Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: Informační studia a knihovnictví

Studijní obor: Informační studia a knihovnictví

Pavel Pacák

Přenos a ochrana informací v mobilních telekomunikacích

The transfer and protection of information in mobile telecommunications

Bakalářská práce

Praha 14.8. 2011

Doc., RNDr. Jiří Ivánek, CSc.

Vedoucí bakalářské práce: Doc., RNDr. Jiří Ivánek, CSc.

Oponent bakalářské práce:

Datum obhajoby:

Hodnocení:

Prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, že jsem řádně citoval všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze, 14. srpna 2011

.....

podpis studenta

Identifikační záznam

PACÁK, Pavel. *Přenos a ochrana informací v mobilních telekomunikacích [The transfer and protection of information in mobile telecommunications]*. Praha, 2011. 50 s. Bakalářská práce. Univerzita karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí práce Doc., RNDr. Jiří Ivánek, CSc.

Abstrakt

Práce se zabývá přenosem a ochranou informací v mobilních telekomunikačních sítích. Nejprve je představen historický vývoj jednotlivých technologií v této oblasti užívaných, posléze je věnován důraz na prvky zabezpečení jednotlivých typů sítí. Uvedeny jsou také různé formy nebezpečí, jež hrozí uživateli mobilního telefonu každým dnem, kdy jej používá. V závěru je představeno několik možných řešení bezpečnostní problematiky. Výstupem jsou navržené způsoby komunikace prostřednictvím mobilních sítí, jež nabízejí vyšší úroveň bezpečnosti a v nichž jsou tedy citlivá data ve větším bezpečí.

Abstract

The work focuses on the transfer and protection of information in mobile telecommunications. First, historical development of each technology used is introduced. Also different forms of thread which user can face in every day use of his cell phone are listed. In the end few possible solutions of security policy are presented. Possible ways of communication with higher level of security which can be used with your cell phone are the conclussion.

Klíčová slova

bezpečnost, šifrování, algoritmus, kodeky, telekomunikace, telefonní sítě, GSM, UMTS, 3G, kryptotelefon, Skype, karta SIM, šifra A5

Keywords

security, encryption, algorithm, codecs, telecommunications, telephone network, GSM, UMTS, 3G, crypto phone, Skype, SIM card, A5 algorithm

Obsah

Předmluva

Tato bakalářská práce se věnuje přenosu a ochraně informací, a to konkrétně v oblasti mobilních telekomunikací.

Mobilní telefon používá denně většina občanů nejen České republiky. Jeho prostřednictvím přenášíme velké množství dat, mnohdy i velmi citlivých, jejichž zneužití by mohlo mít následky mnohem horší, než jsme si ochotni připustit. Bezpečnostní problematice mobilní komunikace však přesto většina lidí nevěnuje téměř žádnou pozornost.

Právě z toho důvodu jsem se rozhodl pro toto téma a rád bych v následující práci přiblížil alespoň základní principy daného problému.

V první části představím jednotlivé technologické standardy v této oblasti užité od jejích historických počátků až po současnost.

Další sekce se věnuje způsobům, jakými jsou telefonní hovory běžně zabezpečené v současné době. Mojí snahou tedy bylo nastínit, jaká úroveň ochrany je standardně věnována datům přenášeným v mobilních sítích.

Jelikož žijeme v době, kdy spousta počítačových hackerů a jim podobných jedinců ráda ostatním dokazuje kam až se mohou v rámci zabezpečení nejrůznějších služeb dostat, věnuji třetí kapitolu bezpečnostním rizikům a tomu, jak se tyto v průběhu let vyvíjely. Právě touto kapitolou bych rád upozornil na bezpečnostní problémy, kterým může být velmi snadno vystaven každý z nás.

Na závěr práce se pak pokusím navrhnout několik různých variant možného řešení bezpečnostní problematiky a pokusím se je blíže představit. Výstupem by měly být způsoby komunikace, jež uživateli nabízí uspokojivější úroveň zabezpečení a tedy lépe chráněná citlivá data.

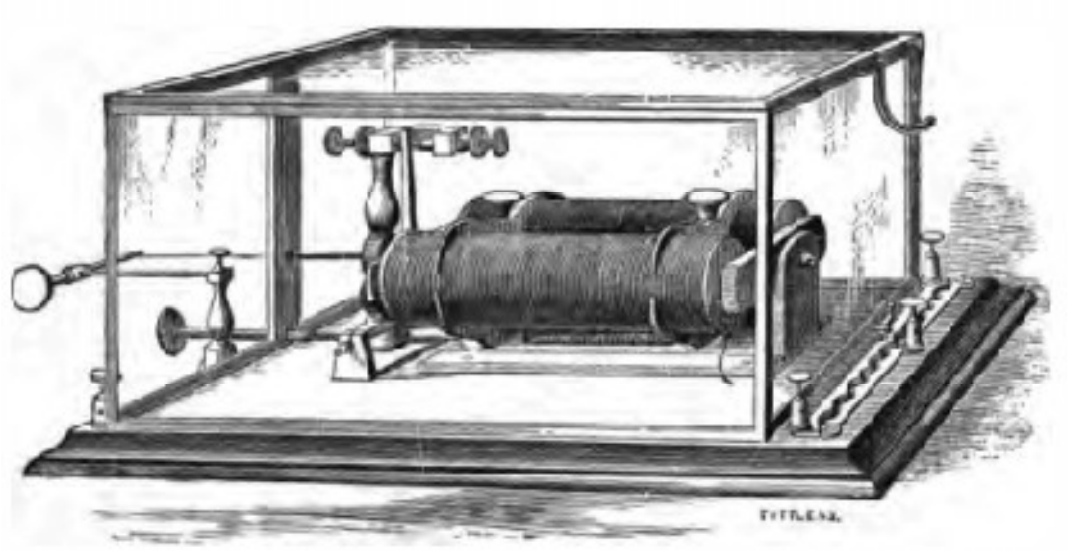
V sekci se zdroji jsou veškeré záznamy tvořeny dle normy ISO 690 a ISO 690-2. Uspořádání pak reflektuje strukturu bakalářské práce. V jednotlivých sekcích je užito abecední řazení.

Za vedení bakalářské práce, podporu a přínosné rady bych rád poděkoval Doc., RNDr. Jiřímu Ivánkovi, CSc.

1 Historie mobilních telekomunikačních sítí

V této kapitole se pokusím představit jednotlivé „mobilní generace“, jejich stručnou historii a základní rozdíly mezi nimi.

Pokud bychom se chtěli vrátit až k úplnému prapočátku mobilní komunikace, pravděpodobně bychom se dostali až do roku 1837, tedy k době, kdy Samuel Morse sestrojil první telegraf [obrázek č.1]. Ten byl tehdy samozřejmě ještě limitován dráty, ačkoliv již roku 1865 uskutečnil zubař M. Loomis pokus, při němž vypustil do vzduchu dva papírové draky s kovovou kostrou, přičemž jeden z nich měl k sobě připojenu vysílací část telegrafu, druhý pak galvanometr, jenž přijímané signály zaznamenával. Morseova abeceda, zakódována do různých hodnot elektrického proudu byla takto přenášena na vzdálenost až 18 mil. [6, str. 73-99]



Obr. 1

O první mobilní přenosy se pro změnu v roce 1879 zasloužil v ulicích Londýna D.E. Hughes, jež dokázal vygenerovat a následně také zachytit signály přenesené za pomoci rádiových vln. O své zkušenosti se Hughes pokusil podělit také s Královskou vědeckou společností. Nebyl však správně pochopen (mysleli si, že jde o přenos pomocí magnetické indukce jako u Loomise), proto zklamaný Hughes nikdy své objevy nepublikoval. [1]

Dalším zásadním milníkem byl rok 1888, kdy Němec Heinrich Hertz potvrdil a experimentem dokázal tzv. Maxwellovu teorii, tedy že vzduchem

lze přenášet elektrické radiové vlny. O děvět let později pak Ital Guglielmo Marconi získal patent na úspěšně sestrojený a zprovozněný radiový systém, ačkoliv o toto prvenství se vedly mnohaleté spory.

Zatímco zpočátku bylo radio využíváno k přenosu telegrafních kódů, již roku 1906 se podařilo R. Fessedenovi pomocí radia přenést lidský hlas.

Tímto se již dostáváme k samému vynálezu prvního mobilního telefonu. Psal se rok 1910, když L.M. Ericsson (zakladatel společnosti Ericsson, známý výrobce mobilních telefonů, který se později spojil se značkou Sony a dnes vyrábí pod označením Sony Ericsson) přišel s prvním telefonem do automobilu. Jednalo se o klasický telefon, který však nebyl připojen do běžné telefonní sítě, nýbrž jeho součástí byly dvě kovové tyče, jež bylo možné připojit k telefonním kabelům na libovolném místě.

Desátá a dvacátá léta minulého století se nesla v duchu obrovského zájmu o radiové vysílání a jeho rozmachu. Průkopníkem, co se používání radia týče, byla policie města Detroit, která roku 1921 instalovala do prvního vozu radiopřijímač morseovy abecedy.

O pouhé tři roky později bylo v Bell Laboratories vyvinuto první mobilní radio, jež bylo schopné přenášet hlas v obou směrech. Za druhé světové války pak již byla na bojišti využívána přenosná vysílačka od společnosti Motorola.

Zcela zásadní zlom přišel 17. června 1946, kdy v Saint Louis společnost AT&T (jeden z největších současných mobilních operátorů v USA) spolu s firmou Southwestern Bell představila první radiotelefony pro veřejnost, jež bylo možné montovat do automobilů. [11]

Autotelefony samozřejmě vzbudily velký zájem o oblast mobilní komunikace a ve významné míře tak přispěly k jejímu masivnímu rozvoji. Již o rok později (1947) zveřejnili v interních materiálech Bell Laboratories W.R. Young a D.H. Ring článek poprvé popisující základní principy mobilních celulárních sítí (v podstatě dnešní GSM). Jednalo se o síť rozdělenou na menší oblasti (zvané buňky), kdy každá z nich obsahovala přijímač/vysílač a celá síť byla monitorována řídícím střediskem.

Ještě téhož roku Bell Laboratories zažádali o přidělení dalších frekvencí. V tomto jim bylo vyhověno, avšak k jejich velké nelibosti byly frekvence přiděleny i dalším zájemcům. Na poli mobilní komunikace tak začala vznikat konkurence.

Dalším průkopníkem byla společnost Richmond Radiotelephone Company, jež spustila první plně automatizovanou síť. Zatímco do té doby byla pro uskutečnění hovoru potřebná účast živého operátora na ústředně, nyní byly telefonáty spojovány přímo. Většina společností však až do 60. let operátory nadále využívala.

Celá 50. a 60. léta se nesla ve znamení nejprve výzkumu a posléze také vývoje celulárních sítí. Největších pokroků nadále dosahovali v Bell Laboratories. Právě této společnosti byl 16. května 1972 přidělen patent na „mobilní komunikační síť“. Díky byrokratickým průtahům však povolení k spuštění první opravdové mobilní sítě přišlo až o celých pět let později, roku 1977.

1.1 NMT (1G)

V těchto a následujících řádcích se pokusím popsat jednotlivé generace mobilních sítí s důrazem kladeným zejména na ty, jež byly nasazeny i v České republice. Začněme tedy generací první a standardem NMT, jež u nás provozovala od roku 1991 společnost Eurotel (dnešní Telefónica O2 Czech Republic). [13]

První generace mobilních služeb byla ještě realizována analogově. Spolu s prvním celulárním telefonem vznikla v 80. letech. V této době hrál hlavní roli přenos hlasu, nikoliv dat. Do první generace patřily zejména tyto tři analogové systémy:

- NMT (Nordic Mobile Telephone)
- AMPS (Analog Mobile Phone System)
- TACS (Total Access Communications System)

První komerčně provozovanou sítí byla malá síť provozovaná od roku 1978 společností Batelco. Původně se jednalo o komunikační řešení pro královskou rodinu v Bahrajnu, později však byla tato celulární síť zpřístupněna i ostatním obyvatelům. [9]

AMPS byla provozována v USA. První pokusné spuštění této sítě se odehrálo ještě v laboratořích AT&T. V první fázi byla testována pouze zaměstnanci Bell Laboratories, roku 1978 byl spuštěn komerční testovací provoz v okolí Chicaga. Síť pracující na frekvenci 800 MHz měla úspěch a začala se budovat i v několika dalších zemích. Úřady však povolily spuštění této sítě až v roce 1983, kdy se konečně objevil dostatek zájemců o její provozování – to proto, aby AT&T nevytvořilo telekomunikační monopol. [9]

Zatímco v USA byla provozována jedna síť na celém jejím území, v Evropě byla situace složitější. V různých zemích vznikaly různé sítě. Původně pro Velkou Británii byla specifikována síť TACS, fungující na frekvenci 900 MHz, jež později našla uplatnění také v Asii a oblasti Pacifiku. V Západním Německu a Rakousku vznikla síť C-Netz, v Itálii RTMS, Francie přišla s Radiocom 2000, Dánsko, Finsko, Norsko a Švédko (právě pro tuto kombinaci byl zvolen název Nordic Mobile Telephone) společnými silami budovali síť NMT450, jež pracovala na frekvenci 450 MHz a byla poprvé spuštěna roku 1981.

Jak již bylo výše zmíněno, v České republice byla nasazena síť NMT, tedy stejná síť, která byla představena v předchozím odstavci jako výsledek spolupráce čtyř severských zemí. U nás bylo NMT spuštněno roku 1991. Z dnešního pohledu se však jedná o technologii již značně překonanou, což dokládá i fakt, že v roce 2006 společnost Telefónica O2 Czech Republic provoz této sítě ukončila a frekvence, jež byly tímto krokem uvolněny, začala využívat pro datový provoz technologie CDMA. [13]

1.2 GSM (2G)

Z předchozích řádků jasně vyplývá, nakolik byla situace v Evropě složitá. Jakákoliv jednota a s ní spojené standardy byly v té době pouhým snem. To

s sebou samozřejmě přinášelo mnoho problémů. Mezi nejvýznamnějšími je možno zmínit třeba nekompatibilitu mobilních telefonů (a s tím spojené vyšší výrobní náklady firem, jež tato zařízení vyráběla) či nemožnost využití roamingu.

Právě tyto problémy vedly k iniciativě, na jejímž konci byl vznik standardu GSM (na obrázku č. 2 logo). Tím, kdo tento standard přivedl na světlo světa byla roku 1982 Evropská komise pro pošty a telekomunikace (čítající 26 členů tvořených evropskými telekomunikač-ními společnostmi). Projekt se tehdy jmenoval Groupe Spéciale Mobile a jeho cílem bylo vyvinout jednotnou mobilní celulární síť pro celou Evropu. [12]

Obr. 2

GSM bylo specifikováno jako síť využívající již digitálního způsobu přenosu, fungující na frekvenci 900 MHz a zaměřující se opět primárně na hlasové služby. Prostupnost sítí proto nepřekračovala 20 kbps.

V roce 1989 se za rozvoj GSM stal zodpovědným Evropský telekomunikační institut a o dva roky později následoval první oficiální návrh standardu. Ještě téhož roku byla v Ženevě spuštěna testovací síť GSM a význam této zkratky byl změněn na Global System for Mobile Communications.

Spuštění prvních komerčních sítí typu GSM následovalo velmi záhy, již roku 1992 se k tomuto kroku odhodlaly Dánsko, Finsko, Francie, Itálie, Německo, Portugalsko a Švédsko. Ještě téhož roku také Telecom Finland a Vodafone UK podepsali vůbec první roamingovou dohodu. To byl jasný počátek realizace snu o sjednocené mobilní Evropě.

Pro zajímavost mohu uvést, že již o rok později, na sklonku roku 1993 využívalo GSM více jak milion zákazníků. Mezi 69 členy asociace z 48 zemí

byla mimo jiné také australská Telstra. GSM tak překročilo hranice evropského kontinentu. [2, str. 5-6]

V září 1993 byla po dalším vývoji ve Velké Británii spuštěna také upravená síť GSM fungující na frekvenci 1800 MHz (dnes spolu s 900 MHz frekvencí naprostý standard), mezi jejíž hlavní výhody patřilo mnohem větší množství kanálů. Nevýhodou však oproti tomu byl menší dosah, což znamenalo potřebu stavby velkého množství základnových stanic. Toto řešení bylo vhodné například pro velká a hustě osídlená města.

Po roce 1994 sáhly po standardu GSM i USA, které jej však začaly provozovat na jiných frekvencích, a to 850 a 1900 MHz. Dlouho proto byla mobilní zařízení z Evropy za oceánem nepoužitelná a ani Američané si u nás se svým telefony nezavolali. Netrvalo to ale dlouho a objevily se první takzvaně triální telefony (podpora evropských frekvencí a jedné z amerických) a posléze také telefony podporující frekvence všechny čtyři. [9]

Z technického hlediska můžeme zjednodušeně říci, že GSM je síť dělící se na malé buňky, jež jsou obsluhovány jednotlivými základnovými stanicemi (BTS, Base Transceiver Station), které mají na starosti všechny uživatele vyskytující se v daném obslužném okruhu. Nad těmito stanicemi pak ještě funguje síť ústředen, jež zajišťují přepínání hovorů do dalších ústředen v síti vlastní, v sítích jiných mobilních operátorů či v pevné síti. Ústředny obsahují též různé registry, jež v sobě nesou informace potřebné k identifikaci koncového uživatele. [8]

V sítích druhé generace sice původně nebylo počítáno s žádnou možností přenosu dat, časem však i tato funkce přibyla. Jednalo se o z dnešního pohledu již velmi pomalé vytáčené připojení pomocí technologie CSD (Circuit-Switched Data, 9,6 kbps) a později prostřednictvím její vylepšené verze HSCSD (High Speed Circuit-Switched Data, až 43 kbps). Uživatelé se za jejich pomoci připojovali k w@pu, speciálně upraveným, datově nenáročným internetovým stránkám tvořeným pro mobilní telefony.

1.3 GPRS/EDGE (2,5G)

Z hlediska historického vývoje mobilních sítí není možné opomenout ani takzvanou síť „dvaapůlté“ generace. Jedná se konkrétně o datové standardy, které byly jakýmsi mezistupněm mezi GSM a UMTS (zástupce sítí třetí generace, o nichž bude řeč později).

Základní rozdíl mezi sítěmi druhé a třetí generace je v tom, že zatímco GSM je postavené na principu přepínání okruhů, technologie modernější (např. UMTS) jsou již koncipovány jako sítě využívající tzv. přepínání paketů, což znamená zejména umožnění efektivnějšího přenosu dat. [8, str. 230]

Zrod 2,5G se většinou datuje rokem 2001, kdy přišla na trh technologie GPRS (General Packet Radio Service) umožňující mobilní připojení k internetu teoretickou rychlostí až cca 115 kbps. Nejzásadnějším rozdílem pro uživatele byla zpočátku změna účtování dat. Neplatilo se již za čas strávený na Internetu, nýbrž za přenesená data. Znamenalo to tedy, že uživatel mohl být připojen k Internetu neustále a přenášely se jen „balíčky“ dat, tzv. pakety, kdykoliv telefon začal využívat data. [14]

Z technického hlediska GPRS ovlivňuje několik základních elementů. Prvním je schéma kódování (Coding Scheme), jež existovalo ve čtyřech variantách: CS-1 (9 kbps / jeden časový úsek), CS-2 (13,4 kbps), CS-3 (15,6 kbps) a CS-4 (21,4 kbps). Volbu kódovacího schématu uživatel nemohl vlastním přičiněním nijak ovlivnit, probíhala automaticky, a to v závislosti na vzdálenosti mobilní stanice (telefonu) od základnové stanice a na kvalitě signálu.

Víme tedy, že kódovací schéma stanovuje maximální rychlost v jednom časovém úseku. Faktorem, který ovlivňuje tyto časové úseky je třída GPRS (GPRS Multislot Class), jež určuje množství úseků, které může mobilní stanice v jeden okamžik použít. Každá stanice podporuje jednu stanovenou třídu. Může to být např. 4+1, což znamená, že může využívat čtyři úseky pro download a jeden pro upload dat.

Rychlost GPRS však není konstantní, tzn. že uživatel vždy nemůže využívat maximální možnou rychlost danou kódovacím schématem a třídou. V sítích GSM jsou totiž prioritou hlasové hovory. Ty využívají již zmíněné časové úseky taktéž, a to na úkor připojení GPRS. Zjednodušeně tedy můžeme říci, že čím více je vytížena síť (čím více lidí volá), tím pomaleji či vůbec bude fungovat GPRS. Připojení se v takové situaci zpomalí či pozastaví a k obnovení rychlosti dojde ve chvíli, kdy se kapacita sítě opět uvolní.

V neposlední řadě se pak k GPRS váže ještě jedno technické specifikum, a to je režim GPRS třídy: A, B, nebo C. Tento režim stanovuje, jakým způsobem se bude chovat mobilní stanice připojená k internetu v okamžiku, kdy se na ni někdo pokusí dovolat či na ni směřuje příchozí SMS zpráva.

Třída A značí, že pro stanici není problém udržet ve stejném okamžiku datové připojení a zároveň odbavit hovor. B je potom symbolem režimu, ve kterém je telefon schopen v určitém momentu provozovat pouze jednu z těchto dvou služeb. V takové chvíli dojde při příchozím hovoru k přerušení datového spojení a po jeho ukončení se spojení opět obnoví. Poslední variantou je třída C, která umožňuje využití pouze jedné ze služeb, to znamená, že ve chvíli, kdy je mobilní stanice připojena k Internetu, jeví se pro hovory jako nedostupná a uživatel se o příchozím hovoru v reálném čase nijak nedozví. Logicky je tedy třída C nejméně komfortní variantou, z toho důvodu se dnes již téměř nevyužívá. [8]

Další technologií spadající do 2,5G je EDGE (Enhanced Data for GSM Evolution), jež je v podstatě evolucí sítí GSM/GPRS. Jedná se sice o technologii založenou na bázi GSM, k sítím třetí generace má však již velmi blízko. V ideálních podmínkách je tato technologie až třikrát rychlejší nežli GPRS a dosahuje tak teoretické rychlosti až 384 kbps. Reálné údaje však hovoří o rychlosti nepřesahující 250-300 kbps. Veškerá omezení, která má technologie GPRS, sdílí i rychlejší varianta EDGE.

1.4 UMTS (3G)

Jestliže systém GSM měl být zjednodušením a velkým přínosem pro celou oblast telekomunikací, je nutné podotknout, že s příchodem další generace mobilních sítí se situace obrátila a došlo k opětovnému tříštění.

3G totiž není pouze jediná technologie. Jedná se o několik různých telekomunikačních standardů, přičemž UMTS (Universal Mobile Telecommunications System), v našich končinách asi nejznámější z těchto technických řešení, je pouze jednou z variant.

Chceme-li však tomuto dělení lépe porozumět, je třeba vysvětlit si, proč k němu vůbec došlo.

Na počátku všeho byla Mezinárodní telekomunikační unie ITU, jež chtěla celou třetí generaci harmonizovat a vytvořit tak prostředí ještě kompatibilnější, než jak tomu bylo v případě GSM. Problém však nastal již v počátcích celé harmonizace, a to na území USA, kde tamní úřady rozprodaly frekvence, s nimiž bylo pro UMTS počítáno, operátorům k jiným účelům.

Trio velkých hráčů této oblasti tvořené společnostmi Motorola, Lucent a Qualcomm se pak rozhodlo lobbovat pro odlišný 3G systém, a to hlavně z důvodu hladkého přechodu od sítí druhé generace k sítím generace třetí. Americký standard CDMA2000 (Code Division Multiple Access 2000), o kterém bude řeč později, totiž umožnil existenci stávajících 2G a nových 3G sítí ve frekvenčním pásmu, jež by si jinak přivlastnilo samotné UMTS.

Nebyli to však pouze Američani, kteří plány na sjednocené 3G zkomplikovali. Přidala se totiž i WTO, která se ozvala s požadavkem nediskriminačního prostředí. Jinými slovy nechtěla, aby bylo komukoli nařizováno, jakou technologii má použít. Naštěstí však i přes to většina evropských operátorů využila technologie UMTS, a to zejména ze dvou důvodů. Jednak pro snadnost přechodu z GSM na tuto novinku, dále pro snadné řešení roamingu, kdy koncový uživatel nepotřebuje mít pro každou zemi jinak vybavený telefon. Toto samozřejmě šetří peníze i výrobcům mobilních stanic. [9]

K technologii UMTS se váže také sada přijatých doporučení specifikujících technologie pro sítě 3G zvaná IMT-2000 (International Mobile Telecommunications 2000), kterou připravila již zmiňovaná ITU. Číslo 2000 obsažené v názvu v tomto případě znamená hned tři věci, a to rychlost připojení do 2 Mbps, kmitočet kolem 2GHz a předpokládané uvedení systému do provozu okolo roku 2000.

IMT-2000 však není jediným projektem věnujícím se této problematice. Vhodné je zmínit také program 3GPP (Third Generation Partnership Project, logo na obrázku č. 3), jež vznikl v roce 1998 a věnuje se přípravě specifikací pro UMTS. Existuje také projekt 3GPP2 věnující se americké obdobě UMTS, již zmiňované technologii CDMA2000. [10]

Obr. 3

Aby však situace s 3G byla ještě složitější, vedle evropského a amerického standardu jich existuje hned několik dalších:

- W-CDMA (Wideband Code Division Multiple Access)
    - UMTS (Universal Mobile Telecommunications System)
    - FOMA (Freedom of Mobile Multimedia Access)
- CDMA2000 (Code Division Multiple Access 2000)
- TD-SCDMA (Time Division Synchronous Code Division Multiple Access)

Z právě uvedeného rozdělení můžeme vidět, že v České republice používaná technologie UMTS je pouze jednou ze dvou variant japonsko-evropského standardu W-CDMA, přičemž jeho druhou variantou je technologie zvaná FOMA, jež je využívána v Japonsku. Tyto dvě technologie jsou si velmi podobné, liší se však v některých detailech, a tak i přes společný zastřešující standard jsou bohužel vzájemně nekompatibilní.

CDMA 2000 je standardem americkým, který je možné dále rozdělit ještě na 4 varianty:

- 1xRTT (1x Radio Transmission Technology, až 144 kbps)
- 3xRTT (3x Radio Transmission Technology, až 2 Mbps)
- 1xEV-DO (Data Optimised, síť určená pouze pro data, až 2,45 Mbps)
- 3xEV-DV (Data Voice, síť kombinující podporu dat i hlasu)

Posledním výrazným typem 3G sítí je pak standard TD-SCDMA. Jedná se o řešení čínské. Jelikož má Čína více uživatelů mobilních telefonů než kterákoliv jiná země na světě, rozhodla se její vláda nepodřídit se mezinárodnímu „diktátu“ a přišla s vlastním řešením. Výhodou TD-SCDMA je pro Čínu i fakt, že takto nemusí platit za patenty spojené s jinými, mezinárodně uznávanými standardy. [8]

1.5 HSDPA/HSUPA (3,5G)

A jakým směrem se 3G sítě ubírají? Hlavním důraz je kladen na další zvyšování propustnosti sítě. Výsledkem posouvání hranic možností mobilníh připojení jsou zejména dvě datové nadstavby UMTS sítí. Jedná se o technologie HSDPA a HSUPA.

HSDPA (High-Speed Downlink Packet Access) bylo vyvinuto jako rešení rychlejšího proudění dat směrem k uživateli (download). Ačkoliv se původně počítalo s rychlostí až 4,3 Mbps, dnes se teoretické maximum vyšplhalo až na hranici 14,1 Mbps. [10]

Jedná se však samozřejmě o číslo teoretické. Rychlost totiž ovlivňuje hned několik faktorů. Jednak je to vytíženost sítě (zde můžeme vidět podobnost se sítěm 2,5G), kdy kvůli sdílení rychlosti může v době „špičky“ být datový provoz značně zpomalen, dále je to vzdálenost od základnové stanice BTS. Zákazník, který bude v její přímé blízkosti, využije v ideálních podmínkách (pokud nebude vytížená síť) téměř maximální rychlost, kterou operátor umožňuje. Čím dále se však zákazník bude od BTS nacházet, tím větší část datové kapacity bude sítí využívána na ochranu proti chybám přenosu.

Druhým krokem ve vývoji rychlých UMTS dat bylo poté HSUPA (High-Speed Uplink Packet Access). Díky této technologii bylo mobilní internetové

připojení opět výrazně zrychleno, neboť HSDPA bylo tímto technickým řešením doplněno. HSUPA je totiž určeno primárně pro proudění dat směrem od uživatele do sítě (upload). [8]

Původně se u HSUPA počítalo s maximální rychlostí okolo 1-5 Mbps, dnes však lze teoreticky provozovat i síť s uploadem až 11,5 Mbps.

HSUPA je možné znát také pod zkratkou EUL (Enhanced UpLink).

Kombinací obou technologií se pak dostáváme k finálnímu produktu zvaném HSPA (High-Speed Packet Access), který využívá jak rychlého stahování pomocí HSDPA, tak rychlého odesílání dat pomocí HSUPA. Vývoj tohoto technického řešení nebyl do dnešního dne ukončen. Protože funguje na principu, kdy je jeho rychlost v přímé úměře s množstvím mobilních vysílačů (BTS), limity maximálních rychlostí je tak možné dále posouvat. Teoreticky se hovoří až o hranici 100 Mbps pro upload a 50 Mbps pro download. [15]

1.6 LTE (4G)

UMTS/HSPA je vrchol, jakého zatím tuzemské mobilní telekomunikace dosáhly. Ve světě však jsou mobilní operátoři dále a budují to, co je z našeho pohledu zatím jen krásná budoucnost. Řeč je o sítích čtvrté generace, mezi které se oficiálně řadí technologie LTE (logo na obrázku č. 4) a WiMAX.

LTE (Long Term Evolution) je dalším technologickým standardem vznikajícím pod hlavičkou 3GPP. [7]

Nejzásadnější novinkou a velkou výhodou pro všechny jsou rychlosti toku dat v obou směrech. LTE totiž teoreticky podporuje rychlost až 326 Mbps při stahování dat a až 86 Mbps při jejich odesílání. Při praktických testech se sice těchto hodnot nepodařilo dosáhnout a testy naměřily reálné hodnoty při stahování okolo 173 Mpbs, přesto se oproti UMTS jedná o obrovský skok. [3]

Prvním, kdo LTE začal budovat a uvedl do komerčního provozu, byl operátor TeliaSonera, který tuto síť zprovoznil ve švédském Stockholmu a norském Oslu. Právě v prvním z jmenovaných měst podrobil tyto sítě opravdu reálnému měření redaktor vydavatelství IDG. Ten se dostal nejvýše k hodnotám 59,1 Mbps pro download a 18,2 Mbps pro upload. V průměru se pak stahoval data rychlostí 33,4 Mbps, což je sice zhruba desetina standardem avizované rychlosti, přesto je to však více než třicetinásobek toho, co je dnes dostupné na našem území přes technologii UMTS/HSPA. [4]

Norsko a Švédsko následovaly ve výstavbě nových sítí i další země. LTE se tak dočkali uživatelé v Polsku, Uzbekistánu či Německu. Údaje z loňského října hovoří o plánech k výstavbě LTE u více než 100 operátorů z 41 zemí světa.

V České republice je však situace tradičně o něco složitější, neboť i budování UMTS sítí našim operátorům trvalo o dost déle nežli zbytku světa. Zatímco za hranicemi se tedy uživatelé pomalu začínají těšit vysokým rychlostem LTE, tady operátoři s velkou slávou konečně začínají intenzivněji budovat UMTS sítě, k jejichž výstavbě získali (s výjimkou Vodafone Czech Republic) licence již před deseti lety. Jedinou výhodou s tímto chováním spojenou je fakt, že aktuálně stavěné 3G vysílače jsou již připravené ke snazšímu přechodu právě na LTE. [4]

K celé situaci ohledně sítí čtvrté generace se na sklonku roku 2010 vyjádřil například tiskový mluvčí Vodafone Czech Republic Miroslav Čepický poté, co byl tázán redaktory serveru MobilMania.cz:

> *„V současné době testujeme LTE ve vybraných zemích skupiny Vodafone (například Německo, Španělsko) a podle dosažených výsledků se bude odvíjet načasování LTE v ČR. Spuštění LTE v ČR bude záviset na mnoha faktorech. Jedním z nich je i proces přidělování vysílacího spektra, o kterém bude rozhodovat Český telekomunikační úřad.“*

Obdobně reagovali i zástupci dalších dvou mobilních operátorů na trhu. Příliš naděje na brzké spuštění LTE v našich končinách tato tvrzení tedy nepřinášejí.

K otázkám budování LTE se rozhodla postavit čelem Evropská komise, která se v květnu 2010 vyjádřila ve smyslu podpory rozhodnutí nabídnout operátorům k provozu této nové technologie frekvence uvolněné ukončením analogového televizního vysílání.

V souladu s uvedeným návrhem se o takovém řešení uvažuje i v České republice. Jednalo by se o frekvenci 800 MHz a jako hlavní výhoda se jeví nižší náklady na výstavbu právě díky této frekvenci. Dosah signálu z BTS by byl totiž větší, nebylo by tedy třeba rozmisťovat takové množství vysílačů jako v případě vyšších frekvenčních pásem.

V neposlední řadě je pak možné zmínit také technologii WiMAX (Worldwide Interoperability for Microwave Access), jež má však blíže k bezdrátovým sítím wi-fi, nežli k mobilním telekomunikačním sítím.

Oproti svému mladšímu sourozenci by WiMAX měl nabídnout dosah až 70 km v otevřeném prostoru (reálně tedy až několik desítek kilometrů) a rychlost dosahující až 70 Mbps.

U nás již Český telekomunikační úřad (ČTÚ) přidělil WiMAXu frekvence, a to 3410-3480 a 3510-3580 MHz. Takto by neměl kolidovat s klasickým wi-fi. Zároveň se ani nepočítá za jeho konkurenta, spíše by se měly tyto dvě technologie doplňovat. [5]

2 Technická řešení a bezpečnost

V předchozí kapitole jsme si blíže představili nejdůležitější mezníky v historii mobilních telekomunikací a také technické standardy v této oblasti využívané. V další části se zaměříme zejména na to, jak je řešeno zabezpečení dat, jež v těchto sítích každým dnem přenášíme. Rizika jejich odposlechu a případného zneužití totiž mohou být v mnoha případech značná.

Konkrétně se budeme věnovat hlavně dvěma standardům. Nejprve se pokusíme osvětlit bezpečnostní řešení v oblasti GSM, dále pak změny, které v této problematice přišly s nástupem sítí třetí generace. Záměrně opomeneme standard NMT, neboť je již neaktuální a na území naší země nevyužívaný. Zabývat se nebudeme ani LTE, neboť jako technologie spíše vzdálenější budoucnosti příliš nekoresponduje s cílem postihnout aktuální stav dané problematiky v rámci České republiky.

2.1 Zabezpečení GSM

Bezpečnost v rámci systému GSM můžeme rozdělit do dvou základních skupin. Na jedné straně se jedná o ověření totožnosti uživatelovy, mobilní stanice a karty SIM, na straně druhé pak jde o proces, v jehož rámci probíhá samotné šifrování dat přenášených v síti. V každém případě je účelem zabránit v systému GSM (ostatně obdobně jako i v jiných telefonních sítí) nejen odposlechu, ale také třeba zneužití telefonu ztraceného či odcizeného, potažmo volání na cizí účet.

2.1.1 Proces autentizace

Každý uživatel má přidělen jedinečný identifikátor známý pod zkratkou IMSI (International Mobile Subscriber Identity). Tento se skládá ze tří základních částí, jež jednoznačně identifikují zemi, mobilní síť a konkrétního uživatele. IMSI je uložen na kartě SIM a spolu s dalšími údaji taktéž v registru HLR (Home Location Register) v síti mobilního operátora. [24]

SIM (Subscriber Identity Module) je čipová karta, kterou dnes zná prakticky každý. Původně měla velikost klasické platební karty (85 x 54 mm), postupně však docházelo k jejímu zmenšování. Nejprve na velikost tzv. mini-SIM (25 x 15 mm), kterou dnes využívá většina mobilních telefonů, nejnověji pak dokonce na velikost mikro-SIM (15 x 12 mm), se kterou přišel jako první mobilní telefon iPhone 4 a jejíž rozšíření do dalších mobilních zařízení můžeme v nejbližších letech jistě očekávat. Firma Apple se však zároveň snaží o to, aby do budoucna byla fyzická forma karty SIM zcela opuštěna. V jejich podání by se celá věc měla tak, že čip SIM by byl obsažen již v telefonu, zákazník by si zařízení koupil přímo od výrobce a online by si vybral poskytovatele služeb, který by mu vyhovoval. Zatím však s tímto modelem narazili na velký odpor operátorů, kteří by tak prakticky přišli o zisky z prodeje telefonů a stali by se pouhými poskytovateli služeb. Do budoucna tedy můžeme jen odhadovat, jak se celá situace vyřeší. [16; 22]

Nyní již víme, co je to karta SIM a také to, že je na ní obsaženo jedinečné číslo IMSI. Pojďme se tedy podívat na to, co se stane po prvním, nejběžnějším kroku mobilního uživatele, tedy ve chvíli, kdy zapneme telefon. Po tomto úkonu dojde k tomu, že se mobilní stanice pokusí navázat spojení s mobilní sítí. Koná tak právě prostřednictvím již zmíněné karty SIM, jež kromě IMSI obsahuje také tajný šifrovací 128bitový klíč, který bývá označován jako „Ki“, dále autentifikační algoritmus A3 a algoritmus pro generování šifrovacího klíče zvaný A8 (A3 a A8 bývají často pro zjednodušení popisovány souhrnně jako algoritmus A38). V obou případech se jedná o symetrické proudové šifry, které nejsou nikterak standardizovány a každý telekomunikační operátor tak může použít vlastní algoritmy A3 a A8. Obě šifry jsou tajné, což v sobě skrývá zásadní nevýhodu, jíž je nemožnost jejich bližšího prozkoumání.

Vraťme se však zpět k procesu autentizace, tedy do momentu po zapnutí telefonu. Jedná se o okamžik, ve kterém se přístroj pokusí o přihlášení do mobilní sítě. Pro úspěšné vykonání tohoto úkolu si vybere vhodnou BTS stanici (zjednodušeně řečeno můžeme říci, že se jedná v podstatě o vysílač mobilního signálu, jak si jej představí běžný uživatel), této stanici odešle identifikační číslo SIM karty IMSI. Síť GSM následně vygeneruje náhodné

číslo (128bitové), jež obratem odešle zpět do telefonu. Telefonní přístroj v tuto chvíli využije svého tajného klíče (Ki) a zmiňovaného algoritmu A3. Za jejich pomoci obdržené číslo zašifruje a odešle zpět vybrané základnové stanici BTS. Trik však spočívá v tom, že tato stanice si udělala úplně stejný výpočet (v registru sítě se nachází také klíč Ki) a zašifrované číslo, jež získala od mobilního telefonu, porovná se svým vlastním výsledkem šifrování. Pokud v tomto okamžiku dojde k úspěšnému ověření, že se jedná o totožná čísla, považuje síť tuto kartu SIM za autentizovanou.

V následujícím okamžiku se dostává ke slovu další část šifry A38, jíž je výše zmíněný algoritmus A8. Obě strany procesu (tedy karta SIM i základnová stanice BTS) provedou v této chvíli další výpočet z již daného náhodně vygenerovaného čísla pomocí tohoto druhého algoritmu a vypočítají tak další šifrovací klíč. Ten je od tohoto momentu využíván při šifrování libovolné komunikace, ať už se jedná o přenos směrem telefon-síť či naopak síť-telefon. Samozřejmě se však jedná o tvrzení lehce zjednodušené, avšak k pochopení problematiky dostačující. Ve skutečnosti si telefon společně se sítí z bezpečnostních důvodů ustanoví čas od času klíč nový, jedná se však o naprosto stejný postup a odstup mezi těmito změnami je natolik dlouhý, že můžeme tuto skutečnost pro naše účely v podstatě přehlédnout. [23]

Celý výše popsaný proces by však nebyl možný bez mnohem triviálnější záležitosti, jíž je ověření totožnosti samotného uživatele karty SIM. Toto probíhá, jak mnohé jistě napadne, pomocí zadání číselných kódů PIN (Personal Identification Number, Osobní identifikační číslo) a PUK (PIN Unlock Key, volně přeloženo jako Kód pro odblokování kódu PIN).

Uživatel má po zapnutí telefonu (pokud tuto možnost ochrany nevypnul v nastavení své mobilní stanice) tři možnosti zadání čísla PIN (pro případ chyby). Jedná se numerický o kód, který dle jeho technické specifikace může mít 4 až 12 míst, pro pohodlné užívání se však doporučuje užití maximálně šesti číslic. V případě, že si uživatel svůj PIN nepamatuje, či pokud jej třikrát zadá špatně, přichází na řadu PUK. Jedná se o osmimístný kód, k jehož zadání má uživatel dokonce deset možností. Po vložení správné kombinace je možná změna zapomenutého PIN. Někdy se uživatel může setkat také s kódy PIN 2 a

PUK 2, které fungují na stejném principu a které obvykle slouží k zabezpečení nejrůznějších osobních nastavení v telefonu. Nicméně vraťme se ke kódu PUK. Pokud uživatel ani po deseti pokusech toto číslo nezadá správně, dochází k znehodnocení SIM karty a v takovém případě samozřejmě nedojde k procesu autentizace uživatele v síti.

V případě bezproblémového ověření totožnosti uživatele karty SIM dochází ještě k ověření totožnosti daného mobilního telefonu. Tento proces využívá výrobního čísla telefonu IMEI (International Mobile Equipment Identity). Jedná se o patnáctimístné číslo skládající se ze čtyř částí – kódu země, kódu výrobce, sériového čísla konkrétního telefonu a závěrečné cifry využívané pro kontrolní součet. IMEI je uloženo hned na dvou místech. Jednak samozřejmě přímo v telefonu (můžeme jej zobrazit zadáním kódu *#06# na klávesnici telefonu), dále potom v registru EIR (Equipment Identity Register, Registr mobilních stanic). Po ověření karty SIM tedy dochází k ověření totožnosti telefonu. IMEI je porovnáno s údaji z registru a následně zařazeno do jednoho z trojice seznamů. Může se jednat o tzv. white list, black list či grey list. [21]

Do bílého seznamu (white list) jsou zařazeny veškeré mobilní stanice, jimž je přístup povolen bez jakýchkoliv omezení. Jedná se tedy o bezproblémové stanice. Druhý jmenovaný seznam je pravým opakem.

Black list totiž zahrnuje všechny mobilní telefony, jež byly nahlášeny jako ukradené. V minulosti tento seznam využívala v České republice jen společnost Eurotel a v případě krádeže a jejího nahlášení tak došlo k tomu, že telefon byl dále nepoužitelný jen v této síti. Dnes však již black list využívají všichni naši operátoři a data navíc navzájem sdílí, proto je jeho využití mnohem účinější. Neradujme se však předčasně. Zloději již přišli na to, jak IMEI v telefonu přepsat, tudíž do budoucna je role black listu nepříliš významná.

Posledním zmíněným je tzv. šedý seznam (grey list). V tomto případě se jedná o výčet telefonů, u nichž existuje podezření, že byly zcizeny či ztraceny, nebylo však ještě zažádáno o jejich zařazení do black listu. Takovýto telefon

bude v síti fungovat, ale v okamžiku jeho přihlášení do sítě je operátor upozorněn, že v jeho síti funguje podezřelá mobilní stanice. [18]

Již na začátku této kapitoly jsme si ujasnili, že bezpečnost v sítích GSM se dělí na dvě hlavní skupiny, tedy na jedné straně ověření totožnosti uživatelovy, mobilní stanice a karty SIM a na straně druhé samotné šifrování přenášených dat. Nyní se tedy podíváme na druhou zmiňovanou část tohoto procesu.

Dosud víme pouze o algoritmu A38 tvořeném algoritmem A3, sloužícím jako nástroj pro autentizaci karty SIM, a A8, který má na starosti generování takzvaného relačního klíče.

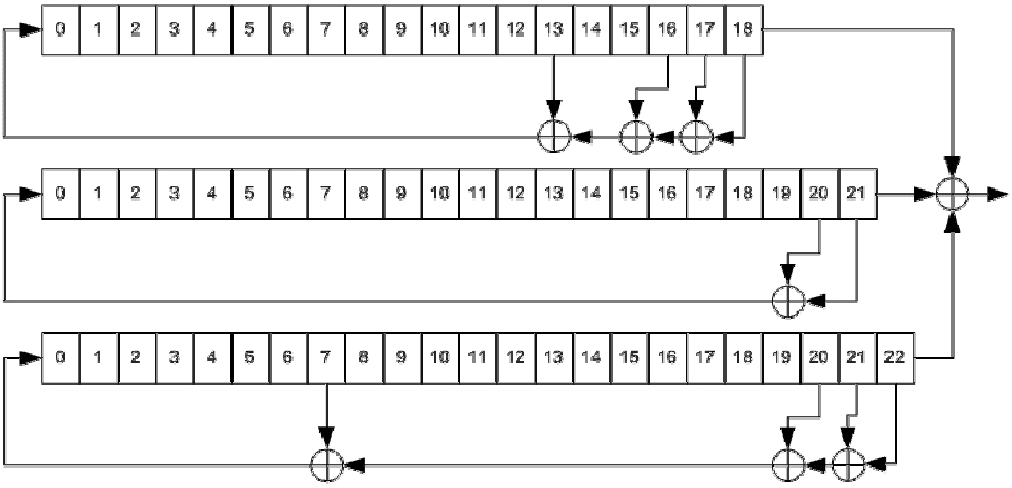
Právě relační klíč je využíván také šifrou A5, která zajišťuje v podstatě veškeré další šifrování v přenosu informací v mobilních sítích. Tuto šifru se tedy nyní pokusím více přiblížit.

2.1.2 Šifra A5

Jak již bylo řečeno, šifra A5 slouží k samotnému šifrování přenášených dat. Existují čtyři různé modifikace této šifry, přičemž veškeré současné mobilní stanice by ideálně měly podporovat (a tedy umět využívat) všech těchto variant, ať už se jedná o modifikaci A5/0, A5/1, A5/2 či nejnovější A5/3. Představme si však tato řešení postupně. [23]

Nejméně využívanou verzí šifry A5 je modifikace A5/0, která zkrátka a jednoduše v podstatě téměř nešifruje a je určena hlavně pro takzvaně „problematické“ země, jako například Irák.

Pravým opakem k verzi A5/0 pak měla být varianta A5/1, jež v době svého uvedení nabízela prakticky nejkvalitnější šifrování (princip šifry A5/1 na obrázku č. 5). S touto verzí jsme se mohli setkat a dodnes setkáváme třeba i u nás v České republice. Jedná se o proudovou 64bitovou šifru s veřejně známým číselným rámcem dlouhým 22bitů, která byla v některých zemích úmyslně oslabena tím, že posledních osm až deset pozic bylo obsazeno nulami a její efektivní délka se tak snížila na 54 - 56 bitů.



Obr. 5

Existují však ještě další dvě varianty. První z nich je verze A5/2. Jedná se o značně oslabenou verzi řešení A5/1. Rozdílem mezi těmito šiframi je fakt, že A5/2 záměrně ignoruje některé bity šifrovacího klíče a tímto se dostává k efektivní délce pouze 40 bitů. Původní určení této šifry bylo v době vzniku GSM standardu pro země bývalého východního bloku.

Zatím posledním řešením je šifra A5/3 (zvaná též Kasumi), jež je na rozdíl od své předchůdkyně založena na silnějším, 128bitovém šifrování a která měla svoji již značně překonanou předchůdkyni nahradit a stát se nevyužívanějším šifrovacím algoritmem světa. V současnosti ji využívá na 1,2 miliardy mobilních zařízení. Tato šifra je však využívána až v sítích 3G (v této části ji tedy uvádím jen proto, aby byl výčet kompletní), kde je určena pro kódování přenášeného internetového provozu, nikoliv pro telefonování. [27]

Pokud by si však měl uživatel po přečtení předchozích řádků myslet, že informace, které svěřuje síti prostřednictvím svého mobilního telefonu, jsou v naprostém bezpečí, rád bych jej vyvedl z omylu.

Je pravdou, že algoritmus A5 byl po velmi dlouhou dobu jedním z nejpřísněji utajovaných algoritmů. Každý jedinec, jenž byl s touto šifrou seznámen, musel nejdříve podepsat smlouvu, v níž se zavazoval k doživotní mlčenlivosti. V tomto případě šlo zejména o vědce, pracovníky vývoje mobilních telefonů, inženýry a další. V roce 1994 však bohužel veškeré utajení padlo, a to díky obyčejnému lajdáctví britské společnosti BTT, jež

zapomněla dát tuto smlouvu podepsat doktoru Shepherdovi, který okamžitě této chyby využil a celý algoritmus prezentoval světu na své přednášce. [30]

Ani přes snahy britské tajné služby, jež měla v úmyslu uvalit na celou přednášku embargo, se bohužel informace utajit nepodařilo. Než mohlo k uplatnění embarga dojít, popis celého algoritmu stačil uniknout do prostředí Internetu, odkud se dále rozšířil do celého světa.

Právě v tomto momentu leží počátek snah, jež postupně dospěly až k prolomení šifry A5/1, což bylo dlouho nemyslitelné a o čemž odborné časopisy ve svém bláhovém přesvědčení psaly jako o nereálném. V roce 2010 pak byla prolomena také zmiňovaná šifra A5/3, určená pro sítě 3G. Vývoji této problematiky bude věnována jedna z dalších kapitol. [17]

2.2 Zabezpečení UMTS

S nástupem sítí třetí generace, v případě České republiky tedy UMTS, se situace týkající zabezpečení mobilních telekomunikací samozřejmě zlepšila. Úroveň ochrany přenášených dat je vyšší zejména proto, neboť šířka pásma této sítě dovoluje šifrovat hovory bez dopadu na kvalitu služby či rychlost přenosu dat. S čím dál větším využitím internetových služeb, kdy uživatelé prostřednictvím této sítě přenášejí stále objemnější množství dat v mnoha případech velmi citlivých na zneužití (údaje internetového bankovnictví apod.) je toto samozřejmě nezbytné.

Jak poznamenává Rita Pužmanová ve své knize Bezpečnost bezdrátové komunikace, bezpečnostní prvky sítí UMTS lze rozdělit do čtyř skupin, a to: utajená identita účastníků (uživatelů sítě), autentizace účastníků, přenositelný modul SIM a samotné šifrování přenosu. [25]

2.2.1 Identita uživatele

Co se identity uživatele a jejího utajení týče, můžeme tento problém rozdělit v rámci UMTS sítí hned do tří skupin. Jednak dochází k utajení identity samotného uživatele, neboť tuto identitu není možné odposlechnout

na rádiovém přístupovém spoji, dále obdobně není možné zjistit místo, na kterém se uživatel vyskytuje a také služby, jež se váží ke konkrétnímu účastníkovi sítě. [25]

2.2.2 USIM a proces autentizace

Další dvě výše jmenované složky zabezpečení UMTS spolu úzce souvisí. Řeč je o procesu autentizace a kartě SIM, neboť právě tato karta, obdobně jako v případě GSM je k autentizaci využívána. Ačkoliv se jedná o kartu SIM, často bývá chybně označována jako USIM. Ve skutečnosti je USIM označením pouhé aplikace na modulu SIM, jež umožňuje přístup do UMTS sítí.

Pro samotný proces autentizace je využíváno několik různých čísel či klíčů:

- 128 bitové náhodné číslo RAND
- autentizační odpověď RES
- očekávaná odpověď XRES
- 128bitový šifrovací klíč Ki
- 128bitový šifrovací klíč CK
- 128bitový klíč integrity IK

RAND je číslo, jež mobilní stanice využije pro výpočet čísla RES a klíčů CK a IK. RAND je takto využit ve spolupráci s klíčem Ki, který je uložen jak na kartě SIM, tak v autentizačním centru sítě. Tento klíč se nikdy nepřenáší.

Při pokusu o přihlášení do sítě mobilní zareaguje mobilní stanice na výzvu k autentizaci odesláním odpovědi RES, jež vznikla právě využitím čísla RAND a klíče Ki. V autentizačním centru se pak toto číslo porovná s očekávanou odpovědí XRES, která byla vypočítána obdobným způsobem. Pokud čísla odpovídají, došlo k autentizaci USIM. Následně jsou využívány klíče CK a IK. CK slouží k šifrování u uživatele i v síti, IK je pak určen k zajištění integrity přenášených zpráv. [20]

2.2.3 Šifra A5/3

Do této chvíle jsme hovořili o autentizaci. Data, která jsou přenášena po úspěšném dovršení tohoto procesu, jsou šifrována pomocí algoritmu Kasumi, nazývaného též A5/3 (byl zmíněn již v sekci věnující se bezpečnosti GSM). Tato šifra využívá 128bitový klíč, což znamená zásadní zlepšení zabezpečení přenášeného obsahu komunikace. Je však nutné podotknout, že tato šifra je využívána pouze pro přenášená data, nikoliv pro hlasovou komunikaci, u níž je stále užívána primárně starší varianta algoritmu A5 (viz kapitola 2.1.2). [29]

Zatímco Pužmanová ještě v roce 2006 hovoří o tom, že „se uživatelé nemusí obávat používat širokopásmovou bezdrátovou komunikaci ani pro citlivá data“, dnes už je situace opět jiná. Na počátku roku 2010 totiž média informovala o tom, že šifra A5/3 byla úspěšně prolomena. Jedná se o zásadní informaci, neboť mnoho uživatelů prostřednictvím mobilního telefonu stále častěji přistupuje například ke službám mobilního bankovnictví a přenáší tak velmi citlivá data. O to více šokující je fakt, že k prolomení bezpečnostních opatření stačil vědcům z izraelského Weizmannova ústavu obyčejný notebook vybavený dvoujádrovým procesorem a operačním systémem Linux. [17]

Celkově vývoj bezpečnosti mobilních telekomunikačních sítí shrnuje trefně dále ve své knize opět Pužmanová:

> *„Bezpečnost ani u tak technicky vyspělého typu sítě jako 3G nemůže být stoprocentní. To by totiž vyžadovalo, aby výrobci pracovali na základě bezpečnostních norem a provozovatelé implementovali bezpečnostní opatření, ale také aby se eliminoval lidský faktor, který s sebou přináší největší bezpečnostní rizika.“*

Vzhledem k zmiňovanému incidentu vázájícímu se ke společnosti BTT, který byl zmíněn výše, nelze s tímto tvrzením než souhlasit.

2.3 Hlasové kodeky

Do této chvíle jsme si již představili způsoby zabezpečení aktuálně využívaných mobilních sítí a také jsme si nastínili vývoj jednotlivých telekomunikačních technologií, včetně informací o maximálních současných rychlostech přenosu dat v nich možných.

K této problematice se váže také otázka hlasových kodeků v mobilních telekomunikacích využívaných. Právě na těchto kodecích totiž závisí, jak datově náročný bude přenos hlasu. To samozřejmě ovlivňuje kvalitu využití jednotlivých mobilních sítí, neboť jejich kapacita pro přenos dat (tedy i hlasu) je omezená a tento problém je třeba řešit.

Nejprve se tedy ve stručnosti pokusím vysvětlit základní fakta, která se ke kodekům váží.

Slovo kodek je složeninou dvou výrazů – kodér a dekodér (z anglického codec: coder, decoder). Jedná se o zařízení či počítačový program, jenž slouží k převedení analogového signálu na digitální a také opačně, tedy ke zpětnému převedení digitálního signálu, v našem případě na řeč. [19]

Kodeků existuje celá řada, pro naše účely jsou však důležité ty, které jsou využívány k přenosu zvuku.

S tvorbou kodeků jsou spojeny dva hlavní požadavky, které se vzájemně v podstatě vylučují. Na jedné straně je požadována co nejvyšší kvalita přenášeného hlasu, na straně druhé pak co nejmenší objem přenášených dat. Vyšší kvalita však s sebou logicky nese vyšší datový objem. Z toho důvodu je tedy tvorba zvukových kodeků snahou o nalezení co nejlepšího kompromisu, přičemž mobilní telekomunikace se od počátku snažily spíše o co nejvyšší kvalitu hovorů.

Postupně tak vzniklo několik různých řešení. Prvním z nich byl kodek zvaný Half-rate, který umožnil přenos hlasu při objemu dat 5,6 kbps. Jeho nástupcem pak byl Full Rate, jenž využíval 13 kbps pro přenos samotného hlasu a dalších 9,8 kbps pro korekci případných chyb, dohromady tedy šlo o 22,8 kbps. Již tyto kodeky měly jednu zásadní a pro telekomunikační oblast

velmi přínosnou vlastnost – umožnily rozpoznat důležité části audiostopy a na základě tohoto rozlišení přidělit takto vybraným částem vyšší prioritu, což následně znamenalo také lepší zajištění signálu. [28]

Evolucí kodeku FR (Full-rate) pak bylo v roce 1997 řešení zvané EFR (Enhanced Full-rate), jež umožnilo zlepšení kvality přenášeného zvuku při zachování šířky pásma signálu. Použitelná rychlost měla hodnotu 12,2 kbps – nároky na datovou kapacitu sítě se tedy dokonce ještě snížily. Mnozí mohou mít ještě dnes v paměti, jak se zavedením této technologie naši mobilní operátoři chlubili. Společnost EuroTel dokonce v roce 1999, kdy s EFR přišla na trh, přinesla vlastní označení SuperSound. Redakce internetového magazínu Mobil.cz rozdíl mezi FR a EFR přirovnala k rozdílu mezi zvukem vinylové desky a kompaktního disku. [26]

EFR však není koncem evoluce hlasových telekomunikačních kodeků. Zatím posledním masově užívaným zástupcem této oblasti je AMR (Adaptive Multi-Rate Speech Codec), jenž se prosadil s nástupem sítí třetí generace.

Hlavní výhodou AMR je flexibilita objemu přenášených dat. Každý hovor, v němž je AMR uplatněn, je rozdělen do úseků dlouhých vždy 5 ms. Každý z těchto úseků pak může být přenášen jinou rychlostí (12,2 kbps, 10,2 kbps, 7,95 kbps, 7,4 kbps, 6,7 kbps, 5,9 kbps, 5,15 kbps či 4,75 kbps), jelikož telefon využívající AMR by měl být schopný rozpoznat, které části hovoru jsou důležité.

Pokud tak například jedna strana mlčí, telefon nepřenáší v podstatě nic. Tato funkce bývá označována jako DTX (Discontinuous Transmission). Podobnou funkcionalitu měly už předcházející kodeky, ale až u AMR je na ni kladen větší důraz a je více využita. Jejími hlavními přínosy jsou úspora baterie mobilního telefonu a hlavně kapacity mobilní sítě. Následně pak díky tomu může být odbaveno více hovorů a nedochází k případnému přetížení sítě. [19]

S DTX je spojena také zkratka VAD (Voice Activity Detection). Jelikož AMR díky DTX občas nepřenáší žádný zvuk, mohl by se uživatel cítit

zvláštně, kdyby slyšel úplné ticho. Proto VAD přímo v telefonu generuje tichý šum tak, aby si zákazník sítě myslel, že se jedná o součást hovoru.

AMR je současným maximem, které jsou naše mobilní telekomunikační sítě schopny využít. Do budoucna však samozřejmě můžeme očekávat další rozvoj této oblasti, neboť se stále rychlejšími sítěmi budou pravděpodobně zákazníci klást čím dál větší důraz i na kvalitu hovorů. [28]

3 Bezpečnostní rizika

V předchozích sekcích jsme si osvětlili vývoj mobilních telekomunikačních technologií a také řešení zabezpečení dat v nich přenášených. V této části si představíme možná rizika, která uživatelé mobilních telefonů mohou čekat.

Existují v podstatě tři hlavní hrozby, kterým může být uživatel při běžném užívání mobilní stanice vystaven.

První souvisí s odcizením samotného mobilního telefonu, kdy jsou v ohrožení zejména data v přístroji obsažená, logicky však nikoliv data přenášená při hovoru. V tomto případě je řešení poměrně jednoduché. Důležité je chránit telefon již dříve zmiňovaným kódem PIN, který mnohé přístroje umožňují doplnit ještě dodatečným bezpečnostním kódem, jenž bývá vyžadován vždy, když se uživatel pokusí o odemčení klávesnice telefonu. Tento kód může být v éře chytrých mobilních telefonů zadáván například i ve formě obrázku kresleného prstem na plochu displeje.

Problém však může způsobit fakt, že když už ke krádeži dojde, ne všechna data musí být nutně uložena přímo v paměti telefonu. Mnoho dnešních zařízení totiž umožňuje ukládat data také na paměťové karty, jejichž obsah není nikterak obtížné zobrazit; kartu stačí jednoduše vyjmout z telefonu a vložit do čtečky paměťových karet.

Řešení takové situace se však dnes již také nabízí. Jedním z nich je třeba služba společnosti HTC, jež u svých nejnovějších přístrojů umožňuje v případě krádeže zadat telefonu na dálku (přostřednictvím sítě Internet) požadavek na kompletní vymazání dat, tedy v podstatě na změnu paměti do tzv. továrního nastavení. [35]

Další hrozbou po odcizení telefonu může být tzv. klonování SIM karty. Jedná se v podstatě o proces, kdy je obsah této karty nakopírován na jinou fyzickou kartu a jejím prostřednictvím využíván. Riziko je zřejmé – podvodník, jenž kartu naklonoval, může volat na cizí účet a způsobit tak pravému majiteli karty značnou finanční škodu, kterou pak postižený

s největší pravděpodobností bude muset uhradit, ačkoliv sám danou útratu nezpůsobil. [38]

V současné době však klonování již nepředstavuje zcela aktuální problém. Uživatele se může dotknout pouze tehdy, pokud má kartu SIM vyrobenou do roku 2002, neboť tehdy se začal využívat jiný typ karet, který této praktice zamezil. Mít devět let starou kartu SIM je dnes jev již dost vzácný, neboť už jen kvůli fyzickému opotřebování s nejvyšší pravděpodobností dojde k její výměně mnohem dříve, případně může také zákazník měnit mobilního poskytovatele služeb (operátora) – v tom případě dostane kartu novou zcela automaticky. Na výměnu karty má uživatel u našich operátorů bezplatný nárok.

Pojďme si však i přesto říci, jak ke klonování karet docházelo, případně může stále docházet. K provedení tohoto nám postačí jeden z mnoha přístrojů, které se dají na Internetu zakoupit (příklad na obr. č. 6). Většinou již nejsou o mnoho větší než klasický USB flash disk. Do tohoto přístroje vložíte SIM kartu, ten z ní vyčte IMSI a Ki, případně také telefonní seznam či zprávy SMS. Veškeré potřebné informace je pak schopný přenést na „prázdnou kartu“, kterou taktéž není problém zakoupit online. Na takovou kartu je pak možné nahrát data až deseti karet SIM, tudíž ji pak je možné používat (samozřejmě ne ve stejnou dobu) jako až deset telefonních čísel. [34]

Obr. 6

Klonování karet SIM vždy neznamenalo jen nechtěnou operaci. Mnohdy toto prováděli uživatelé i z vlastní iniciativy. Docházelo k tomu zejména na přelomu tisíciletí, když chtěl uživatel používat stejné telefonní číslo například jak v autotelefonu, tak ve svém klasickém mobilním telefonu. Postupně pak tomuto požadavku vyšli vstříc i operátoři a umožňili pořízení dvou „totožných“ karet také oficiální cestou. Za všech okolností však platila jedna

podmínka – v provozu (na příjmu) mohla být vždy jen jedna z těchto karet. To stejné platí i pro neoficiálně naklonované karty SIM.

Poslední z trojice nejzásadnějších hrozeb je prolomení šifrování mobilních hovorů, využívajících algoritmu A5, a jejich případný odposlech.

Ačkoliv algoritmus A5 není zrovna jedním z nejjednodušších, byl roku 2000 prolomen. Veškerá média o tomto informovala s dostatečně bulvárním podtónem paniky a snažila se všechny přesvědčit, že veškerá bezpečnost padla. Jak to tedy ve skutečnosti s prolomením šifry A5 je?

Jak jsme si již řekli dříve, verze A5/0 je přímo čitelná a pro její prolomení není potřeba udělat vůbec nic. S šiframi A5/1 a A5/2 (dále jen A5) a jejich prolomením je práce samozřejmě podstatně více.

První informace o struktuře šifry vynesl do světa dříve zmiňovaný doktor Shepherd.

Úplné pokoření šifry A5 si však vzali na starost až odborníci z Weizmannova institutu v Izraeli. Tito specialisté využili v roce 1999 k nesnadnému úkolu naprosto běžné PC s pouhými 128 MB operační paměti a dvěma pevnými disky, přičemž každý z nich měl kapacitu 73 GB. Nejednalo se tedy o žádné extrémně technologicky výkonné zařízení. Z jejich řešení víme, že tím nejzákladnějším krokem, který je k danému úkolu zapotřebí, je získání alespoň dvouminutového záznamu dat v šifrované i nešifrované podobě. Následně počítač v době nepřesahující jednu sekundu (rok 2001, dnes bude potřebná doba pravděpodobně mnohem kratší) využije útoku hrubou silou k získání klíče, jehož používá šifra A5. Posléze je tedy umožněno automatické dešifrování veškerých dat, jež budou dále přenášena – telefonní hovory, krátké textové zprávy, datové přenosy... Zkrátka všechna uživatelova data. [32]

Výše popsaný postup může znít až bláhově jednoduše. Počítač s tak nízkým výkonem není v dnešní době ničím nedostupným. Problém však vězí ve dvou minutách dat, jež k prolomení šifry potřebujeme.

Tím nejmenším problémem je získání dat v podobě nezašifrované. Pokud bychom obětí našeho experimentu nebyli my, ale někdo jiný, můžeme například zkusit donutit dotyčnou osobu, aby si prostřednictvím svého mobilního telefonu stáhla například javovou aplikaci takové velikosti, aby k jejímu stažení bylo zapotřebí alespoň dvouminutového stahování. Takto tedy můžeme vyřešit otázku nešifrovaných dat. Pokud se nám nepodaří takovýto postup, stále zde zůstává možnost nahrání obyčejného dvouminutového hovoru s danou osobou, a to za využití například takových triků, jako fingovaného průzkumu trhu, prodeje po telefonu, oznámení o výhře atd. [31]

Podstatně větším problémem bude získání zašifrovaných dat – jednoduše řečeno se jedná o odposlech komunikace, jež probíhá mezi mobilním telefonem a základnovou stanicí BTS. Zde sice nejde o nikterak nápadnou činnost, neboť se nikam nic nepřipojuje a ani se nemusíme přiblížit k telefonnímu přístroji, avšak musíme řešit problémy s přeskakováním nejen mezi různými frekvencemi, ale i mezi základnovými stanicemi BTS. Celý proces výrazně zjednodušují speciální zařízení zvané GSM scannery, jež se o celý tento proces postarají za vás a ve výsledku produkují pouze čistá získaná data. [33]

Další variantou pro možnost odposlechu komunikace je získání klíče Ki, a to přímo z karty SIM. Toto nelze uskutečnit přímo – Ki je však možné zjistit, a to provedením asi sto padesáti tisíc vhodně zvolených dotazů pro algoritmus A38. Toto se však týkalo opět hlavně starých karet SIM (takto pracovala i zařízení pro klonování karet), a proto mobilní operátoři na karty implementovali čítače, které kartu po asi 100 000 příkazech znehodnocovali. Dnes se již používá zcela jiný typ karet. [37]

V době prolomení šifry A5 odborníky z Weizmannova ústavu bylo zapotřebí získat otevřená i zašifrovaná data. Pokrok se však nezastavil, proto v roce 2008 dvojice hackerů (název, kde) představila zařízení, které dokázalo pasivně dešifrovat zachycené hovory v síti GSM. Zařízení mělo hovor dešifrovat během 30 minut a mělo být komerčně dostupné za pouhých 1000 dolarů, což vzhledem k možné hrozbě pro uživatele a možným benefitům pro

odposlouchávající stranu, není částka nikterak vysoká. Zároveň si zmiňovaná dvojice hackerů připravila i dražší a výkonější variantu zařízení – konkrétně se jednalo o přístroj, jež stejný úkon dokázal provést nikoliv za 30 minut, nýbrž již za 30 sekund. Cena již však byla značná – začínala na více než dvou stech tisících dolarů.

Ani to však nebyl konec pokusů o prolomení ochrany mobilních hovorů. Počátkem roku 2011 totiž světová média informovala o tom, že výzkumník Karsten Nohl ze Security Research Labs sídlící v Berlíně, předvedl na konferenci Chaos Computer Congress konané v témže městě, řešení operující s ještě lepším poměrem cena/výkon. Konkrétně mu stačil obyčejný telefon značky Motorola v ceně několika set korun se speciálně upraveným firmwarem (software telefonního přístroje), notebook s bezplatně dostupným softwarem a asi tři minuty času. [36]

Postup je zhruba následovný. Mobilní telefon obsahující modifikovaný firmware poslouží v síti jako zařízení pro vyhledání konkrétního uživatele, následně jsou získána hrubá data, ta jsou přenesena do notebooku, tam jsou pak crackovacím programem prolomena, a to během asi dvaceti sekund. Vzápětí je možné již začít přímo nahrávat odposlech telefonního hovoru. Celý postup Nohl na zmíněné konfreneci názorně předvedl, aby dokázal jeho funkčnost.

Aby byl vývoj útoků na šifru A5 popsán kompletně, je nutno podotknout, že v roce 2010 se podařilo prolomit také variantu A5/3, jež je určena pro sítě třetí generace, v našem prostředí tedy UMTS. Zde je však potřeba upozornit na zásadní rozdíl. Zatímco algoritmy A5/1 a A5/2, o kterých je řeč výše, již byly prolomeny kompletně, v případě řešení A5/3 se jedná o metodu, kdy je zapotřebí otevřených i zašifrovaných dat – ocitáme se tedy v podobné situaci, kde jsme byli s A5/1 a A5/2 v roce 1999 s odborníky z Weizmannova institutu. [17]

Dříve než přejdeme k následující kapitole, je třeba zmínit také to, že existují i další varianty, jak odposlechnout telefonní hovory.

První z nich je notoricky známou záležitostí. Řeč je o „štěnicích“. Takovéto zařízení se dá vmontovat přímo do mobilního telefonu, případně může být součástí speciálně upravené baterie stroj pohánějící. V obou případech se jedná o dodatečné zařízení, jež by se mělo projevovat rychlejším vybíjením baterie. V případě podezření na přítomnost odposlouchávacího zařízení je vhodné nechat si telefon zkontrolovat. Dnes již existuje řada firem specializujících se na tuto problematiku, případně může posloužit také patřičně vybavený servis mobilních telefonů.

Kromě „štěnic“ však existují také speciální zařízení, která dokáží odposlechnout hovor až na několik desítek metrů od přístroje. Zde je tedy nutná fyzická přítomnost takového zařízení v blízkosti volajícího. Technicky se jedná o vysoce citlivý mikrofon, patřičné technické vybavení a sluchátka na uších poslouchajícího jedince. [33]

4 Možná řešení

V předchozí kapitole jsem se pokusil představit možná rizika, kterým je uživatel mobilního telefonu vystaven a která ohrožují důvěrné informace, jež jeho prostřednictvím sdílí. V závěrečné sekci se pokusím představit možná řešení problému – tedy způsoby, kterými se uživatel mobilní stanice může bránit a svoje osobní data chránit.

V zásadě by se řešení dala rozdělit do několika hlavních skupin. První z nich tvoří hardwarová ochrana. V tomto případě se může jednat o tzv. kryptotelefony, tedy telefony s dodatečným šifrováním či o externí šifrovací zařízení, jež je možné připojit ke stávajícímu telefonnímu přístroji. Druhou skupinou jsou řešení softwarová. Zde je nutné zmínit nejrůznější aplikace pro tzv. chytré telefony (smartphones) s operačním systémem či pro telefony s podporou technologie Java, jež se o nadstandardní šifrování postarají. Poslední reálně použitelnou skupinou je pak oblast internetové telefonie, ať už se jedná o služby VoIP (Voice over IP, Volání přes internetový protokol) či o službu známou pod komerčním názvem Skype.

V předchozím odstavci jsem použil slovní spojení „reálně použitelná skupina“. Tento výraz jsem zvolil zcela úmyslně, neboť samozřejmě zbývá ještě nejméně jeden způsob, kterým lze svá data bezpečně ochránit, a to s účinností 100 %. Touto možností samozřejmě myslím vůbec citlivé informace nesdílet prostřednictvím mobilního telefonu. Je to ovšem řešení nepraktické a krajně úsměvné, neboť málokdo je dnes již schopen se takto zařídit a přenášet veškerá data osobně. Z toho důvodu tedy budu dále rozvádět jen dříve zmiňované varianty ochrany.

Jak již bylo řečeno, jednou z variant možného zabezpečení přenášených informací je dodatečný software nainstalovaný do mobilního telefonu.

Příkladem takového řešení může být třeba aplikace zvaná CryptoCult od české firmy CircleTech, o níž v loňském roce informoval server iDnes.cz. Konkrétně tento program je určen pro chytré telefony vybavené operačním systémem Symbian, tedy většinu dražších modelů značky Nokia. Kromě nutnosti vlastnit odpovídající mobilní přístroj je požadavkem také stejné

řešení na druhé straně, jinými slovy obdobně softwarově vybavený příjemce hovoru. Aplikace se pak postará o dodatečné šifrování telefonního spojení, hovory tedy nebudou zabezpečeny jen klasickou ochranou sítí GSM. Je také nutno podotknout, že toto nadstandardní šifrování není přidáno do klasického telefonního hovoru, přenos hlasu spolu s dodatečnou šifrou probíhá prostřednictvím internetového připojení a využívá technologie SIP, tedy v podstatě internetové telefonie, o které bude ještě řeč dále. Tu CryptoCult zabezpečuje 256bitovým šifrováním. Jako zdroj náhodných dat k zašifrování konkrétních hovorů slouží digitální fotografie v bázi firmy, jež software vyvíjí. [44]

V každém případě je třeba počítat s tím, že kvůli dodatečnému šifrování trvá sestavení hovoru delší dobu a kvůli s tím související datové náročnosti je též zapotřebí rychlejších datových přenosů. V ideálním stavu by se mělo jednat o 3G či wi-fi, stačit by však mělo i EDGE. GPRS se nedoporučuje z důvodu zachování kvality. Zvuk hovorů by měl svojí úrovní odpovídat internetové telefonii.

Vhodné je zmínit také fakt, že CryptoCult umožňuje nejen šifrování hovorů, nýbrž také textového chatu či e-mailů. Umožněna je tedy vcelku komplexní mobilní komunikace.

Při spoustě výhod podobného řešení je však třeba zmínit také zásadní nevýhodu, kterou je v tomto případě cena. Licence pro právnické osoby, která se vztahuje až na třicet telefonních čísel, stojí 2 500 000 Kč a platí doživotně. Fyzické osoby si pak tutéž službu mohou pořídit za 3 000 Kč měsíčně, či za 60 000 Kč na rok pro dvě čísla.

Kromě takto komplexního řešení existují i specifičtější programy. Jako příklad můžeme uvést aplikaci SMS007 – taktéž z dílny CircleTechu, jež je určena většině mobilních telefonů podporujících programy psané v jazyce Java. I v tomto případě je nutné, aby bylo softwarové řešení shodné na obou koncích probíhající komunikace. Jak již název programu napovídá, dochází k šifrování pouze SMS zpráv, mobilní telefonní hovory aplikace nepokrývá. Co se bezpečnosti týče, je samotný program chráněn vstupním heslem. Zvláštní heslo má ovšem také každý uživatel, se kterým chce volající komunikovat. Na

tomto heslu je třeba se předem domluvit a bude vyžadováno při každém hovoru, a to na obou stranách telefonátu. Tvůrci doporučují nastavit heslo komplikované, ideálně využívající různých symbolů, čísel atp. V opačném případě je totiž možno využít tzv. "slovníkového útoku", kdy narušitel za pomoci počítače vyzkouší pro rozšifrování hovoru mnoho různých slov.

SMS007 využívá šifrování AES, jež bylo schváleno vládou USA jako vyhovující k ochraně citlivých informací. V neposlední řadě je pak vhodné zmínit, že v tomto případě se nejedná o řešení tak finančně náročné jako v případě aplikace CryptoCult – program SMS007 je dnes k mání za 250 Kč měsíčně, asi o dvě třetiny levněji než v době jeho uvedení. Odvrácenou stranou mince je však fakt, že SMS007 funguje pouze jako Javová aplikace a nepodporuje většinu novějších mobilních telefonů. V případě nutnosti využití dodatečného šifrování pro přenos krátkých zpráv tak nezbývá než zakoupit nějaký starší přístroj třeba v nějakém bazaru. [40]

Pokud si nevyberete na trhu šifrovacích aplikací pro mobilní telefony, máte možnost poohlédnout se po hardwarovém řešení. Zaujmout vás může třeba některý z tzv. kryptotelefonů. Jedná se o mobilní stanice speciálně upravené tak, aby bez nutnosti jakéhokoliv dalšího zařízení či instalovaného softwaru dokázaly telefonní hovory šifrovat (na obr. č. 7 příklad – zařízení Tripleton Enigma).

Obr. 7

Kryptotelefony původně používaly zejména armádní složky. Při vývoji odposlechu mobilních telekomunikačních sítí směrem k levnému a nenáročnému řešení však zájem o zabezpečení uživatelských informací roste; roste tedy také poptávka po kryptotelefonech, které díky tomu značně zlevnily. Zatímco v roce 2002 byl u nás v České Republice dostupný jen model společnosti Siemens zvaný TopSec, který stál zhruba 140 000 Kč a ještě nebyl pro každého (Siemens pečlivě zvažoval komu jej prodá), dnes se

obdobná zařízení dají sehnat již za cenu příliš nepřevyšující částky, jež jsou žádány za špičkové modely jednotlivých výrobců mobilních telefonů.

Každý model kryptotelefonu má jiné specifikace a využívá jiného typu šifrování. Společnou vlastností však je, že musí být stejně vybavena i mobilní stanice, které je z kryptotelefonu voláno. Šifrování je v tomto případě vkládáno přímo do telefonního hovoru a v případě pokusu o odposlech a prolomení ochrany sítí GSM uslyší odposlouchávající jen šum. [39]

Na Internetu se dají sehnat také nejrůznější externí zařízení, která se připojí k vašemu stávajícímu mobilnímu telefonu a dále se o šifrování postarají. Zjednodušeně by se tak dalo říci, že v podstatě váš obyčejný telefon promění v kryptotelefon. Takové řešení může být obsaženo třeba i v baterii mobilního telefonu.

V souvislosti se softwarovým řešením našeho problému již byl zmíněn pojem internetová telefonie. V případě programu CryptoCult se však nejednalo o klasickou VoIP telefonii, která dokáže zcela nahradit (dnes již nejen) pevné telefonní přípojky.

VoIP je technologie umožňující, jak již její název napovídá, volat přes Internet. K tomuto je nutné pouze to, aby obě strany byly vybaveny příslušným softwarem, reproduktorem a mikrofonem. Uživatel se pouze zaregistruje u jednoho z mnoha poskytovatelů, bude mu přiděleno telefonní číslo a dál už může přes VoIP volat dle libosti. Volání na jiná čísla v rámci služby VoIP je většinou zdarma, hovory na klasická telefonní čísla pak již bývají zpoplatněná. My se však dále klasickou VoIP zabývat nebudeme, neboť u této služby existuje obrovské množství poskytovatelů a velká většina z nich se kvalitnímu zabezpečení přenášených hovorů nikterak více nevěnuje. Toto řešení bych tedy dále nedoporučoval. [45]

U internetové telefonie však zůstaneme, jen se zaměříme na její jiný typ. Řeč je v tomto případě o službě Skype.

Skype je výtvorem dvojice pracovníků, kteří původně pracovali pro společnost Tele2, jež se ve více zemích (včetně České republiky) pokoušela konkurovat monopolním poskytovatelům pevných linek. Právě zde pánové

Niklas Zennström a Janus Friis získali svoje první zkušenosti z oblasti telekomunikačního průmyslu, které měli později zúročit.

Na úplném počátku stál jako inspirace program ICQ určený k tzv. instant messagingu (výměna textových zpráv v reálném čase mezi uživateli). Právě ten byl totiž založen na technologie P2P (Peer2Peer, volně přeloženo jako od uživatele k uživateli). Ta umožňuje, že data cestují přímo od jednoho uživatele k druhému, aniž by procházela a zdržela se v nějaké ústředně.

ICQ bylo pouhým začátkem, tehdy ještě nic nenasvědčovalo tomu, že by se přes P2P dalo přenášet objemnější množství dat. S tím jako první přišla služba Napster, kterou zejména studenti využívali ke sdílení hudby v mp3 v dobách, kdy tento formát zažíval svůj největší rozkvět. Napster nicméně brzy kvůli právním problémům byl nucen svoji činnost ukončit. Velmi rychle jej nahradila služba KaZaA s podobnou funkcionalitou, která byla vyvíjena právě zmíněnou dvojicí (Niklasem Zennströmem a Janusem Friisem) a jejich zaměstnanci.

Tímto projektem získali svoje první zkušenosti s využitím technologie P2P a odtud již tedy bylo blízko k nápadu, jež dostal jméno Skype. Jeho beta verze byla spuštěna roku 2003 s tím, že se snad budou uživatelé napojovat ke službě s lavinovým efektem, tedy že každý uživatel přivede několik svých známých. Tento předpoklad se splnil – po půl roce měl Skype již více než 6 milionů uživatelů, po roce překročil magickou hranici jednoho sta milionů stažení softwaru. V současnosti je využíván více než 75 miliony jedinečnými uživateli a od roku 2005 patří společnosti eBay provozující stejnojmenný internetový aukční portál. [42]

Dnes je Skype celosvětovým fenoménem, který umožňuje mnohem víc než pouhé telefonování. K němu totiž přibyly také konferenční hovory (komunikace více uživatelů ve stejnou dobu), videohovory, chatování či přenos souborů.

Skype také velmi dbá na bezpečnost komunikace probíhající jeho prostřednictvím. Jak již bylo řečeno v popisu technologie P2P, veškerá komunikace probíhá od uživatele k uživateli přímo. To odstraňuje možnost

odposlouchávat uživatele na ústředně. Společnost má také svoje 4 základní bezpečnostní pravida (Skype Security Policy):

1) Každý uživatel má jedinečné heslo.
2) Každý se před použitím programu musí ověřit zadáním uživatelského jména a hesla.
3) Uživatelé si při sestavování hovoru prokáží identitu tím, že se oba přihlásili k programu.
4) Komunikace je šifrována od uživatele k uživateli, bez prostředníků.

Každý uživatel tak při přihlášení ke Skypu pro sebe získává tzv. pověřovací list, který prokazuje jeho identitu.

Šifrování samotné komunikace pak využívá jak šifrování s pomocí veřejného klíče, tak i šifrování se symetrický klíčem. Pro přenos dat mezi uživateli je použita 256bitová varianta symetrické blokové šifry AES, pro výměnu AES klíčů pak 1536 až 2048bitové šifrování s veřejným klíčem RSA. [43]

Kvalita ochrany informací přenášených prostřednictvím Skypu je dokonce na takové úrovni, že údajně Národní bezpečnostní agentura Spojených států amerických známá pod zkratkou NSA vypsala odměnu ve výši několika miliard pro toho, kdo zabezpečení Skypu dokáže prolomit. [41]

Odposlouchávání Skypu totiž není ani zdaleka tak jednoduché jako „napíchnutí“ klasických GSM sítí. To komplikuje život zejména policii a naopak zpříjemňuje nejrůznějším podvodným živlům. Odposlech se sice dá soudně nařídit a v takovém případě pak Skype musí policii vyhovět, není to však tak snadné jako v případě sítí GSM, kdy už si dnes policie může odposlouchávat každého kdykoliv téměř jak se jí zachce.

Je však vhodné zmínit, že takto zabezpečené jsou jen hovory mezi uživateli Skypu. Pokud využijete služby SkypeOut (pro volání na běžná telefonní čísla) či SkypeIn (bude vám přiřazeno lokální číslo; z běžných telefonních přístrojů se pak lidé dovolají vám na Skype), vězte, že policie může hovor odposlouchávat na druhé straně hovoru.

Nakonec bych měl vysvětlit, proč je vůbec internetová telefonie či přímo Skype zahrnutá v řešeních šifrování mobilních hovorů. Skype dnes již není pouze počítačovým programem. Zavoláte si s ním totiž i v rámci mobilních telefonů. Stačí nainstalovat do chytrého telefonu odpovídající aplikaci a už můžete přes Skype telefonovat jak jste zvyklí. Toto řešení se pak jeví jako jedno z nejlepších, protože vás používání Skypu nic nestojí a zároveň nabízí velmi slušnou úroveň ochrany.

Závěr

V závěrečné části se pokusím zrekapitulovat poznatky, jež jsem v průběhu psaní této práce získal a zpracoval.

Bakalářská práce se věnuje mobilním telekomunikacím a bezpečnosti informací v nich přenášených. Jedná se o téma aktuální a v době technologického rozkvětu dosti zásadní, neboť únik informací cílený či neúmyslný je téma, jež se v médiích řeší dnes a denně.

V souladu s mými plány jsem v první části představil historické pozadí rozvoje mobilních telekomunikačních sítí a jejich jednotlivé standardy, od úplných prvopočátků až po současnost. V další části jsem se věnoval technickému zabezpečení těchto sítí a v kapitole třetí pak možným rizikům, jež uživateli hrozí každým dnem, kdy svůj mobilní telefon používá.

Závěrečná kapitola má poskytnout několik možných řešení, kterými lze své důvěrné informace dodatečně zabezpečit v případě, kdy uživatel opravdu musí tato data na dálku sdílet. V ideálním případě by tak měl samozřejmě činit pouze velmi zřídka, neboť v absolutním bezpečí nemohou být jeho informace prakticky nikdy.

Pokud je uživatel ochotný do zabezpečení investovat peníze, může si pořídit tzv. kryptotelefon, tedy speciálně upravený mobilní telefon s dodatečným šifrováním, který ovšem musí vlastnit i protistrana. Pořídit se dají i různá přídavná zařízení, jež dokáží obyčejný telefon proměnit v cosi kryptotelefonu podobného.

Řešit se dá ochrana samozřejmě i softwarově. V prvním případě jde o speciální aplikace pro telefony s operačním systémem. Ty však často nejsou nikterak levnou záležitostí. Vyplatí se tak tedy zejména firmám či uživatelům, kteří bezpodmínečně nutně potřebují mobilním telefonem přenášet citlivá data často, například k výkonu své profese.

Druhým softwarovým řešením je využití programu Skype, jehož zabezpečení je na tak vysoké úrovni, že o jeho prolomení usiluje i americká Národní bezpečnostní agentura, která vypsala vysokou odměnu tomu, komu se podaří algoritmus Skypu prolomit. V tomto případě se jedná o řešení

bezplatné a zároveň účinné, jeví se tedy jako ideální pro běžné uživatele. Program lze zároveň nahrát do novějších mobilních telefonů vybavených operačním systémem a volat si tak vzájemně jeho prostřednictvím.

Závěrem ovšem musím ještě jednou podotknout, že spoléhat se zcela na tyto formy dodatečného zabezpečení telefonních hovorů by bylo bláhovým jednáním. Na světě se vždy najdou jedinci, kteří nebudou mít klid, dokud tyto formy ochrany neprolomí a neprokáží světu, že sdílená data nikdy nebudou v bezpečí. Nezbývá tedy než přenášet důvěrných informací „vzduchem“ co nejméně.

Použitá literatura

1. Vývoj mobilních telekomunikací

1. D.E. Hughes and the first radio-telephone reception. *Privateline : telecomunications expertise* [online]. January 02, 2006, [cit. 2011-07-05]. Dostupný z WWW: <http://www.privateline.com/mt_digitalbasics/ii_wireless_history/08_de_hughes_and_the_first_radiotelephone_reception/>.

2. HILLEBRAND, Friedhelm. GSM and UMTS : the creation of Global Mobile Communication. 1st ed. Chichester : John Wiley & Sons, 2002. GSM's Achievements, s. 1-10. ISBN 0470-84322-5.

3. LÁSKA, Jan. Budoucnost mobilního internetu má jméno LTE. MobilMania.cz [online]. 26. 1. 2008, [cit. 2011-02-03]. Dostupný z WWW: <http://www.mobilmania.cz/clanky/budoucnost-mobilniho-internetu-ma-jmeno- lte/sc-3-a-1117856/default.aspx>. ISSN 1214-1887.

4. POSPÍŠIL, Aleš. LTE : za hranicemi budují, ČR vyčkává. *MobilMania.cz* [online]. 24. 10. 2010, [cit. 2011-07-06]. Dostupný z WWW: <http://www.mobilmania.cz/clanky/lte-za-hranicemi-buduji-cr-vyckava/sc-3-a-1314643/default.aspx>. ISSN 1214-1887.

5. POSTLER, Štěpán. WiMAX: : spolehlivý bezdrát míří do mobilů. *MobilMania.cz* [online]. 31. 10. 2006, 12345, [cit. 2011-07-06]. Dostupný z WWW: <http://www.mobilmania.cz/clanky/wimax-spolehlivy-bezdrat-miri-do-mobilu/sc-3-a-1113857/default.aspx>. ISSN 1214-1887.

6. PRESCOTT, George B. *History, theory and practice of the electric telegraph*. Boston : Ticknor and Fields, 1870. 468 s.

7. PROCHÁZKA, Juraj. LTE je standard, roztočte kolotoče. MobilMania.cz [online]. 7. 1. 2009, [cit. 2011-02-03]. Dostupný z WWW: <http://www.mobilmania.cz/clanky/lte-je-standard-roztocte-kolotoce/sc-3-a-1121166/default.aspx>. ISSN 1214-1887.

8. PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z. 2. aktualiz. vyd. Brno : Computer Press, 2006. [Kap.] 4.7, Mobilní sítě, s. 229-236. ISBN 80-251-1278-2.

9. RAMBOUSEK, Adam. *Historie mobilní komunikace*. Brno, 2003. 6 s. Seminární práce. Masarykova Univerzita.

10. RHEE, Man Young. Mobile Communication Systems and Security. 1st ed. Chichester : John Wiley & Sons, 2003. Universal Mobile Telecommunication System (UMTS), s. 133-166. ISBN 978-0-470-82336-1.

11. The first commercial American radio-telephone service. *Privateline : telecomunications expertise* [online]. January 02, 2006, [cit. 2011-07-05]. Dostupný z WWW:

<http://www.privateline.com/mt_digitalbasics/ii_wireless_history/17_the_first_american_radiotelephone_service/>.

12. The Rise of GSM. *Privateline : telecomunications expertise* [online]. January 02, 2006, [cit. 2011-07-05]. Dostupný z WWW: <http://www.privateline.com/mt_digitalbasics/ii_wireless_history/30_the_rise_of_gsm/>.

13. TOMEK, Pavel. Mobilní historie : milníky ve vývoji mobilní komunikace. MobilMania.cz [online]. 7. 1. 2006, [cit. 2011-02-03]. Dostupný z WWW: <http://www.mobilmania.cz/clanky/mobilni-historie-milniky-ve-vyvoji-mobilni-komunikace/sc-3-a-1111658/default.aspx>. ISSN 1214-1887.

14. ZIEGLER, Chris. 2G, 3G, 4G, and everything in between : an Engadget wireless primer. Engadget [online]. Jan 17th 2011, [cit. 2011-02-03]. Dostupný z WWW: <http://www.engadget.com/2011/01/17/2g-3g-4g-and-everything-in-between-an-engadget-wireless-prim/>.

15. 3.6 Mbps HSDPA here soon, 100 Mbps not too far away. *M-indya.com* [online]. 2006-07-19, [cit. 2011-07-06]. Dostupný z WWW: <http://www.m-indya.com/shownews.php?newsid=920>.

2. Technická řešení a bezpečnost

16. BROŽ, Petr. Karta SIM : mobilní identita. Mobility. 2005, roč. 7, s. 25-27. ISSN 1212-9879.

17. HAUSER, Pavel. Vědci prolomili další šifru GSM. *SecurityWorld* [online]. 20.01.10, [cit. 2011-08-07]. Dostupný z WWW: <http://securityworld.cz/securityworld/vedci-prolomili-dalsi-sifru-gsm-2234>.

18. HILLEBRAND, Friedhelm. GSM and UMTS : the creation of Global Mobile Communication. 1st ed. Chichester : John Wiley & Sons, 2002. The Subscriber Identity Module, Past, Present and Future, s. 341-370. ISBN 0470-84322-5.

19. HILLEBRAND, Friedhelm. GSM and UMTS : the creation of Global Mobile Communication. 1st ed. Chichester : John Wiley & Sons, 2002. Voice Codecs, s. 371-384. ISBN 0470-84322-5.

20. HILLEBRAND, Friedhelm. GSM and UMTS : the creation of Global Mobile Communication. 1st ed. Chichester : John Wiley & Sons, 2002. Security Aspects, s. 385-406. ISBN 0470-84322-5.

21. KOCMAN, Rostislav. Co je to kód IMEI. MobilMania.cz [online]. 1. 9. 2000, [cit. 2011-02-03]. Dostupný z WWW: <http://www.mobilmania.cz/clanky/co-je-to-kod-imei/sc-3-a-1000236/default.aspx>. ISSN 1214-1887.

22. POSPÍŠIL, Aleš. Asociace GSM posvětila standardizaci „vestavěné SIM“. MobilMania.cz [online]. 22. 10. 2010, [cit. 2011-02-03]. Dostupný z

WWW: <http://www.mobilmania.cz/clanky/asociace-gsm-posvetila-standardizaci-vestavene-sim/sc-3-a-1314956/default.aspx>. ISSN 1214-1887.

23. PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace : jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. 1. vyd. Brno : CP Books, 2005. [Kap.] 1.2, Šifrování, s. 15-22. ISBN 80-251-0791-4.

24. PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace : jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. 1. vyd. Brno : CP Books, 2005. [Kap.] 4.2, Bezpečnost v GSM/GPRS, s. 121-123. ISBN 80-251-0791-4.

25. PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace : jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. 1. vyd. Brno : CP Books, 2005. [Kap.] 4.3, Bezpečnost UMTS, s. 123-128. ISBN 80-251-0791-4.

26. PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace : jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. 1. vyd. Brno : CP Books, 2005. [Kap.] 5.2, Komprimace hlasu, s. 136-138. ISBN 80-251-0791-4.

27. RHEE, Man Young. Mobile Communication Systems and Security. 1st ed. Chichester : John Wiley & Sons, 2003. Cryptographic Protocols Applicable to Wireless Security Technologies, s. 127-132. ISBN 978-0-470-82336-1.

28. SNÁŠEL, Jaroslav. Kodeky v mobilech : aby se hlas mohl přenášet. MobilMania.cz [online]. 17. 3. 2005, [cit. 2011-02-03]. Dostupný z WWW: <http://www.mobilmania.cz/clanky/kodeky-v-mobilech-aby-se-hlas-mohl-prenaset/sc-3-a-1109611/default.aspx>. ISSN 1214-1887.

29. VALTTERI, Niemi; KAISA, Nyberg. UMTS Security. 1st ed. Chichester : John Wiley & Sons, 2003. Security in Telecommunications, s. 3-10. ISBN 0-470-85314-X.

30. ZANDL, Patrick. Šifrovací algoritmus A5.1 prý praskl : konec bezpečnosti GSM?. Mobil.cz [online]. 9. prosince 1999, [cit. 2011-02-03]. Dostupný z WWW: <http://mobil.idnes.cz/mob_tech.asp?r=mob_tech&c=A991208_0002145_mob_tech >.

3. Bezpečnostní rizika

31. ČERMÁK, Ivo. Jak se v Česku odposlouchávají telefony. Mobil.cz [online]. 24. Října 2004, [cit. 2011-02-03]. Dostupný z WWW: <http://mobil.idnes.cz/mob_tech.asp?r=mob_prakticky&c=A041023_5285436_mob_prakticky>.

32. DOSEDĚL, Tomáš. Mobilní zločiny : jak odposlechnout mobil, část první. MobilMania.cz [online]. 26. 3. 2003, [cit. 2011-02-03]. Dostupný z WWW: <http://www.mobilmania.cz/clanky/mobilni-zlociny-jak-

odposlechnout-mobil-cast-prvni/sc-3-a-1104440/default.aspx>. ISSN 1214-1887.

33. DOSEDĚL, Tomáš. Mobilní zločiny : jak odposlechnout mobil, část druhá. MobilMania.cz [online]. 3. 4. 2003, [cit. 2011-02-03]. Dostupný z WWW: <http://www.mobilmania.cz/clanky/mobilni-zlociny-jak-odposlechnout-mobil-cast-druha/sc-3-a-1104476/default.aspx>. ISSN 1214-1887.

34. DOSEDĚL, Tomáš. Klony útočí : k čemu je dobré a jak škodí klonování karet SIM. Mobility. 2002, roč. 4, č. 12, s. 20-22. ISSN 1212-9879.

35. HRMA, Jiří. Vyzkoušeli jsme HTCSense.com : zaměření pozice telefonu a přístup ke kontaktům odkudkoliv. *SmartMania.cz* [online]. 20. září 2010, [cit. 2011-08-09]. Dostupný z WWW: <http://smartmania.mobilmania.cz/index.php?ind=news&op=news_show_single&ide=1362>. ISSN 1801-3066.

36. KŮŽEL, Filip. Odposlech v GSM síti? Notebook, mobil a tři minuty. MobilMania.cz [online]. 4. 1. 2011, [cit. 2011-02-03]. Dostupný z WWW: <http://www.mobilmania.cz/clanky/odposlech-v-gsm-siti-notebook-mobil-a-tri-minuty/sc-3-a-1315295/default.aspx>. ISSN 1214-1887.

37. VOLYŇSKÝ, Tomáš. Jak bezpečná je vaše simkarta?. Mobil.cz [online]. 21. července 2003, [cit. 2011-08-09]. Dostupný z WWW: <http://mobil.idnes.cz/jak-bezpecna-je-vase-simkarta-dis-/mob_tech.asp?c=A030318_5204338_mob_prakticky>.

38. VOLYŇSKÝ, Tomáš. Některé SIM karty se klonují jen pět minut. Mobil.cz [online]. 27. března 2003, [cit 2011-08-09]. Dostupný z WWW: <http://mobil.idnes.cz/nektere-sim-karty-se-klonuji-jen-pet-minut-fj0-/mob_tech.asp?c=A030326_5204868_mob_prakticky>.

4 Možná řešení

39. ČERMÁK, Ivo. Mobily Tresor a Enigma : šifrováním GSM proti policii?. Mobil.cz [online]. 11. září 2002, [cit. 2011-02-03]. Dostupný z WWW: <http://mobil.idnes.cz/telefony.asp?r=telefony&c=A020910_5161509_telefony>.

40. DOSEDĚL, Tomáš. SMS 007 : šifrujte textové zprávy. MobilMania.cz [online]. 7. 12. 2005, [cit. 2011-02-03]. Dostupný z WWW: <http://www.mobilmania.cz/clanky/sms007-sifrujte-textove-zpravy/sc-3-a-1111471/default.aspx>. ISSN 1214-1887.

41. MAX, Harry; RAY, Taylor. Skype : kompletní průvodce. Přel. Lenka Košařová. 1. vyd. Praha : Grada Publishing, 2008. [Kap.] 1.4, Kdo prolomí Skype?, s. 29-30. ISBN 978-80-247-2123-1.

42. MAX, Harry; RAY, Taylor. Skype : kompletní průvodce. Přel. Lenka Košařová. 1. vyd. Praha : Grada Publishing, 2008. [Kap.] 1.8, Příběh Skypu, s. 38-42. ISBN 978-80-247-2123-1.

43. MAX, Harry; RAY, Taylor. Skype : kompletní průvodce. Přel. Lenka Košařová. 1. vyd. Praha : Grada Publishing, 2008. [Kap.] B.1, Bezpečnost Skypu, s. 185-196. ISBN 978-80-247-2123-1.

44. VOKÁČ, Luděk. Vyzkoušeli jsme šifrované telefonování, které nikdo neodposlechne. Mobil.cz [online]. 13. září 2010, [cit. 2011-02-03]. Dostupný z WWW: <http://mobil.idnes.cz/vyzkouseli-jsme-sifrovane-telefonovani-ktere-nikdo-neodposlechne-1f0-/mob_tech.asp?c=A100912_161500_mob_tech_vok>.

45. WALLINGFORD, Ted. Switching to VoIP. 1st ed. Sebastopol : O'Reilly Media, 2005. Replacing the Voice Circuit with VoIP, s. 110-129. ISBN 978-0-596-00868-0.

Obrazový materiál

1. PRESCOTT, George B. *History, theory and practice of the electric telegraph*. Boston : Ticknor and Fields, 1870. 468 s.

2. GSM. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, poslední aktualizace 2011-08-07 [cit. 2011-08-09]. Dostupné z WWW: <http://en.wikipedia.org/wiki/GSM>

3. *3GPP : a global initiative* [online]. 2011 [cit. 2011-08-09]. The Mobile Broadband Standard. Dostupné z WWW: <http://www.3gpp.org/>

4. *3GPP : a global initiative* [online]. 2011 [cit. 2011-08-09]. The Mobile Broadband Standard. Dostupné z WWW: <http://www.3gpp.org/>

5. ROHLÍK, M. Využití proudových šifer v současnosti. *Access Server* [online]. 10. 08. 2009, roč. 9, [cit. 2011-08-09]. Dostupný z WWW: <http://access.feld.cvut.cz/view.php?cisloclanku=2009080001>. ISSN 1214-9675.

6. STUmobil. *STUmobil : vše pro odblok, fleš a servis* [online]. 2011 [2011-08-09]. Produkty GSM. Dostupné z WWW: <http://www.unlock.cz/zarizenihtml/cloning.php>

7. Tripleton. *Tripleton : securing your world* [online]. 2009 [2011-08-09]. Tripleton Enigma Cryptophone. Dostupné z WWW: <http://www.tripleton.com/products/secure-phones/secure-mobile-phone.htm>.

Seznam použitých zkratek

GSM	Group Spéciale Mobile, později význam změněn na Global System for Mobile Communications
NMT	Nordic Mobile Phones
AMPS	Analog Mobile Phone System
TACS	Total Access Communications System
BTS	Base Transceiver Station
CSD	Circuit-Switched Data
HSCSD	High Speed Circuit-Switched Data
WAP	Wireless Application Protocol
UMTS	Universal Mobile Telecommunications System
GPRS	General Packet Radio Service
EDGE	Enhanced Data for GSM Evolution
ITU	International Telecommunication Union
CDMA	Code Division Multiple Access
WTO	World Trade Organisation
IMT-2000	International Mobile Telecommunication 2000
3GPP	Third Generation Partnership Project
W-CDMA	Wideband Code Division Multiple Access
FOMA	Freedom of Mobile Multimedia Access
TD-SCDMA	Time Division Synchronous Code Division Multiple Access
HSDPA	High-Speed Downlink Packet Access
HSUPA	High-Speed Uplink Packet Access
HSPA	High-Speed Packet Access
EUL	Enhanced UpLink
LTE	Long Term Evolution
WiMAX	Worldwide Interoperability for Microwave Access
SIM	Subscriber Identity Module
IMSI	International Mobile Subscriber Identity
HLR	Home Location Register
PIN	Personal Identification Number

PUK	Personal Identification Number Unlock Key
IMEI	International Mobile Equipment Identity
EIR	Equipment Identity Register
USIM	Universal Subscriber Identity Module
EFR	Enhanced Full-Rate
FR	Full-Rate
HR	Half-Rate
AMR	Adaptive Multi-Rate Speech Codec
DTX	Discontinuous Transmission
VAD	Voice Activity Detection
AES	Advanced Encryption Standard
P2P	Peer2peer
RSA	Rivest, Shamir and Adleman - dle nich se šifra jmenuje
NSA	National Security Agency