**Bezpečnost SMS komunikace**

SMS zprávy si za dobu své existence vydobyly nezaměnitelné místo na trhu mobilních komunikací. Přicházejí ke slovu pokaždé, když se nám nechce vyřizovat záležitost telefonicky, když si nepřejeme adresáta vyrušovat, nebo když potřebujeme zaslat nějakou informaci, která nesmí být zkomolena - něčí telefonní číslo, hodinu a místo srazu apod. Spousta uživatelů GSM sítí si na SMS komunikaci zvykla natolik, že ji využívá podstatně více než hlasové služby.

Při tom všem je však nutno mít na paměti, že SMS zprávy – jakkoliv lákavé svojí jednoduchostí a pohodlností – představují pro svoje odesílatele a příjemce řadu bezpečnostních rizik, zejména pokud obsahují informace, které by měly být skryty třetím osobám. Podívejme se na hlavní bezpečnostní rizika, která hrozí uživatelům SMS.

1. Snadné sledování

Vzhledem ke svému charakteru jsou krátké texty jako SMS ideálním předmětem sledování (odposlechu). Náklady na jejich sledování jsou nižší než u hlasové komunikace, a uživatelé na obou koncích nemají naprosto žádnou šanci zjistit, že se na jejich komunikaci někdo „pověsil“. Navíc je velmi snadné prohlížet všechny SMS procházející sítí automaticky na výskyt klíčových slov, což je také běžně prováděno.
Sledování nemusí být prováděno jen prostřednictvím operátora. Přístroje k odposlechu GSM spojení se dají (na černém trhu) zakoupit za cenu několika desítek tisíc euro, což je bezpečně v možnostech řady firem i soukromých osob, včetně např. soukromých detektivů.

2. Prozrazení textu díky nepozornosti uživatele

SMS je trvalejšího rázu než hovor. Osoba, která vstoupila do místnosti 30 sekund poté, co jste ukončili telefonát, má jen mizivou šanci se dozvědět, o čem jste hovořili. Naproti tomu zapomenete-li smazat příchozí či odchozí SMS, bude ve Vašem telefonu ležet tak dlouho, dokud svoje opomenutí nenapravíte. Přitom stačí vzdálit se na chvíli od svého telefonu, a každý, kdo je v tu chvíli přítomen, si může Vaše zprávy prohlédnout.
Totéž se pochopitelně týká situace, kdy Vám bude telefon odcizen.

3. Dlouhá dohledatelnost v záznamech

SMS jsou velmi nenáročné na skladovací prostor, neboť jsou krátké. To v době, kdy jeden gigabyte diskové kapacity stojí méně než dolar, poskytuje operátorům zajímavé možnosti archivace. Ve světě se neustále rozšiřuje okruh zemí, jejichž zákony archivaci všech SMS po dobu několika let přímo vyžadují. Po teroristických útocích v Londýně zvažuje zavedení tohoto opatření i řada zemí EU. To by znamenalo, že k Vaší kompletní korespondenci by určité osoby mohly mít přístup i několik let nazpět.

4. Vedlejší informační kanály

Pro osobu, která se neoprávněně dostane k Vašemu přístroji, může být zajímavý už samotný seznam Vašich telefonních kontaktů. Představa žárlivé manželky, která objeví v telefonním seznamu podezřelou „Mici“, je trochu úsměvná, avšak nabývá podstatně hrozivějšího rázu, pokud jde o zločince zjišťujícího kontakty na Vaše blízké a přátele.

5. Pozměnitelnost SMS zprávy

SMS zpráva, procházející v otevřené podobě sítí operátora, může být cílem nejen pro odposlech, ale i pro mnoho aktivních útoků. Velkou pozornost si v poslední době vysloužilo falšování adresy

odesílatele[1], lze si však představit ještě nebezpečnější varianty, například *změnu textu* samotné SMS. Někdy stačí pozměnit slovo „nesouhlasím“ na slovo „souhlasím“, a aktivní útočník sedící „na vhodném místě“ v síti právě spáchal značnou škodu. U běžné SMS si nemůžete být zcela jisti, kdo je autorem a zda Vám dorazila v původní podobě – to, co se s ní děje mezi telefonem odesílatele a telefonem příjemce, je pro Vás zkrátka nezjistitelné.

Z výše uvedených nebezpečí je zřejmé, že spoléhat na běžné služby SMS při výměně důvěrných dat je rizikové. Uživatel GSM sítě, kterému záleží na soukromí, má tedy v zásadě na vybranou ze dvou možností: buď používat SMS jen k výměně banálních sdělení, která nejsou pro nikoho důležitá, nebo se pokusit svoje SMS nějakým způsobem proti zmíněným rizikům ochránit.

**Ochrana SMS před zneužitím – principy**

Mají-li být zprávy SMS spolehlivým nosičem informace, musejí splňovat několik vlastností, které budou bránit všem možnostem zneužití, vyjmenovaným výše.

1. Musejí být zabezpečeny vůči sledování (odposlechu) nepovolanou osobou.
2. Musejí být „jištěny“ tak, aby bylo možno zaručit jejich nedotknutelnost (každá změna, která vznikla „po cestě“, musí být u příjemce odhalena)
3. Musí být jisté, že odesílatelem přijaté zprávy je osoba, která se za něj vydává.
4. Je potřeba, aby uložené SMS byly chráněny před přečtením v případě, že se telefon dostane do nepovolaných rukou.
5. Stejně tak je před nepovolanými osobami třeba chránit i seznam kontaktů.

Naštěstí jsou díky současnému stavu vědy a techniky tyto cíle dosažitelné i pro běžné uživatele GSM sítí.

*Kryptografie* je část matematické vědy, která se zabývá ochranou informace před nepovolanými osobami. Zprvu byly poznatky kryptografie dostupné pouze úzkému okruhu osob z vojenských kruhů. V 70. letech, s rozvojem počítačové techniky, však došlo k rozsáhlému rozvoji *civilní kryptografie*, která se zabývá ochranou informace v běžné denní praxi. V současné době je civilní kryptografie značně rozvinutým vědeckým odvětvím, s jehož využitím jsou chráněny například bankovní transakce (v hodnotě několika miliard dolarů denně), přístupy k neveřejným databázím a další druhy soukromé komunikace.

**Praktická kryptografie**

V průběhu let byly v kryptografické vědě vytvořeny různé standardy pro šifrování dat, z nichž patrně nejznámější je AES (Advanced Encryption Standard), velmi silná šifra, která je kromě jiných využívána např. americkou armádou a diplomacií. Přes mnohaletý výzkum nebyla dosud objevena žádná reálná slabina standardu AES, která by mohla vést k odhalení zašifrovaných dat nepovolanou osobou. Jiným standardem je SHA-2, což je tzv. hashovací algoritmus, který se sice nedá použít k šifrování, ale s jehož vhodným využitím se dá zabezpečit *integrita* dat (tj. skutečnost, že do nich nikdo nezasáhl).

Základní vlastností dobré šifry je tzv. Kerckhoffův princip, podle nějž znalost principu šifry nesmí nijak ohrozit bezpečnost celého procesu; skutečná bezpečnost musí ležet v použitém *klíči*. Analogie tohoto principu můžeme najít i v reálném světě: například zloději se dříve nebo později dostanou k popisu toho, jak funguje nějaký trezor, ale přesto jim tento popis nesmí pomoci při pokusu o vloupání; bezpečnost trezoru spočívá v klíči, kterým se otevírá.

Podle stavu matematické vědy v létě 2005 splňovaly standardy AES i SHA-2 tento princip bez

1 Viz např. http://mobil.idnes.cz/mob_prakticky.asp?r=mob_prakticky&c=A050815_153733_mob_prakticky_dno

výhrad.

**SMS007 – reálná ochrana SMS**

Společnost CircleTech, s.r.o., vyvinula pro ochranu Vašich SMS speciální program *SMS007*, který používá právě standardy SHA-2 a AES. Naplňuje všechny požadavky, vyjmenované v předchozích odstavcích.

1. *Zabezpečení vůči sledování (odposlechu)*

Zprávy mezi dvěma uživateli programu SMS007 jsou šifrovány pomocí standardu AES a klíče odvozeného ze vzájemně dohodnutého hesla. Protivník sledující provoz vidí pouze nesmyslnou změť znaků, kterou není schopen bez znalosti hesla rozluštit. Při volbě kvalitního hesla trvá luštění jedné jediné zprávy řádově miliardy let.
Klíče ke komunikace s jednotlivými uživateli jsou v paměti telefonu uloženy jako bezpečně zašifrované pomocí „hlavního hesla aplikace“. Nemusíte si je tedy pamatovat, stačí znát „hlavní heslo“ (viz též dále). Po vzájemné dohodě není problém klíče kdykoliv změnit.

2. *Zajištění integrity (nedotčenosti) zpráv*

Každý zašifrovaná zpráva putující mezi dvěma uživateli programu SMS007 obsahuje vevnitř speciální zabezpečovací kód založený na standardu SHA-2. Tento kód slouží jako spolehlivá detekce narušení zprávy po cestě (při jakémkoliv zásahu se změní). V případě, že by aktivní protivník zasáhl do zprávy procházející sítí, program SMS007 zaznamená rozdílnost očekávaného a skutečného kódu a nahlásí uživateli chybu.

3. *Zajištění toho, že odesílatelem je skutečně osoba, která se za něj vydává*

Zašifrování zprávy slouží zároveň jako důkaz, že osoba, která zprávu odeslala, má k dispozici dohodnuté heslo (klíč). Bez znalosti tohoto hesla (klíče) není protivník schopen vygenerovat zprávu, která by se korektně rozšifrovala na telefonu příjemce. To znamená, že již sama skutečnost, že přijatá šifrovaná zpráva je na Vašem telefonu čitelná, zaručuje, že byla odeslána z telefonu Vašeho komunikačního partnera (a není tedy podvržená).

4. *Ochrana přijatých a odeslaných SMS před nepovolanými osobami*

Všechny přijaté a odeslané zprávy jsou v rámci programu SMS007 při ukládání do telefonu šifrovány za pomoci standardů AES (samotné šifrování), SHA-2 (kontrola integrity) „hlavním heslem aplikace“, které si na počátku zvolíte. Program SMS007 se svého uživatele při každém startu dotáže na správné „hlavní heslo“, a pokud je zadáno špatně, není schopen tato bezpečně uložená data rozšifrovat. Stejně tak není schopen tato data rozšifrovat nikdo, kdo by je z telefonu vykopíroval např. do počítače – bez znalosti správného „hlavního hesla“ se uložené údaje jeví jako nesmyslná změť znaků. Je to pouze Vaše znalost správného „hlavního hesla“, která je umožňuje proměnit ve smysluplný text.
Tím jsou Vaše SMS bezpečně chráněny před nepovolanými osobami v okamžicích, kdy nemáte nad svým telefonem dohled (například když se vzdálíte z místnosti a telefon zanecháte na stole, nebo když je Vám telefon odcizen).

5. *Ochrana seznamu kontaktů před nepovolanými osobami*

Program SMS007 si udržuje svůj vlastní seznam kontaktů, nezávislý na hlavním seznamu kontaktů v telefonu. Tento seznam kontaktů je chráněn před přečtením stejným způsobem jako přijaté a odeslané zprávy – šifrováním za pomoci standardů AES, SHA-2 a „hlavního hesla aplikace“.
V případě, že Váš telefon padne do rukou nepovolané osoby, tato osoba nemá možnost zjistit ani to,

s kým si píšete zašifrované zprávy. Tato vlastnost je velmi výhodná, potřebujete-li před jinými lidmi utajit už samotnou skutečnost, že si píšete s určitým člověkem.

**… a mnoho funkcí navíc!**

Program SMS007 se zdaleka neomezuje jen na odesílání a přijímání šifrovaných zpráv. Cílem jeho autorů bylo poskytnout Vám zároveň maximální pohodlí při práci s nimi. Z toho důvodu jej firma CircleTech, s.r.o., vybavila řadou vlastností, které Vám mohou jeho používání zpříjemnit.

– *třídění kontaktů do skupin*

V seznamu kontaktů aplikace si můžete vytvořit až 60 skupin, do nichž můžete svoje kontakty roztřídit. Skupiny se dají otevírat a uzavírat.

– *podpora češtiny, slovenštiny, polštiny ...*

V celém programu je podporována diakritika. To znamená, že si můžete psát zprávy s háčky a čárkami, které se správně uloží a zobrazí odesílateli a příjemci. Stejně tak můžete používat háčky a čárky v pojmenovávání svých kontaktů, skupin kontaktů apod.
Také samotný program SMS007 s Vámi bude komunikovat česky, a ne *cesky* (existují i další jazykové verze, např. anglická či slovenská).

– *rozsáhlé možnosti v seznamu kontaktů*

U každé osoby v seznamu kontaktů si můžete poznamenat její e-mail a můžete si k ní připsat poznámku dlouhou až 150 znaků. Tyto údaje lze samozřejmě kdykoliv měnit.

– *pohodlné odesílání kontaktů jiným lidem*

Jestliže si přejete zaslat člověku, který rovněž vlastní program SMS007, kontakt na někoho, koho máte ve svém seznamu kontaktů, je to v rámci programu velmi jednoduché. Můžete odeslat speciální SMS, která obsahuje dotyčný kontakt se jménem telefonním číslem, e-mailem i poznámkou. Příjemci zprávy stačí jediné kliknutí k tomu, aby si kontakt uložil do svého seznamu. I tato speciální zpráva je samozřejmě chráněna šifrováním.

– *dlouhé zprávy*

Maximální délka zprávy, kterou můžete poslat za pomoci programu SMS007, je 200 znaků.

– *třídění zpráv do skupin*

Stejně jako kontakty, i zprávy mohou být tříděny do až 60 skupin vytvořených uživatelem.

– *barevné rozlišení zpráv podle jejich stavu*

Přijaté, odeslané a rozepsané zprávy mají v seznamu zpráv ikony různých barev, které Vám napovídají, co se s nimi děje. Rozepsané zprávy jsou bílé; úspěšně odeslané zprávy zelené; přijaté a nepřečtené zprávy oranžové; přijaté a přečtené zprávy modré; v případě selhání Vás bude varovat červená. Tato intuitivní volba barev Vám jistě velmi zpříjemní práci se zprávami.

– *„přísně tajné“ zprávy*

Pokud si přejete odesílat zprávy ještě bezpečněji, můžete je označit jako „přísně tajné“. Takové

zprávy se neukládají do seznamu přijatých a odeslaných zpráv. Jakmile „přísně tajnou“ zprávu odešlete, zmizí z Vašeho seznamu odeslaných zpráv, jako by nikdy neexistovala. U příjemce se pak uloží do seznamu přijatých zpráv jen do chvíle, než si ji přečte. Jakmile ji otevře, může si ji jednou přečíst - ihned poté se zpráva smaže i u něj.

– *inteligentní tlačítka*

Program SMS 007 si u uložených šifrovaných zpráv pamatuje, které z nich jste obdrželi a které jste odeslali, a tomu přizpůsobuje nabídku, co můžete se zprávou dělat. Například přijaté zprávy disponují (mimo jiné) volbou „Odpovědět“; zprávy, jejichž odeslání selhalo (např. kvůli výpadku signálu) mají volbu „Poslat znovu“, atd.

– *automatický mazač starých zpráv*

Součástí programu SMS 007 je nastavitelný mazač starých zpráv, který maže všechny nearchivované zprávy starší než určitý počet dnů: k dispozici jsou možnosti 1 den, 3 dny, týden, 14 dní či měsíc. Mazač samozřejmě můžete i vypnout úplně, avšak pokud jej ponecháte zapnutý, bude zajišťovat, že se Vám nepřeplní paměť a program poběží stále velmi rychle (velmi zaplněná paměť zpomaluje start programu, neboť se musí zpracovat více dat).
Pokud Vám na nějaké zprávě záleží a nechcete, aby byla po čase automaticky smazána, nemusíte mazač vypínat – stačí zprávu v seznamu zpráv označit jako „Archivovanou“ a mazač ji ponechá uloženou. Toto označení můžete kdykoliv později zase zrušit.

– *možnost kdykoliv si změnit hesla*

Hlavní heslo aplikace můžete kdykoliv změnit (musíte k tomu znát i heslo staré). Uložená data se ihned přešifrují pomocí nového klíče, a protivník, který bude znát jen staré heslo, na tom nebude o nic lépe, než kdyby ho neznal.
Snadno lze změnit i hesla pro korespondenci s jednotlivými uživateli ve Vašem seznamu kontaktů; k tomu stačí znalost hlavního hesla aplikace, staré „korespondenční“ heslo daného uživatele si nemusíte pamatovat.

– *přehled obsazené paměti*

Program SMS 007 Vám sdělí, kolik máte uloženo kontaktů, zpráv, kolik paměti zabírají a kolik ještě máte volného místa.

– *odesílání hromadných (skupinových) zpráv*

SMS 007 umožňuje odesílat hromadné zprávy celým skupinám lidí ve Vašem seznamu kontaktů. Zpráva se odešle všem lidem ve vybrané skupině, každému z nich zašifrovaná jeho vlastním klíčem.