pro rozpoznávání hlasu a pochopitelně technologie pro vyhodnocování informačního obsahu. Nejde zde ovšem o žádné běžné počítačové technologie. Příkladem budiž dvojice zařízení *SNAPPER a AST 990*, která je schopna zachycovat a vyhodnocovat datové toky o rychlosti až 2488 Gb/s. To je mnohem vyšší rychlost, než jakou mají páteřní spoje na internetu nebo než je telefonní kapacita jakéhokoliv běžného komunikačního satelitu.
Paměť RAM jednoho zařízení odpovídá paměti asi pěti set „nadupaných" PC (48 GB). K rozpoznání informací a k jejich převodu do vhodné digitální podoby se používají speciální čipy. Je jich celá řada a dokážou předzpracovávat obrazové, faxové nebo hlasové „záchyty". Pro vlastní vyhodnocování těchto dat jsou pak používány další speciální čipy. Jinak by to ani nešlo, protože takové informace musí být zpracovány s minimálním zpožděním.

Tento oficiální snímek budovy NSA má symbolizovat její poslání – čerpat informace z éteru.

Příkladem může být čip *FDF* (Fast Data Finder), který pro NSA vyvinula společnost TRW (dodává jí také satelity). Jedna z textových aplikací čipu je schopna například analyzovat tisíce on-line „živých" zdrojů textových dat nebo gigabajty (jedná se o texty!) těchto dat denně. Zdrojová data filtruje přes desítky tisíc složitých zájmových profilů. Pro představu: základními stavebními prvky profilu mohou být slova, jména, telefonní čísla, různé názvy, řeč, lokalita, čas, typ spoje, ale i hlasová identifikace jednotlivé osoby apod. Složité profily mohou být vytvářeny různými logickými výrazy s těmito prvky. NSA také vyvinula vlastní systém pro třídění a získávání informací (tzv. *N-gramová analýza*).

Slovníky

Zúčastněné státy provozují v rámci systému Echelon jednotlivé odposlechové stanice. Za to mají možnost si vytvořit vlastní národní „slovník", který je poskytnut všem ostatním. Slovník obsahuje jednotlivá zájmová slova nebo profily, které zajímají danou tajnou národní službu. Národní slovníky (a jim odpovídající filtry) jsou pak k dispozici ve všech vyhodnocovacích stanicích. Zachycené informace procházejí všemi národními filtry, a pokud je některá z nich některým filtrem označena jako zajímavá, odešle se příslušné národní tajné službě.

Výstupy

Hlavním problémem všech odposlechových systémů je nedat se zahltit informacemi. Podle bývalého ředitele NSA Williama Studemana to bude, jak řekl v roce 1992, hlavní problém americké rozvědky. Aby to vysvětlil, popsal typ filtrování, které je zahrnuto v systémech, jako je Echelon, následovně: Jeden takový systém může generovat milion vstupů za půl hodiny, filtry propustí 6500 vstupů, 1000 jich splňuje další kritéria a jen deset z nich poté vyberou analytici. Ti zkoumají všechno možné, hlavním předmětem je ale politická a obchodně-průmyslová špionáž. Po pádu komunismu ve východní Evropě hledaly tajné služby novou definici svých zájmů. Nikoho nepřekvapilo, že mezi národní zájmy byly nově zahrnuty také **zájmy ekonomické, obchodní a podnikové** (!!!).
Jak to může fungovat, ukazuje americký přístup. Na ministerstvu obchodu byl vytvořen „úřad styčného důstojníka", jehož prostřednictvím rozvědka předává zachycené materiály předním americkým společnostem. V mnoha případech jsou to právě podniky, které vybavují NSA technikou pro systémy, jako je Echelon. Na oplátku do jejich správních rad odcházejí vysocí funkcionáři NSA na dobře placený odpočinek. Podpora americké ekonomice byla prezidentem Clintonem ještě rozšířena v roce 1993, a to zřízením nového úřadu „National Economic Council". Jak může tato pomoc vypadat v praxi, ukazuje několik příkladů vybraných ze zprávy IC 2000.

Příklady

- V roce 1994 NSA zachytila telefonní hovor mezi francouzskou firmou Thomson-CSF a brazilským koncernem SIVAM. Zakázku v hodnotě 1,3 mld. dolarů, o níž se jednalo, nakonec realizovala americká společnost US Raytheon Corporation. Ta později oznámila, že ministerstvo obchodu velmi silně podpořilo americkou ekonomiku v tomto projektu.
- V roce 1995 byly zachycovány všechny faxy a telefonní hovory mezi evropským konsorciem Airbus Industries, saúdskoarabskými aeroliniemi a vládou Saúdské Arábie. NSA z nich zjistila, jaké Airbus nabízí úplatky, a styčný důstojník zařídil, aby společnosti Boeing a McDonnell Douglas nabídly vyšší částku. Výsledný obchod činil 6 miliard dolarů ve prospěch USA.
- Byznys je byznys, a platí to i o dvou hlavních zakladatelích Echelonu, Kanadě a USA, jak to ve své knize „Spyworld" ukázal bývalý kanadský špion Mike Frost. V roce 1981 byla zachycena komunikace amerického velvyslance v Kanadě realizovaná prostřednictvím celulárního telefonu. Výsledkem bylo, že Kanada přebrala USA výnosný obilní obchod s Čínou v hodnotě 2,5 miliardy dolarů.
- Mike Frost také uvedl, že kanadská služba CSE byla pozdější anglickou ministerskou předsedkyní Margaret Thatcherovou požádána o špionáž týkající se dvou ministrů jejího kabinetu (anglická tajná služba to z právních důvodů udělat nemohla) a o „nabourání" mobilního telefonu Margaret Trudeauové, manželky Pierra Trudeaua, který se později stal kanadským premiérem.

Když to jinak nejde...

Šifrování je z legislativního hlediska USA de facto zbraň. Pohled NSA na šifrování vypadá podle bývalého důstojníka CIA Johna Millise takto: „... Šifrování je zde a jeho používání rychle poroste. To jsou pro nás špatné zprávy. Budeme nuceni investovat ohromné množství peněz do nové technologie, abychom byli schopni se dostat k informacím, které stále potřebujeme..."
V článku W. Madsena (viz *http://caq.com/CAQ/caq63/caq63madsen.html*) byla nedávno odhalena komerčněšpionážní šifrová aféra století, která dosud nemá v historii obdoby. Článek pojednává o vztazích NSA a švýcarské společnosti Crypto AG, která dodává šifrovací technologii prominentním zákazníkům na celém světě. Je založen mj. na výpovědi Hanse

Buehlera, bývalého zaměstnance společnosti. Podle článku společnost umožnila pracovníkům NSA takové úpravy v šifrovacích zařízeních, které dovolovaly číst utajovanou vojenskou a diplomatickou korespondenci asi 120 států, jež si tato zařízení nakoupily! Zásahy spočívaly v realizaci tzv. skrytého kanálu, což je kryptografická metoda, jak v rámci přenosu regulérně zašifrované informace předávat i použitý šifrovací klíč. Úpravy přitom byly takového rázu, že ani ten, kdo zařízení kontroloval, neměl mnoho šancí je odhalit. Jinými slovy – tam, kde to nejde běžnými prostředky, se prostě nasadí zpravodajská technika přímo...

Žánrový obrázek našeho věku: V pozadí Menwith Hill (stanice F-83) ve Velké Británii; v podzemí je celé město (blíže viz Chip 8/98), nechybí tam ani supermarket, kostel a stadion...

Nejsou to fámy

V květnu t. r. ředitel australské tajné služby DSD Martin Brady oficiálně potvrdil, že „DSD spolupracuje s účastnickými tajnými službami na základě dohody UKUSA“. Byl to první přímý oficiální důkaz existence systému po padesáti letech od podepsání dohody.

V říjnu 1998 probíhala v Evropském parlamentu debata o americko-evropských vztazích na poli rozvědky. Úředníci Evropského parlamentu vyjádřili obavy, že Echelon je účastnickými státy používán k ekonomické rozvědce. Aby k tomu EP měl relevantní informace, byl odborný orgán EP (STOA) požádán o vypracování příslušné zprávy. Ta byla publikována v dubnu 1999 (viz výše) a je velmi dobrým přehledovým materiálem o situaci v této oblasti.

Co na to Evropa?

Uveďme dosavadní reakce alespoň některých evropských států. (Určitě bude zajímavé sledovat, kterým směrem se vydá naše republika.)

• **Německý** přístup k ochraně dat byl donedávna trochu rozpačitý. Na svém zasedání letos v červnu však německá federální vláda politiku v oblasti kryptografie a ochrany dat rázně změnila. Přijala zásadní dokument o principech německé šifrové politiky „Eckpunkte der deutschen Kryptopolitik“ *(www.bmwi.de/presse/1999/0602 prm1.html*), který předložilo ministerstvo vnitra a hospodářství a který zcela mění dosavadní vládní postoj k silné kryptografii. Dokument, který je i ve světě ojedinělý a který vřele doporučujeme i našim politikům, vysvětluje také význam kryptografie a šifrovacích prostředků. Vláda (!!!) je vnímá jako nástroje nezbytné pro ochranu důvěrnosti, pro dynamický rozvoj elektronického obchodu, digitálních podpisů a digitálních peněz. A co víc, vyjadřuje nespokojenost se stavem používání šifrovacích prostředků. „Je to často v důsledku chybějícího nezbytného bezpečnostního vědomí, přestože **neoprávněná špionáž**, manipulace nebo destrukce dat **může způsobit podstatné ekonomické ztráty**,“ říká se v dokumentu.

K často používanému americkému argumentu, že prostředky se silnou kryptografií by mohly zneužít kriminální živly, se poznamenává, že v Německu to nezpůsobilo žádný problém. A kdyby bylo potřeba získat informace, které by případné kriminální živly chránily silnou šifrou, vládní stanovisko je „použít alternativní prostředky“. Jde zřejmě o technické zpravodajské prostředky, například o skrytou kameru snímající přístupové heslo (klíč), apod. Na takové případy není třeba mít k dispozici ani světový odposlechový systém, ani všeobecný zákaz týkající se použití silné kryptografie.

• **Francie** změnila svoji politiku na poli šifrování letos v lednu. Ministerský předseda Lionel Jospin oznámil, že Francie obrací svoji dlouhotrvající tradiční domácí restriktivní politiku směrem k volnému používání silných šifer až do délky klíče 128 bitů. Do té doby Francie umožňovala na domácím poli (!) používat volně pouze šifry do 40 bitů klíče. V ostatních případech musela mít tajná služba zaručen přístup k zašifrovaným informacím. Tato změna se už promítla do konkrétních kroků.

• **Švédsko:** Podle časopisu Datateknik (č. 10/99, viz *http://www.datateknik.se*) švédské ministerstvo zahraničí studuje zprávu IC 2000 a švédská vláda pověřila tajnou policii SÄPO, aby **vyšetřila průmyslovou špionáž, která je vedena proti švédským národním a průmyslovým zájmům**. Zahrnuje to systém Echelon a dohodu UKUSA.

Naproti tomu jsou zde jiné aktivity, které jdou ve směru systému Echelon. Jsou jimi tzv. Wassenaarská dohoda a systém Enfopol. ***Wassenaarská dohoda*** (*http://www.wassenaar.org*) byla podepsána 33 evropskými státy (i Českou republikou) a účastnické státy se v ní zavázaly, že budou regulovat vývoz silné kryptografie (délka klíče 64 bitů a více) mimo území členských států. Systém ***Enfopol*** je tajný systém, o němž se dosud jedná a který má umožnit spolupráci FBI a policejních orgánů evropských států v oblasti elektronického odposlouchávání. Jejich součinnost předpokládá podobný princip, na kterém funguje Interpol.

Závěr

Další komentář k uvedeným informacím je nejspíš zbytečný. Čtenářům, kteří mají o tento problém hlubší zájem, doporučuji ke studiu prameny uvedené v textu i v infotipech. A pokud chcete trochu nahlédnout pod pokličku tajným službám, jděte se podívat na film „Nepřítel státu“ (The enemy of the state, 1999), který snad ještě občas běží v kinech. Už jenom to, jaké techniky je možné ukázat ve filmu, o lecčems vypovídá.

VLASTIMIL KLÍMA *(VKLIMA@DECROS.CZ)*

infotipy

Zpráva P. S. Poola pro Free Congress Foundation:
fly.hiwaay.net/~pspoole/echelon.html
Informace o systému Enfopol:
www.heise.de/tp/english/special/nfo/6383/1.html
Zpráva STOA ze září 1998:
www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm
Informace o knize Nickyho Hagera a některé kapitoly v plném znění:
www.fas.org/irp/eprint/sp/index.html
Nejnovější zpráva STOA z dubna 1999 (IC 2000):
www.iptvreports.mcmail.com/stoa_cover.htm