo Apple komunikují hned po instalaci – navrhuje nahradit Linuxem. Telefonní operační systém Android plně otevřeným Replicantem, a iOS používaný na iPhonu radí zcela nepoužívat. K populárním sociálním sítím, které „v tom jedou s NSA“ nabízí deset otevřených alternativ. [21]

K seznamu by asi mělo přibýt ještě „stahovací servery“ –> bittorent. Zatímco úložiště typu ukládej.to patří obvykle jedné firmě a jsou provozovány z jedné centrální lokality, kterou je snadno blokovat či cenzurovat, BitTorrent, protokol pro sdílení souborů mezi uživateli samotnými, nepotřebuje žádné centrální úložiště. Uživatelé si kousky souborů vyměňují libovolně, automatizovaně a hlavně přímo sami mezi sebou.

Tento systém sdílení je velmi obtížné cenzurovat. Zranitelné jsou ale „organizační“ tracker servery, a spor o službu The Pirate Bay *(Pirátská zátoka)* hýbal švédskými soudy tři roky [20]. Existují i vartianty zcela decentralizované, které je lepší preferovat. Není však nutné uživatelům nic nařizovat ani doporučovat. Stačí tlak zvenčí. A krátce poté, co z populárního portálu Ulož.to zmizely některá videa (patrně z důvodu porušení autorských práv [23]), objevily se tamtéž jejich odkazy na torrent. Anonymita sdílení informací na BitTorrentu však zatím není uspokojivě vyřešena a pro skutečně anonymní sdílení nabízejí znalci síť FreeNet.

Hypermarket a místní zelinář

Obecně by se obrana proti PRISM dala přirovnat ke konsumeristickému hnutí. Po vpádu hypermarketů na lokální trhy se stalo moderním ba módním – ale ještě více snad zodpovědným – nakupovat zeleninu od místních zemědělců a při nákupu v obchodě se podívat, odkud zboží pochází.

Stejně tak první recept proti masivnímu sledování je vyhnout se firmám, které se na něm podílejí. Hledat alternativy za Google, Facebook, Twitter a používat něco jiného. Pít něco jiného než kokakolu a jíst něco jiného než McTlouštík. Neukládat si nic do cloudu. Zvážit, které služby Internetu používám denodenně a kdo za nimi stojí. Dále zjistit, kde všude tyto korporace mají chapadla a vědět o tom, že jejich trasovací značky se nacházejí téměř v každé webové stránce. Nainstalovat si do internetového prohlížeče doplňky, které toto sledování blokují (např. *AdBlock, Random userAgent, HTTPS Everywhere, Flash Block, NoScript* pro Firefox). Vedlejším efektem je výrazné omezení reklam.

Pokročilejší nebo paranoidnější se mohou pokusit vyštvat korporace ze svého osobního počítače. Nainstalovat firewall a bránit všem připojením tam, kam nechceme, například k „serverům ověřování pravosti software“ či dokonce k celé doméně facebook.com.

Ještě pokročilejší si patrně nainstalují některou z variant Linuxu – k uživatelské přívětivosti se za poslední roky udělaly velké kroky a systém se u nás začíná s úspěchem používat i na základních školách. Učitelé hlásí, že žáci nemají s použitím Linuxu problém. [22] A člověk nežije se stigmatem toho, že „ukradl“ operační systém. Software, který má otevřené zdrojové kódy, je navíc něco jako když stát zveřejňuje všechny uzavírané smlouvy nebo příjmy poslanců – je zkrátka pod veřejnou kontrolou a kdo chce, může překontrolovat, co vlastně s jeho počítačem provádí. Oproti tomu uzavřené operační systémy jsou jako firmy anonymních akcionářů, které dostávají tučné zakázky od státu, s odvoláním na obchodní tajemství nezveřejňují detaily a říkají „všechno je v pořádku, nám můžete věřit“.

Nejpokročilejší uživatelé zašifrují své pevné disky a povedou všechnu komunikaci dovnitř i ven šifrovanými kanály. Použijí anonymizační služby jako Tor nebo VPN (na Slovensku už byl – zatím neúspěšně – navržen zákon, který použití anonymizačních služeb zakazuje [14]), platit budou Bitcoinem a budou provozovat vlastní nezávislé servery, jimž budou vládnout jenom oni. Tyto servery budou skrývat svoji identitu, jejich vzájemná komunikace bude šifrovaná. Server může být i notebook ve spíži. Má malou spotřebu a nechcípne, když vypnou elektriku. Je totiž důležité si uvědomit, že zatímco paranoidně a krypticky šifrujeme komunikaci, koncové body zůstávají často velmi zranitelné. Osobní počítač s nainstalovanými Windows, děravý jak řešeto, nebo pošta v nešifrované podobě na serverech Gmailu, kam si „služby“ sáhnou pro jakákoliv data.

A jestli ten hangár plný počítačů, který si NSA postavila [10], není ohromný cluster na dešifrování, budou alespoň trošku v bezpečí. NSA ovšem mnohé šifrovací algoritmy sama navrhla a je největším zaměstna-

vatelem matematiků v USA. [15] Existují však stále ještě algoritmy, které jsou považovány za bezpečné. Nejsou to rozhodně všechny a jak řekl Thomas Drake: „Nepoužíval bych šifrování, na němž je razítko státu.“ [17]

Hackeři mezi tím vyvinou technologie umožňující další skrývání. Veřejnost je otestuje, projdou evolucí a buď se ujmou, nebo zaniknou. Už teď geekové pořádají CryptoParty, ŠifroMejdany, něco na způsob workshopů, které mají běžné uživatele naučit práci se šifrováním a anonymizací. Každý měsíc se koná Cryptoparty v pražském klubu Cross, v půli července proběhne první v bratislavském hackerspacu ProgressBar [27] a další v Brně. V pozadí se už dvacet let rozvíjí hnutí CypherPunk, které proti systému nebojuje propíchutým obočím, ale šifrováním. [26] Rychlé šíření zpráv o ohrožení soukromí i nápady, jak se proti němu bránit, zajišťuje mailinglist Cypherpunk na ironicky pojmenovaném serveru al-qaeda.net. [25]

Umění války

Reakcí na útok je snaha o hledání obrany. Reakcí na šmírování skrze okno je vznik záclon. Reakcí na možnost odposlechu je vývoj šifrování. Reakcí na zákaz šíření informace je samizdat.

Je otázkou, jestli po „informační revoluci“ nevstupujeme do fáze informační normalizace.

Jak říká mistr Sun:

> „Odhalíš-li rozmístění a záměry nepřítele, sám však pro něj zůstaneš neviditelný, tvé síly se mohou spojit, zatímco jeho budou roztříštěné.“
>
> [24, s. 40]

Reference

[1] Glenn Greenwald, Ewen MacAskill: *NSA Prism program taps in to user data of Apple, Google and others*. The Guardian, 7. 6. 2013. Elektronicky, `http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data`, získáno 3. 7. 2013.

[2] Lucy Madison: *Obama defends "narrow" surveillance programs*. CBS News, 19. 6. 2013. Elektronicky, `http://www.cbsnews.com/8301-250_162-57590025/obama-defends-narrow-surveillance-programs/`, získáno 3. 7. 2013.

[3] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, James Ball: *Mastering the internet: how GCHQ set out to spy on the world wide web*. The Guardian, 21. 6. 2013. Elektronicky, `http://www.guardian.co.uk/uk/2013/jun/21/gchq-mastering-the-internet`, získáno 3. 7. 2013.

[4] Jaroslav Spurný: *Tajemství Jaromíra Nohavici*. In: Respekt, 28. 5. 2006. Elektronicky, http://respekt.ihned.cz/c1-36265420-tajemstvi-jaromira-nohavici a http://www.hutka.cz/new/html/nohavica2.html.

[5] Violet Blue: *Anger mounts after Facebook's 'shadow profiles' leak in bug*. ZDnet.com, 23. 6. 2013. Elektronicky, http://www.zdnet.com/anger-mounts-after-facebooks-shadow-profiles-leak-in-bug-7000017167/, získáno 3. 7. 2013.

[6] Patrick Zandl: *František Vrabel: Newstin šel od vojenských technologií ke zpravodajství*. Lupa.cz, 20. 2. 2009. Elektronicky, http://www.lupa.cz/clanky/frantisek-vrabel-newstin-vojenske-zpravodajstvi/, získáno 2. 7. 2013.

[7] (autor neuveden): *Nebezpečí měřitelnosti sociálních médií*. Jeden Bod. Elektronicky, http://jedenbod.cz/1234-nebezpeci-meritelnosti-socialnich-medii.html, získáno 3. 7. 2013

[8] Wikipedia: *iPhone*. Elektronicky, https://en.wikipedia.org/wiki/Iphone. Citováno 30. 6. 2013.

[9] xkucf: *Týden bez Googlu*. ABClinuxu.cz, 29. 9. 2012, elektronicky, https://www.abclinuxu.cz/blog/xkucf03/2012/9/tyden-bez-googlu, získáno 30. 6. 2013.

[10] James Bamford: *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*. Wired, 15. 3. 2013. Elektronicky, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1, získáno 19. 4. 2012.

[11] Wikipedia: *Exabyte*. Elektronicky, https://en.wikipedia.org/wiki/Exabyte, získáno 1. 7. 2013.

[12] Wikipedia: *Internet traffic*. Elektronicky, https://en.wikipedia.org/wiki/Internet_traffic, získáno 1. 7. 2013.

[13] Cisco: *The Zettabyte Era—Trends and Analysis*. Cisco, 29. 5. 2013. Elektronicky, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/VNI_Hyperconnectivity_WP.pdf, získáno 12. 7. 2013.

[14] Rastislav Guľaša: *Ministerstvo vnútra navrhuje zakázať používanie anonymizérov a uchovávať údaje používateľov verejných internetových fór*. Inet.sk, 20. 10. 2009. Elektronicky, http://archiv.inet.sk/8135-8135ministerstvo-vnutra-navrhuje-zakazat-pouzivanie-anonymizerov-a-ucho
html, získáno 4. 7. 2013.

[15] James Bamford: *NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us Into Cyberwar*. Wired, 12. 6. 2013. Elektronicky, http://www.wired.com/threatlevel/2013/06/general-keith-alexander-cyberwar/all/, získáno 2. 7. 2013.

[16] luk: *Snowdenův předchůdce pro ČT: Špehování ohrožuje celou společnost.* ČT24, 20. 6. 2013. Elektronicky, http://www.ceskatelevize.cz/ct24/svet/232081-snowdenuv-predchudce-pro-ct-spehovani-ohrozuje-celou-spolecnost/, získáno 1. 7. 2013.

[17] Jesselyn Radack, Thomas Drake, William Binney: *Enemies of the State: What Happens When Telling the Truth about Secret US Government Power Becomes a Crime.* Chaos Communication Congress 2012 (29C3), 27. 12. 2012. Elektronicky, http://events.ccc.de/congress/2012/Fahrplan/events/5338.en.html a http://media.ccc.de/browse/congress/2012/29c3-5338-en-enemies_of_the_state_h264.html (video).

[18] Peter Eisler and Susan Page: *3 NSA veterans speak out on whistleblower: We told you so.* USA Today, 16. 6. 2013. Elektronicky, http://www.usatoday.com/story/news/politics/2013/06/16/snowden-whistleblower-nsa-officials-roundtable/2428809/, získáno 6. 7. 2013.

[19] Franta: *Týden bez Googlu – vyhodnocení*. Kinderporno.cz, 7. 10. 2012. Elektronicky, http://kinderporno.cz/d/node/868, získáno 30. 6. 2013.

[20] Wikipedia: *The Pirate Bay Trial*. Elektronicky, https://en.wikipedia.org/wiki/The_Pirate_Bay_trial. Citováno 30. 6. 2013.

[21] Electronic Frontier Foundation: *Opt out of PRISM, the NSA's global data surveillance program*. Prism-break.org, elektronicky, http://prism-break.org/. Citováno 29. 6. 2013.

[22] Jaroslav Krejčí: *Devět let Linuxu na přerovské základní škole.* LinuxExpres, 27. 10. 2012. Elektronicky, http://www.linuxexpres.cz/business/devet-let-linuxu-na-prerovske-zakladni-skole, získáno 1. 7. 2013.

[23] Martin Vyleťal: *Jiří Srstka (Dilia): Uložto.cz nám jednostranně vypovědělo smlouvu.* Lupa.cz, 14. 5. 2013. Elektronicky, http://www.lupa.cz/clanky/jiri-srstka-dilia-ulozto-cz-nam-jednostranne-vypovedelo-smlouvu/, citováno 30. 6. 2013.

[24] Sun-c': *Umění války*. Přeložil Radim Pekárek. B4U Publishing, Brno, 2008.

[25] *Cypherpunks Mailing List Information*. al-Qaeda.net, 5. 1. 2011. Elektronicky, http://www.al-qaeda.net/cpunk/, získáno 1. 7. 2013.

[26] Jakub Mikuláš: *Cypherpunkeři: Stav diskuze a prostředků digitální kryptografie.* Masarykova universita, Brno, 2011. Elektronicky, http://jedenbod.cz/1262-cypherpunkeri-stav-diskuze-a-prostredku-digitalni-kryptografie.html a http://jedenbod.cz/wp-content/uploads/2011/12/Crypto.pdf, získáno 3. 7. 2013

[27] ProgressBar: *Cryptoparty: Prism edition*. Elektronicky, https://progressbar.sk/calendar/cryptoparty-prism-edition.