Věda a technika stojící za ztrátou soukromí

J. Vávra
Fakulta jaderná a fyzikálně inženýrská, ČVUT, Břehová 7, 11519 Praha 1
jiri_vavra@centrum.cz

Abstrakt

Cílem je představit technické prostředky, které jsou k využívány ke špehování lidí – jak pro to speciálně vytvořené, tak ty, které mohou být zneužity.

1 Úvod

„The man who trades freedom for security does not deserve nor will he ever receive either.“ ("Ti, kdo se vzdají základních svobod, aby byli na přechodnou dobu v bezpečí, si nezaslouží ani svobodu, ani bezpečnost.")

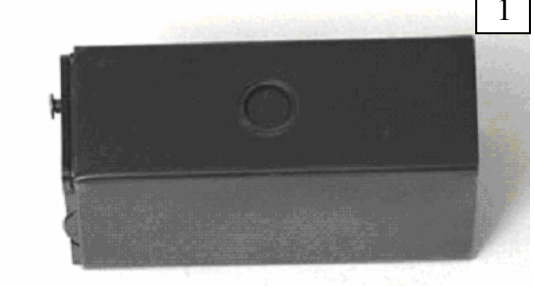
Benjamin Franklin

Tento článek bude lehce paranoidní, ale ne bezúčelně. Každý měsíc přichází několik zpráv ze světa, že „kvůli teroristům musíme odposlouchávat telefony/ číst emaily/ shromažďovat biometrická data/ … o vás“. A lidé přestávají tyto zprávy vnímat jako zásah do čistě soukromého prostředí se slovy „Nemám se čeho bát, já nic špatného nedělám.“

2 Historie - budoucnost

Historie není příliš bohatá, protože až od přelomu 2. a 3. tisíciletí začíná být lidstvo dostatečně technologicky na výši, že je možno pomocí počítačů analyzovat data z mnoha zdrojů a každý člověk už je si schopen nějaký prostředek na špehování sám vyrobit nebo zakoupit (zhruba od 500 Kč). Dříve se užívalo především k vojenské a průmyslové špionáži.

1



2

Obrázek 1 – Matchbox od easter kodak company, zamaskování jako krabička sirek.
Obrázek 2 – kamera Minox používaná od roku 1937 a je na 50 snímků

Jak už bylo psáno, dnes si nějakou tu „hračku“ může pořídit každý. Ty nejjednodušší se maskují jako zásuvka na elektřinu nebo na telefon a mohou tak být v provozu prakticky neomezeně a posílat informace třeba přes elektrický rozvod, takže se nedají tak lehce

vystopovat. Nejvýše v evoluci stojí asi ornitoptéra vážící 2g schopná posílat obraz i zvuk do vzdálenosti 2km.

Mobilní telefony

Telefon vám může odposlouchávat nejen policie. Při HW a SW úpravě se dá nastavit tak, že pokud na něj zavoláte, automaticky se zvedne (i když na sobě nedá nic najevo) a můžete poslouchat jeho okolí. Starší analogové telefony měly nekódované vysílání a pracovali kolem 450MHz, takže se dali poslouchat rádiem (některé z tržnic to opravdu zvládali). Hlavně v USA a Británii je poměrně rozšířený verilokační systém, který určuje polohu určitého telefonu. Používá se hlavně na naleznutí zaměstnanců a potomků, samozřejmě pouze za souhlasu majitele. Vystopování mobilního telefonu můžete několika metodami s přesností od 35 km do 50 m.

Biometrie (vsuvka)

Věda zkoumající charakteristické znaky buď tělesného rázu (duhovka) nebo chování (chůze, podpis). „Založil" francouzský antropolog Alphonse Bertillion. Jeho systém stojí na kombinaci měr některých částí těla. Konec přišel r.1903, kdy došlo k prvnímu zjištění dvou lidí se stejnými mírami. V roce 1880 Henry Faulds vydal článek o snímání otisků. Ještě lepší je snímání duhovky, kde se zkoumá přes 400 rysů a je tak 7x víc možností než u otisku. Dále se může sledovat obličej (na letiště proti teroristům), otisk prstu (už prodává Microsoft, IBM, firmy na bezpečně zámky), podpis (nesleduje se tvar, ale sklon, rychlost psaní, …). Analýza DNA je užitečná zatím pouze pro policii –v reálném čase je zatím neproveditelná.

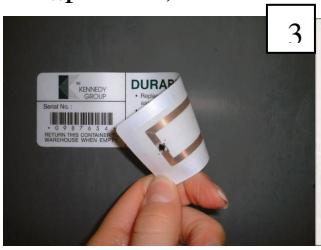
RFID (Radio Frequency Identification)

V RFID čipech je veliká budoucnost. Je to malý čip s velkou anténou – uvidíte je běžně nalepené na výrobcích v obchodě. Už se mohutně využívají a budou se využívat čím dál více. Výhodou je nízká cena, snadná instalace a „nekonečná" životnost (získávají energii z antény). Je několik druhů: jednorázové nálepky, tagy (znovupoužitelné, odepínací), PCB nosiče (do výrobků, např. palety). Největší dopad pro naše soukromí bude implantování těchto čipů do lidského těla – prvně lidem se sníženou možností obrany (zločinci, děti, nemocní – probíhá), pak dobrovolníkům (taktéž probíhá), časem možná všem povinně.

Mají zatím kapacitu od desítek bitů po desítky kilobitů a dosah od milimetrů po 2,5 metru (oficiálně. Mluví se ale o schopnosti přečíst data speciálními čtečkami do vzdálenosti desítek metrů). Pracují na různých frekvencích od 50kHz po 2,5GHz. Do pasů a bankovek jsou připraveny čipy o rozměrech 0,4×0,4×0,06 mm.

Používání: běžně už se „čipují" psi; ve výrobcích proti krádežím, u pokladen mohou být umístěny čtečky a zboží se bude automaticky načítat; v paletách pro jednodušší evidenci pohybu zboží; čipy v obalech potravin spolu s „chytrou ledničkou" nás mohou upozornit na kazící se a docházející potraviny, … Voperovaná do paže nebo připevněna na oděvu či ruce může povolovat přístupy do částí budov, sledovat pohyb dětí, nemocných.

Ale dá se také uložit otisk prstu, vzhled, podpis, výpis nemocí aj. Spolu s přístupem do databází a informací o obsahu zákazníkovy peněženky se může komukoli (kdo zaplatí nebo má „přátele") dostat do rukou mocná zbraň.



3

4

Obrázek 3 – RFID jak ho všichni známe

Obrázek 4 – tento se voperovává do těla

Satelity a GPS

Satelity jako takové nejsou na sledování příliš vhodné. Sice už mají kvalitní rozlišení (4 cm – satelit KH-13 z roku 1999), ale je jich příliš málo a jsou poněkud drahé)

Více využitelné jsou GPS čipy vysledovatelné po celém světě. Puška Id Sniper střílí tyto čipy do těla beze stop zásahu a bezbolestně (bolí méně jak štípnutí od komára). Má dostřel 1100 metrů a je vybavena kamerou aby se vědělo, kdo je novým nositelem čipu.

Senzorické bezdrátové sítě

Jsou tvořeny malými bezdrátovými přístroji, které měří fyzikální veličiny. Mají dlouhou výdrž (99% času mohou spát), nepotřebují instalaci a jsou levné.

ZigBee – vyvíjena ZigBee aliancí, která je nevýdělečná, rostoucí a založena na Open Standard. Založena od např. Samsung, Philips, Motorola, nyní má přes 100 společností. Jsou napájeny 2 AAA bateriemi, funguje jako síť (centrála, routry, stanice).

Smart dust (mot) – ještě nejsou používány v praxi, velikostně jsou od kostek cukru až po velikost písku, vytváří také síť. Energii získávají např. z baterie, ale i změnou tlaku či sluncem. Komunikační systém je ale založen na světelném paprsku. Stačí je pouze rozprášit.

Využití: v betonu v pilotech zatloukaných do země – čtou charakteristiky vln odražených od okolní zeminy (druh, nosnost); kažení potravin. V konstrukci budov zjišťují jejich stav. A nebo mohou zjišťovat pohyby osob a o čem se baví.

5

Feature(s)	IEEE 802.11b	Bluetooth	ZigBee
Power Profile	Hours	Days	Years
Complexity	Very Complex	Complex	Simple
Nodes/Master	32	7	64000
Latency	Enumeration upto 3 seconds	Enumeration upto 10 seconds	Enumeration 30ms
Range	100 m	10m	70m-300m
Extendability	Roaming possible	No	YES
Data Rate	11Mbps	1Mbps	250Kbps
Security	Authentication Service Set ID (SSID)	64 bit, 128 bit	128 bit AES and Application Layer user defined

6

Obrázek 5 – Mot

Obrázek 6 – Srovnání sítě ZigBee s jinými způsoby spojení

Počítače

Velice široké téma. Neustále se objevují zprávy o nabourávání do našich dat, odesílání informací o kreditkartách, heslech. Ale taky je monitorována naše komunikace přes email, IM, prohledáván obsah stránek apod. Zvláště pokud obsahují nějaká zajímavá slova (Osama, boom, dollar, …). Obsah emailů se dá šifrovat, 128 bitové je dostačující. Buď je třeba spousta času na rozlousknutí nebo spousta strojů. Řešením může být projekt Seti@home, který má doma cca 5 mil. lidí. Rozlousknout takovou šifru je potom otázkou okamžiku. (Je to ale čirá spekulace.) V některých státech je 128 bitová šifra maximální povolenou.

Velice důležitá organizace pro výzkum a vývoj v této oblasti je DARPA (Defense Advanced Research Projects Agency), patřící pod ministerstvo obrany USA. Chtějí vytvořit databázi všech hovorů, emailů, nákupů kartou, velké výběry nákup chemikálií, cesty, … a to během několika příštích let. Projekt LifeLog má zaznamenávat kompletní lidskou zkušenost – co slyší, vidí, cítí, …

3 Co se děje

RFID čipy se rozšiřují obroskou rychlostí. Firmy WalMart a Metro už začínají pomalu přecházet z čárových kódů na čipy. V USA mají v roce 2006 všechny nové pasy obsahovat čip s biometrickými informacemi držitele, to samé se plánuje v EU (po mírném nátlaku USA).

Sice byl nalezen jiný, k soukromí šetrnější způsob, založený na rozpoznávání mikroskopických vad papíru vzniklých při výrobě, ale pravděpodobně čipy nenahradí. Firma VeriChip zásobuje svými implantovatelnými i externími čipy nemocnice, firmy i jednotlivce na sledování pohybu osob (nemocných, zaměstnanců, dětí) a věcí.

Jeb Bush ve státě Florida prosadil zákon o povinném čipování (GPS čip) pro těžké zločince do konce života. V jižní Americe je tento čip určen pro děti kvůli únosům. Systém elektronického mýtného založený na GPS bude sledovat pohyb každého auta.

Neustále se rozšiřuje monitorovací systém, ve Westminsteru se radnice rozhodla na každý sloup veřejného osvětlení nainstalovat bezdrátový mikrofon. Údajně proti hlučným sousedům. V Chicagu budou mít nová policejní auta na předním skle mikrofon, který bude schopen zachytit konverzaci na půl bloku. A to i u aut, která budou vypadat civilně.

Neustále padají návrhy ze všech koutů světa, aby odposlechy, čtení emailů a vstupy do databází bylo možné i bez povolení soudu.

4 Závěr

"Ať je kdekoli, ať spí či bdí, pracuje či odpočívá, ať je v posteli či ve vaně, může být sledován bez varování, aniž ví, že je sledován."

G. Orwell, „1984"

Lidé mlčky vyměňují pocit bezpečí za své soukromí. Myslí si, že nová opatření teroristy zastaví. Nezastaví, akorát jim lehce znepříjemní jejich činnost. Co je jednoduššího než unesené oběti vyndat její GPS čip? A nejen kvůli teroristům, ale i kvůli pohodlnosti. Marketingové firmy si zjistí, co nakupuji v supermarketu a vytvoří reklamu šitou mě na míru. Již nedaleko je doba, kdy počítače v reálném čase budou schopny analyzovat data o každém jednotlivci a pak na objednávku vydat pouze ty informace, který si zákazník (ať už policie nebo soukromá osoba/firma) bude žádat. Vítejte v roce 1984.

5 Reference

[1] www.cia.gov/cia/information/artifacts/index.htm
[2] bigear.webpark.cz/
[3]www.scienceworld.cz/sw.nsf/ID/38DD9ADAAC5BE9DAC1256E970048FAB9?OpenDocument&cast=1
[4] technet.idnes.cz/hardware.asp?r=hardware&c=A041103_5285953_hardware
[5] www.verichipcorp.com
[6] www.rfidjournal.com
[7] www.21stoleti.cz/view.php?cisloclanku=2004082127
[8] en.wikipedia.org/wiki/Spy_satellites
[9] www.backfire.dk/EMPIRENORTH/newsite/products_en001.htm
[10] www.zigbee.org
[11] www.21stoleti.cz/view.php?cisloclanku=2004121703
[13] www.darpa.gov/ipto/programs/lifelog/index.htm
[14] www.prisonplanet.com/archive_big_brother.html
[15] wired-vig.wired.com/news/privacy/0,1848,68271,00.html
[16] zive.cz/h/Byznys/AR.asp?ARI=117972&CAI=2034
[17] www.21stoleti.cz/view.php?cisloclanku=2004120601
[18] technet.idnes.cz/sw_internet.asp?r=sw_internet&c=A041106_5286119_sw_internet