Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Zabezpečení mobilního telefonu

Lenka Fořtíková

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Fořtíková Lenka

Informatika

Název práce

Zabezpeceni mobilního telefonu

Anglický název

Security of the mobile phone

Cíle práce

Cílem práce je popsat principy fungování mobilních telefonů, analyzovat související bezpečnostní rizika a v praktické části pak navrhnout konkrétní zabezpečení včetně konfigurace a volby vhodného bezpečnostního software při využití OS Android.

Metodika

Při psaní práce jsou informace čerpány z četby odborné literatury v tištěné a/nebo elektronické podobě. Na základě získaných teoretických poznatků je navrženo vhodné zabezpečení včetně konfigurace a volby bezpečnostního software. V závěru jsou shrnuty výsledky a celkový přínos práce.

Harmonogram zpracování

1) Příprava a studium odborných informačních zdrojů, upřesnění dílčích cílů práce a volba postupu řešení: 6/2013 - 7/2013
2) Zpracování přehledu řešené problematiky dle informačních zdrojů: 7/2013 - 9/2013
3) Vypracování vlastního řešení, diskuze a zhodnocení výsledků: 9/2013 - 11/2013
4) Tvorba finálního dokumentu diplomové práce: 11/2013 - 2/2014
5) Odevzdání diplomové práce a teze: 3/2014

Rozsah textové části

60 - 80 stran

Klíčová slova

mobilní telefon, soukromí, bezpečnost, osobní data, Internet

Doporučené zdroje informací

PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. Brno: CP Books, 2005. 179 s. ISBN 80-251-0791-4.
LOCKHART, Andrew. Bezpečnost sítí na maximum. Brno: CP Books, 2005. 276 s. ISBN 80-251-0805-8.
KLANDER, Lars. Hacker Proof: váš počítač, vaše síť, vaše připojení k Internetu - je to opravdu bezpečné?. Brno: Unis, 1998. 648 s. ISBN 80-86097-15-3.
CRAIG, Paul, HONICK, Ron, BURNETT, Mark. Softwarové pirátství bez záhad. Praha: Grada Publishing, 2008. 212 s. ISBN 978-80-247-1765-4.
DOBDA Luboš. Ochrana dat v Informačních systémech. Praha: Grada Publishing, 1998. 286 s. ISBN 80-7169-479-7.
RAAB, Stefan, CHANDRA, Madhavi W. CISCO: mobilní IP technologie a aplikace. Praha: Grada Publishing, 2007. 299 s. ISBN 978-80-247-1611-4.
Vávrů, Jiří. jQuery Mobile. Brno: Computer Press, 2013. 247 s. ISBN 978-80-2513-811-3.
Procházka, David. Mobilní telefony: příručka pro stávající i budoucí majitele mobilu. Olomouc: Rubico, 2000. 104 s. ISBN 80-85839-57-1.

Vedoucí práce

Brechlerová Dagmar, RNDr., Ph.D.

Termín odevzdání

březen 2014

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

doc. Ing. Zdeněk Havlíček, CSc.
Vedoucí katedry

prof. Ing. Jan Hron, DrSc., dr. h. c.
Děkan fakulty

V Praze dne 30.10.2013

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Zabezpečení mobilního telefonu" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 26. března 2014 Lenka Foltýnová

Poděkování

Ráda bych touto cestou vyjádřila poděkování RNDr. Dagmar Brechlerové, Ph.D. za její cenné rady a trpělivost při vedení mé diplomové práce.

Zabezpečení mobilního telefonu

Security of the mobile phone

Souhrn

Tato práce se zabývá problematikou bezpečnosti dat a osob v souvislosti s používáním mobilního telefonu s operačním systémem Android. Jsou zde řešeny možnosti zabezpečení před souvisejícími útoky. Hlavním cílem je nastínění konkrétního řešení, ať už ve formě nastavení mobilního telefonu, nebo doporučeného chování uživatele tak, aby se předešlo případným hrozbám či útokům, které mohou vzniknout při používání mobilního telefonu. Hlavního cíle je dosaženo dvěma kroky; zaprvé studií a analýzou aktuálních a obecných principů fungování mobilních technologií a dále možných bezpečnostních hrozeb a rizik souvisejících s použitím nezabezpečeného mobilního telefonu; v druhém kroku je provedena podrobnější analýza jednotlivých hrozeb a na základě dosažených znalostí je navrženo či doporučeno konkrétní řešení problematiky, včetně uvedení grafického návodu nastavení bezpečnostních opatření na daném mobilním telefonu.

Summary

This thesis deals with the issue of data security and users in connection with the use of mobile phones running Android. There are addressed security options against related attacks here. The main objective is to outline specific solutions, whether in the form of a mobile phone settings, or a recommendation to user behavior in order to avoid potential risks or attacks that can occur when using a mobile phone. The main goal is achieved in two steps; first, by studies and analysis of current and general principles of operation of mobile technologies and potential security threats and risks associated with the use of unsecured mobile phone; the second step is to perform a more detailed analysis of threats and then, based on the proposed acquisition of knowledge, provide recommendations

addressing each of the specific issues, including the graphical instruction set of security settings on the mobile phone.

Klíčová slova: mobilní telefon, soukromí, bezpečnost, osobní data, internet

Keywords: moible phone, privacy, security, personal data, the Internet

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

3G ..... 3rd Generation of Mobile Phones
A2DP ..... Advanced Audio Distribution Bluetooth Profile
AC ..... Authentification Centre
AMPS ..... Advanced Mobile Phone System
APK ..... Android Application Package File
B-ISDN ..... Broadband Integrated Services Digital Network
BND ..... Bundesnachrichtendienst
BSC ..... Base Station Controller
BTS ..... Base Transciever Station
DES ..... Data Encryption Standard
EDGE ..... Enhanced Data for GSM Evolution
EIR ..... Equipment Identity Register
FDMA ..... Frequency Division Multiplex Access
GPRS ..... Global Packet Radio Services
GPS ..... Global Positioning System
GSM ..... Global System for Mobile Communication
HDPA ..... High-Speed Downlink Packet Access
HLR ..... Home Location Register
HSDPA ..... High Speed Downlink Packet Access
HSUPA ..... High Speed Upload Packet Access
HTC ..... High Tech Computer Corporation
ID ..... Identification
IMSI ..... Inernational Mobile Subscriber Identity
IMT-2000 ..... International Mobile Telecommunications-2000
IP ..... Internet Protocol
ISND ..... Integrated Services Digital Network
LG ..... LG Group
LPC ..... Local Procedure Call
LTP ..... Long Term Prediction
MHz ..... MegaHertz

MMS ..... Multimedia Messaging Service
MSC ..... Mobile Switching Centre
MTA ..... Mail/Message Transfer Agent
MTS ..... Message Transfer/Telephone Services
NFC ..... Near Field Communication
NMT ..... Nordic Mobile Telecommunication
OS ..... Operating System
PBAP ..... Phone Book Access Bluetooth Profile
PDC ..... Programme Delivery Control
PIN ..... Personal Identification Number
PSTN ..... Public Switched Telephone Network
QR ..... Quick Response
RPE-LTP ..... Lond Pulse Excitation – Long Term Prediction
SIM ..... Subscriber Identity Module
SMS ..... Short Message Service
TCP/IP ..... Transmission Control/Internet Protocol
TDMA ..... Time Division Multiple Access
TRAU ..... Transcoding and Adaptation Unit
UMTS ..... Universal Mobile Telecommunications System
VLR ..... Visitor Location Register
WAP ..... Wireless Application Protocol
WATM ..... Wireless Asynchronous Transfer Mode
WCDMA ..... Wideband Code Division Multiple Access
Wi-Fi ..... Wireless Fidelity

1. ÚVOD

V dnešní době jsou mobilní telefony jedním z nejčastějších prostředků komunikace. Staly se samozřejmostí i nezbytností. Jejich rozšíření jen potvrzuje fakt, že uživatelé mnohdy vlastní a používají i více než jen jeden mobilní telefon. Moderní mobilní telefony dnes slouží k soukromým a pracovním účelům, zábavě, focení, tvorbě videí, brouzdání na internetu, sdílení různých typů dat, ale také ke komunikaci na sociálních sítích. Uživatelé mohou téměř kdykoliv a kdekoliv telefonovat, posílat SMS nebo MMS, připojit se k e-mailu, vzdálené ploše nebo se připojit do videokonference. Mohou si instalovat různé aplikace, propojit si telefon se svým účtem na internetové sociální síti nebo synchronizovat se svým počítačem. Na svém mobilním telefonu si mohou hrát hry, chatovat nebo s jeho pomocí na dálku ovládat svou televizi. Dále je možné pomocí mobilního telefonu ovládat svůj bankovní účet nebo s ním platit účty u obchodníků. Možnostem využití moderních mobilních telefonů se meze nekladou.

Avšak mobilní telefony mají i své stinné stránky. Jsou velmi snadno zneužitelné. Již od samých začátků používání je běžné mít svůj osobní počítač dobře zabezpečený například antivirovým systémem, firewallem nebo šifrováním, ale na ochranu mobilních telefonů se zpravidla už tolik nemyslí. Přitom je-li mobilní telefon připojený do internetové sítě, je stejně zranitelný jako počítač. Stále častější a agresivnější útoky na mobilní telefony se bohužel neomezují pouze na zcizení osobních informací a citlivých dat, ale dochází také k narušení soukromí a identity oběti nebo v krajních případech k fyzickým či psychickým útokům.

2. CÍL PRÁCE A METODIKA

Cílem této práce je popsat principy fungování mobilních telefonů, analyzovat související bezpečnostní rizika a v praktické části pak navrhnout konkrétní zabezpečení včetně konfigurace a vhodného bezpečnostního software při využití operačního systému Android. Pro účely práce slouží jako pokusné zařízení mobilní telefon HTC Wildfire S A510e s operačním systémem Android 2.3.3 Gingerbread.

Při psaní práce jsou informace čerpány z četby odborné literatury v tištěné a/nebo elektronické podobě. Na základě získaných teoretických poznatků je navrženo vhodné chování uživatele a zabezpečení mobilního telefonu, včetně konfigurace a volby bezpečnostního software. V závěru jsou shrnuty výsledky a celkový přínos práce.

Práce je zpracována dle následujícího harmonogramu:

- Příprava a studium odborných informačních zdrojů, upřesnění dílčích cílů práce a volba postupu řešení: 6/2013 – 7/2013
- Zpracování přehledu řešené problematiky dle informačních zdrojů: 7/2013 - 9/2013
- Vypracování vlastního řešení, diskuze a zhodnocení výsledků: 9/2013 - 11/2013
- Tvorba finálního dokumentu diplomové práce: 11/2013 – 2/2014
- Odevzdání diplomové práce a teze: 3/2014

3. PŘEHLED ŘEŠENÉ PROBLEMATIKY

3.1 Vývoj mobilních telekomunikací

Technologie mobilních telekomunikací prošly dlouhým vývojem rozděleným do několika fází.

Nejdříve docházelo k pokusům o přenos zvuku na delší vzdálenosti za použití velkých nepřenosných stanic analogového typu. Pokusy se prováděly na vysokých školách, univerzitách nebo ve vědecko-výzkumných laboratořích.

V další fázi, a to zejména pro využití v armádě, se začalo uvažovat o možnostech přenosu a zmenšení přístrojů. Výsledek pečlivých studií a mnoha testování dal za vznik přenosných vysílaček. Tyto vysílačky však fungovaly jen nezabezpečeně na nekódovaných frekvencích, tedy ani možný odposlech hovoru nebyl nijak obtížný. Služba vytáčení telefonního čísla volaného nebyla k dispozici a veškeré hovory byly v této době spojovány pouze telefonními spojovatelkami.

S postupem času následovaly snahy o vytvoření takové sítě, kde by měl každý přístroj své vlastní identifikační číslo a komunikace by probíhala současně na dvou kanálech. Hlavní myšlenkou bylo odstranění nutnosti přepínání módů poslechu, respektive vysílání, během komunikace. A právě tehdy vznikla první celulární síť.

S rychlým pokrokem vědy a technologických možností se i nadále zvyšovaly požadavky na oblast mobilních komunikací, jež dalo za vznik digitálních sítí tak, jak je známe dnes.

3.2 Významné osobnosti a události mobilního světa

První známý popis komunikace na principu telefonu pochází již z roku 968. Jedná se o takzvaný trubkový telefon, který sloužil ke komunikaci na dálku skrze trubkový systém a byl využíván především v lodní dopravě.

„*Historie pevné telefonie a telefonování se začala psát v roce 1876, kdy Alexander Graham Bell uskutečnil první telefonní hovor, skrze vlastnoručně zkonstruovaný telefonní přístroj. Nebyl to ještě žádný dálkový hovor, ale pouze vzkaz spolupracovníkovi Thomasu*

Watsonovi, nejspíše do sousední místnosti, aby za ním přišel („Mr. Watson, come here, I want you"). Nicméně na začátek velké a slavné éry telefonování to stačilo."[1]

Později, v roce 1896 získal italský fyzik a vynálezce Guglielmo Marconi patent na bezdrátový telegraf. Po pěti letech úspěšných pokusů o vysílání na kratší vzdálenosti uskutečnil Marconi první bezdrátové telegrafické spojení přes Atlantický oceán. Přestože byl Marconi všeobecně považován za autora bezdrátového telegrafu, uznání za tento vynález patří jinému autorovi, vynálezci Nikolovi Teslovi. Ten se už v roce 1891, tedy deset let před uskutečněným Marconiho transatlantickým spojením, začal zabývat radiovými přenosy a v roce 1893 představil světu první radiokomunikační přístroj. Tesla bohužel neměl výrazné podnikatelské schopnosti a zřejmě si ani neuvědomoval potenciál svých vynálezů, proto velká řada jeho nápadů nebyla veřejnosti nikdy představena.

„*Společnost Ericsson uvedla světově první plně automatický mobilní telefonní systém (MTA) v roce 1956. Systém pracoval v pásmu 160 MHz a byl používán v automobilech ve dvou švédských městech v letech 1956 až 1967. Váha telefonu MTA se pohybovala kolem 40 kg! V dobách své největší slávy měla síť MTA pouze 125 uživatelů a většina lidí neměla vůbec tušení, že mobilní komunikace existuje. Důvodem byla hlavně technická náročnost na údržbu systému a cena přístroje.*"[2]

Obrázek č. 1 První komerční mobilní systém MTS

Zdroj: zpracováno dle *http://smartphones.wonderhowto.com/inspiration/from-backpack-transceiver-smartphone-visual-history-mobile-phone-0127134/*

---

[1] Zpracováno dle *http://www.earchiv.cz/b07/b0700001.php3*

[2] Zpracováno dle *http://www.servis-sonyericsson.cz/zajimavosti.html*

Historicky prvním, veřejnosti dostupným mobilním telefonem se stala Motorola DynaTAC 8000X. Dne 21. září 1983 jej světu představil doktor Martin Cooper, který byl nejen jeho vynálezcem, ale byl také vůbec prvním člověkem na světě, který si zatelefonoval z opravdového přenosného mobilního telefonu. Než v ten den svůj mobilní telefon předvedl široké veřejnosti, chtěl ho doktor Cooper nejdříve vyzkoušet na soukromém hovoru. Cooperův první telefonát byl uskutečněn z ulice na Manhattanu v New Yorku a byl určen jeho rivalovi doktorovi Joel. S. Engelovi z Bell Labs. Procházející lidé v němém úžasu sledovali procházejícího doktora telefonujícího s kompaktním přístrojem, navíc bezdrátovým.

Tehdy DynaTAC 8000X fungoval na analogové síti standardu NMT. Nabízel 30 minut hovoru a 8 hodin pohotovostního režimu. Vážil bezmála jeden kilogram a na výšku měřil zhruba 25 cm. Jeho prodejní cena byla necelých 4.000,- amerických dolarů, jež je v dnešních penězích hodnota deseti automobilů Bentley.

Obrázek č. 2 Motorola DynaTAC

Zdroj: zpracováno dle *http://en.wikipedia.org/wiki/File:DynaTAC8000X.jpg*

V roce 1987 byl Mikhail Gorbatchev, prezident Sovětského svazu, zachycen fotografy na tiskové konferenci, uskutečňujíc mobilní telefonní hovor z Moskvy do Helsinek. Jeho telefonním zařízením byl tehdy kompaktní mobilní telefon Nokia typu Mobira City Man 900 a právě tímto snímkem si telefon Mobira City Man vysloužil přezdívku „Gorba“. Ten den mobilní telekomunikace vstoupila do široké povědomosti lidí z celého světa.

„První SMS zpráva z mobilního telefonu byla odeslána v roce 1993 z firmy Nokia. Začátky SMS zpráv nebyly zrovna jednoduché a zákazníci tuto službu od počátku roku 1995, spíše ignorovali. V roce 1995 odeslali 2 zákazníci v průměru jednu SMS zprávu za měsíc! Ale již v roce 2000 se průměrný počet SMS na zákazníka za měsíc, vyšplhal na více než 30. Dnes je zasílání krátkých textových SMS zpráv samozřejmostí a málo kdo si dokáže představit, že by tato služba neexistovala.“[3]

3.3 Technologie mobilních telefonů

Mobilní technologie prošly za poměrně krátkou dobu velmi rychlým vývojem. Co si lidé neuměli před deseti lety představit, je nyní realitou. Dříve tlačítkové telefony s černobílým displejem vystřídali dotykové telefony s brilantními displeji s úžasnými barvami a rozlišením. Telefony bez jakéhokoliv nebo minimálního paměťového prostoru k archivaci dat jsou dnes již minulostí. V současnosti se do mobilních telefonů ukládá až několik desítek gigabyte dat fotografií, hudebních souborů nebo videí. A připojení na internet? To je samozřejmostí. Z novodobých mobilních telefonů se stala především „hračka“ z hlediska uživatele, ale zároveň „velmi silná zbraň“ pro zloděje osobních dat.

Obrázek č. 3 Evoluce mobilních telefonů

Zdroj: zpracováno dle *http://cs.wikipedia.org/wiki/Soubor:Mobile_phone_evolution.jpg*

[3] Zpracováno dle *http://www.servis-sonyericsson.cz/zajimavosti.html*

Mobilní telefony existují mobilní v různých vzhledech a typech. Dříve velmi oblíbené a moderní vysouvací telefony nebo telefony do „vé“ dnes vytřídaly „chytré“ telefony s celoplošným dotykovým displejem z přední strany přístroje. Klasické tlačítkové telefony již pomalu mizí z trhu.

Mezi největší výrobce mobilních telefonů patří Samsung, Apple, Huawei, LG a Lenovo. V posledních letech se do popředí dostává také značka HTC. V mobilních telefonech jsou instalovány různé operační systémy. Mezi nejvíce rozšířené patří Google Android OS, Apple iOS, Window Phone a Blackberry. Na trhu se také snaží prosadit dva nové operační systémy, kterými je Symbian využívaný v telefonech Nokia a systém Bada, který je instalován na vybraných modelech Samsung.

Co do konstrukce jsou mobilní telefony rozděleny do několika kategorií. Největší podíl na trhu zaujímají chytré telefony, tzv. smartphony, které umožňují kromě volání a posílání SMS zpráv také přehrávání hudby, fotografování, natáčení videí, videokonferenci a připojení k internetu. Další kategorií jsou základní telefony, které poskytují pouze služby telefonování a zasílání SMS zpráv. Poměrně novou kategorií jsou odolné telefony, které vydrží velkou zátěž a jsou odolné proti pádu a poškrábání. Jsou většinou vodotěsné a jejich konstrukce má pogumovaný povrch. Tento druh mobilních telefonů je vhodný pro sportovce a osoby pracující v náročném terénu, kteří potřebují být ve stálém kontaktu se světem. Poslední kategorií jsou telefony pro seniory, jež se vyznačují velkými tlačítky a velkým čitelným displejem pro snadnější obsluhu staršími osobami. Tyto telefony ale nachází uplatnění i u osob s mírným zrakovým handicapem.

Kromě funkcí jako jsou Wi-Fi, Bluetooth, GPS, FM rádio, kamera, hudební přehrávač, svítilna, budík, kalendář, 3G, možnost duality SIM a NFC (peněženka v mobilu), jsou standardně do chytrých mobilních telefonů instalovány aplikace k přístupu do sociálních sítí Facebook a Twitter, dále také aplikace Skype, Gmail a YouTube. Na internetu jsou pak k dispozici ke stažení tisíce dalších různorodých aplikací.

3.4 Celulární síť

Celulární, nebo také buňková síť, je základní stavebním prvkem mobilních sítí. Celulární síť je rozdělena na buňky, v případě mobilní sítě se jedná o několik tisíc buněk, a každá tato buňka je pokryta signálem z přiděleného vysílače, tzv. základnové rádiové stanice BTS. Tyto buňky jsou prakticky fyzické území o určité velikosti, která je určena

mnoha faktory. Jiná územní velikost bude zvolena v hustě osídleném městě nebo na venkově, jiná v členitém terénu.

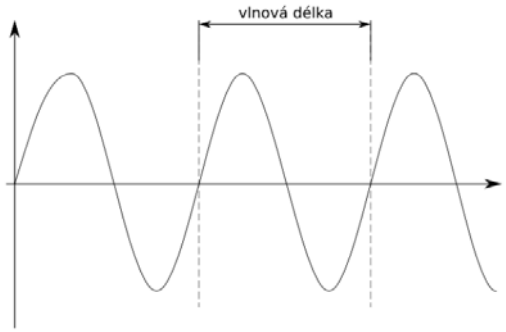
Několik buněk dohromady tvoří svazek buněk a komunikace takového svazku s okolními svazky je zajištěna pomocí základnové řídící jednotky BSC. BSC je řízena z radiotelefonní ústředny MSC, která koordinuje komunikaci účastníků jak ve vlastním svazku, tak s ostatními svazky.

3.5 Frekvence

V mobilních sítích probíhá komunikace přes radiové vlny. Radiové vlny jsou rozděleny na pásma a každému pásmu je přidělená určitá vlnová délka a frekvence. Mobilní telefony využívají frekvence 300 – 3000 MHz a dosahují vlnové délky 1 m - 100 mm. Toto konkrétní pásmo je využíváno také pro televizní vysílání a GPS.

Vlnová délka je vzdálenost mězi dvěma kmitajícími body vlnění.

Obrázek č. 4 Vlnová délka



Zdroj: zpracováno dle *http://cs.wikipedia.org/wiki/Soubor:Vlnova_delka.png*

Frekvence je fyzikální veličina udávající počet opakování periody v určitém časovém úseku.

Mobilní telefony fungují na různých frekvencích pomocí radiových vln. Frekvence jsou operátorům přidělovány podel určitých pravidel a jsou pro každého operátora omezené. A právě z důvodu omezení jsou pro různé hovory probíhající současně využívány stejné frekvence. Poskytovatelé mobilních služeb tak musí zajistit, že se souběžně probíhající hovory nebudou nijak rušit či ovlivňovat. To mohou zaručit jen vetší hustotou buněk celulární sítě.

3.6 Zpracování hlasu

Celý průběh přenosu hlasu se skládá z několika kroků. V první řadě je potřeba, pokud se k přenosu dat využívá digitální síť, převést hlas (akustickou energii) na digitální data (elektrickou energii). Tento proces se skládá z odběru vzorků analogového signálu a jeho následného zakódování a nazývá se zdrojové kódování. K přeměně signálu slouží RPE-LTP kodek, jež obsahuje jak kodér, tak dekodér. „*Při vstupu signálu do kodéru zdroje je rozdělen na úseky o velikosti 20 ms. Tyto bloky jsou kódovány v číslicovém filtru LPC a zároveň probíhá jejich analýza. Poté přejdou do filtru LTP, kde je signál sčítán se signálem filtru LPC a se svým zpožděným a vynásobeným obrazem se nazývá dlouhodobý odklad.*“[4] Výsledkem zdrojového kódování je signál, také nazývaný hovorový rámec, který obsahuje informace jak o samotném hovoru, tak o práci filtrů LPC a LTP. Do jedné vteřiny se vejde 50 hovorových rámců, každý o délce 260 bitů.

Dalším krokem je kanálové kódování, které má zabránit chybám signálu. Ten může být narušen například jiným zdrojem signálu, chyby signálu jsou zase způsobeny lomem, nebo rozptylem. Během kanálového kódování je hovorový rámec rozdělen do tří tříd podle významnosti a následně podle skupin zkontrolovány. Ke každé skupině je přičten určitý počet bitů, který náleží příslušným kódům. Výsledný hovorový rámec má po kanálovém kódování velikost 456 bitů.

Po kanálovém kódování přichází na řadu prokládání. Prokládáním se rozumí rozřazení bitů hovorového rámce do skupin, jehož účelem je zamezení vytváření shluků chyb. Každý hovorový rámec je rozdělen na osm částí, které jsou z obou stran proloženy čtyřmi částmi přechozího a následujícího rámce.

Jakmile jsou data proložena, dochází k šifrování dat. To se provádí za účelem ochrany proti odposlechu třetí stranou a probíhá tak, že po přihlášení do sítě zašle telefon tajný klíč, který se následně využije v algoritmu obsaženém v daném mobilním telefonu.

V závěrečné fázi dochází k modulaci signálu na nosnou vlnu. Modulace je prováděna pomocí modulátoru (elektronického obvodu), který ovlivňuje parametry původního signálu. Původní signál, také nazývaný modulační signál, je tak zkombinován s nosnou vlnou a vzniká výsledný signál, tvz. modulovaný signál. Modulovaný signál má

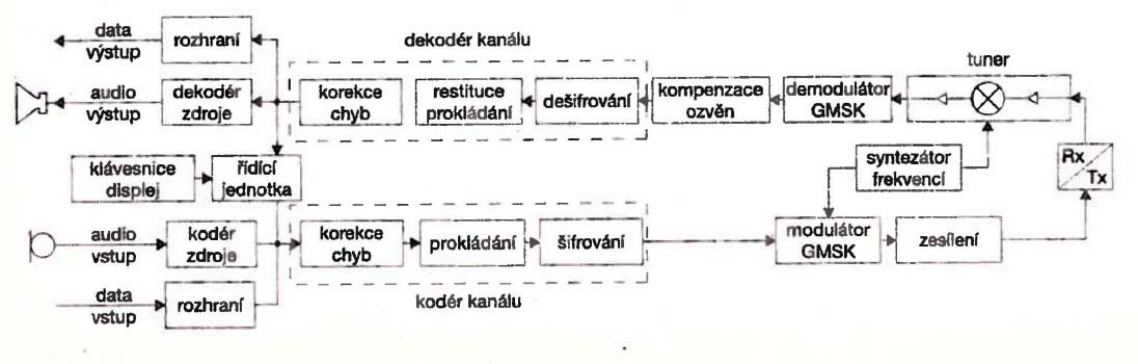
---

4 PROCHÁZKA, D., *Mobilní telefony: příručka pro stávající i budoucí majitele mobilu*, str. 71

podobné vlastnosti jako nosná vlna a je ho možné přenášet pomocí elektromagnetických vln nebo frekvenčního multiplexu.

Celý proces je znázorněn na následujícím obrázku.

Obrázek č. 5 Proces zpracování hlasu



Zdroj: zpracováno dle *Mobilní telefon, David Procházka, str. 72*

3.7 Generace mobilních sítí

3.7.1 Mobilní sítě první generace

Analogovou síť NMT vyvinuly ve spolupráci norské, švédské, finské a dánské telefonní společnosti a její první spuštění proběhlo v roce 1982. Tato síť využívala frekvence 450 MHz, dnes se však tato síť již téměř nevyužívá. Je nevhodně zabezpečená a pro komunikaci jsou používány velké a těžké telefonní přístroje. Mimoto sítě NMT neumožňují volání do zahraničí vzhledem k faktu, že se tyto sítě budovaly jako národní a tudíž jsou s ostatními vzájemně nekompatibilní.

Analogová síť AMPS byla první mobilní sítí v Americe a také první mobilní hovor z přenosného telefonu se uskutečnil v roce 1984 právě v této síti. Síť AMPS využívala frekvence 850 MHz a dnes se již tato síť také téměř nevyužívá.

Pro mobilní sítě první generace byla využívána přístupová metoda FDMA, respektive vícenásobný přístup s kmitočtovým dělením. Zde jsou pásma rozdělena na subpásma, kterým jsou dále přiděleny jednotlivé kanály, a komunikace účastníků probíhá na různých kmitočtech.

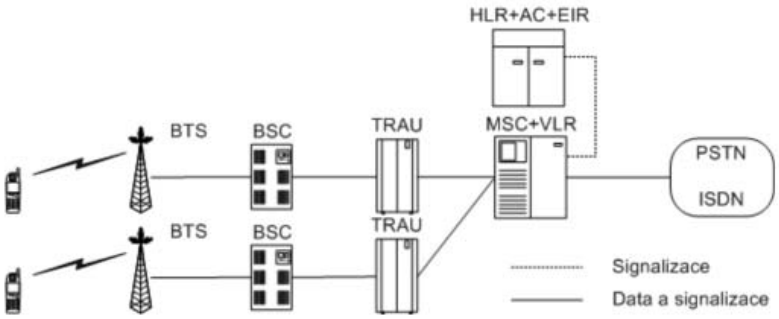
3.7.2 Mobilních sítě druhé generace

V roce 1992 byla uvedena do provozu síť nové generace, síť GSM. „*Díky použití digitální modulace zvuku je systém GSM mnohem složitější, než kterýkoliv analogový, zato*

při mnohem kvalitnějším přenosu zvuku i v extrémně obtížných podmínkách. Je to způsobeno zavedením systému zpětné korekce chyb.“[5]

Další mobilní sítě IDEN a IS-136 se používají v Americe a Kanadě, síť IS-95 je používána v Americe a některých částech Asie, a síť PDC je používána pouze v Japonsku.

Obrázek č. 6 Základní verze sítě GSM



Zdroj: zpracováno dle *http://www.umts.wz.cz/Mob_radio_site_3G/uvod_do_site_3G.htm*

V sítích GSM je používána metoda TDMA, tedy vícenásobný přístup s časovým dělením. Tato metoda rozděluje dané frekvenční pásmo na určité časové intervaly (rámce), které jsou přidělovány jednotlivým účastníkům komunikace.

Technologie GPRS, která je vylepšením GMS sítě, umožňuje přístup do sítě internet přidáním nových bloků jako paketový přenos přes IP protokol.

3.7.3 Mobilní sítě třetí generace

Mobilní sítě třetí generace podporují celosvětové roamingové propojení využívající stejné frekvenční pásmo. Tento systém se nazývá UMTS nebo také IMT-2000. „*Systém třetí generace UMTS by měl podporovat všechny služby zamýšlené pro pevné širokopásmové sítě (B-ISDN). Na rozhraní mezi mobilní stanicí a sítí se bude využívat pro přenos dat na principu CDMA (Code Division Multiple Access). Jedná se o metodu, kde je možné celé frekvenční pásmo ve stejném čase sdílet více účastníky pomocí kódového dělení. Účastníci budou komunikovat se sítí za využití WATM (Wireless Asynchronous*

[5] PROCHÁZKA, D., *Mobilní telefony: příručka pro stávající i budoucí majitele mobilu*, str. 21

Transfer Mode), který umožňuje garantovat požadovanou kvalitu služby. Zajímavá vlastnost UMTS je také to, že jako první systém umožňuje mezinárodní handover.“[6]

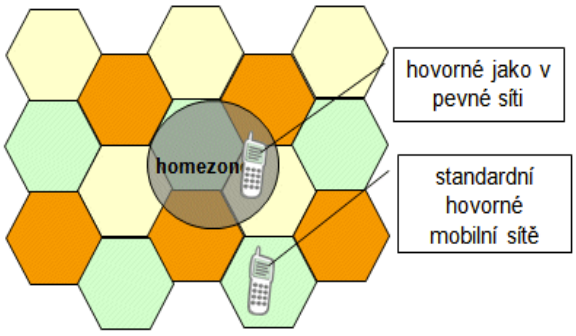
3.8 Propojení mobilních a pevných sítí

Dnes fungují oba typy mobilních a pevných sítí, odděleně a každá z nich má své výhody a nevýhody. Výhodou pevných sítí jsou kapacitní možnosti a výhodou mobilních sítí je zase mobilita. Jednou z možností je v budoucnosti úplná náhrada pevných sítí mobilními, druhou variantou je spojení a propojení toho „lepšího“ z obou typů sítí.

3.8.1 Fixně-mobilní substituce

„*Skutečná a dlouhodobě udržitelná služba fixně-mobilní substituce vypadá poněkud jinak. Například tak, jak ji v Německu nabízí tamní O2 v podobě služby Genion. Je založena na principu tzv. domácí zóny (homezone): zákazník oznámí svému mobilnímu operátorovi, kde je jeho domov (byt, kancelář atd.), a operátor kolem tohoto místa vytyčí pomyslný okruh, o průměru cca 300 až 500 metrů. Když pak uživatel volá ze svého mobilu, a přitom se nachází ve své domácí zóně (homezone), je jeho hovor zpoplatněn jako hovor z pevné sítě (tj. výhodněji). Pokud volá odjinud, je jeho hovor zpoplatněn jako klasický hovor z mobilní sítě (tj. je dražší).*“[7]

Obrázek č. 7 Představa služby fixně-mobilní substituce



Zdroj: zpracováno dle *http://www.earchiv.cz/b07/b0200003.php3*

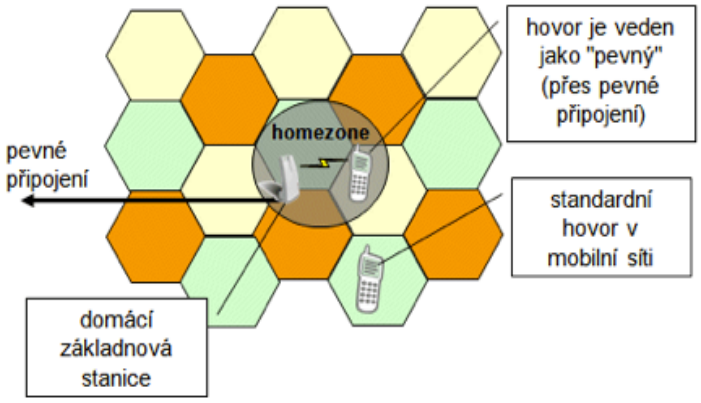
[6] Zpracováno dle *http://access.feld.cvut.cz/view.php?cisloclanku=2004072801*

[7] Zpracováno dle *http://www.earchiv.cz/b07/b0200003.php3*

3.8.2 Fixně-mobilní konvergence

„Také služby fixně-mobilní konvergence jsou typicky založeny na principu domácí zóny (homezone), podobně jako služby charakteru substituce. Ovšem oproti substituci, kde je rozdíl pouze ve způsobu zpoplatnění hovoru uvnitř a mimo domácí zóny, je zde rozdíl i v tom, jak je hovor veden. Pokud se totiž volající zákazník nachází uvnitř své domácí zónu, je jeho hovor veden skrze pevnou síť, resp. jeho pevné připojení (a mimo domácí zónu přes mobilní síť).“[8] A jak bude vypadat realizace? Domácnost bude muset být vybavena vlastním přístrojem, tzv. koncovou stanicí. Ta přijímá data z mobilního koncového zařízení a posílá je dál skrze pevnou síť. Komunikace koncové stanice s mobilním zařízením je realizovatelná pomocí Wi-Fi nebo Bluetooth (ovšem s koncovou stanicí mohou komunikovat pouze ty mobilní přístroje, které těmito funkcemi disponují), nebo klasickým způsobem na buňkovém principu a koncové zařízení se tak bude chovat jako BTS stanice v mobilní síti. Tyto nové buňky, nazvané femto buňkami, budou mnohem menší, než buňky v klasické mobilní síti.

Obrázek č. 8 Představa služby fixně-mobilní konvergence



Zdroj: zpracováno dle *http://www.earchiv.cz/b07/b0200003.php3*

V České republice je zatím v nabídce pouze konvergentní balíček fixně-mobilních služeb.

8 Zpracováno dle *http://www.earchiv.cz/b07/b0200003.php3*

3.9 Analogová versus digitální síť

„Analogová síť je nejstarší celulární sítí, kde se lidský hlas přenáší modulován analogovým signálem mezi telefonem a statutární stanicí.“[9] Vyhodnocuje se zde konkrétní hodnota přenášeného signálu, jako je například velikost napětí. Analogová síť je funkční na frekvenci 450 MHz.

Naopak pokud se vyhodnocuje příslušnost aktuální hodnoty do předem určeného intervalu, jedná se digitální přenos, resp. digitální síť. Digitální síť je nástupcem analogové sítě, umožňuje výborný přenos zvuku a poskytuje mnoho služeb, které analogová síť není schopná poskytnout. Digitální síť funguje na frekvenci 900, 1800 a 1900 MHz.

3.10 Hrozby a obrana

3.10.1 Funkce internetu

Internet je rozsáhlý globální otevřený informační systém vzájemně propojených počítačových sítí, ve kterých probíhá komunikace mezi počítači pomocí soustavy protokolů TCP/IP. Název TCP/IP vznikl spojením jmen dvou nejvýznamnějších protokolů z celé soustavy, protokolu IP a TCP protokolu. Protokol IP je protokolem síťové vrstvy a má za úkol přepravu dat na místo jejich určení, a to na principu paketového přenosu. TCP je transportním protokolem, který sám využívá služby IP protokolu, ale navíc garantuje spolehlivé doručování dat ve správném pořadí. Paket je blok dat přenášených v počítačové síti.

Internet pracuje pomocí protokolů TCP/IP, které jsou sice velmi odolné proti různým poruchám a jejich fungování je velmi efektivní. Bohužel je nutné podotknout, že jsou také nespolehlivé a nezabezpečené.

IP protokol původní data rozdělí do potřebného počtu bloků, které se nazývají datagramy. Tyto IP datagramy následně přenáší nespojovaným způsobem, přenášená data nešifruje a není předem známo, kudy budou datagramy cestovat. Jelikož mohou být „stejná data“ rozdělena do více datagramů, mohou cestovat různými cestami. Pokud se některá data poškodí, IP protokol to sice zjistí, ale nehledá, kde a proč se data poškodila, nezjedná nápravu a tato poškozená data zahodí.

---

[9] PROCHÁZKA, D., *Mobilní telefony: příručka pro stávající i budoucí majitele mobilu*, str. 22

Tento kanál lze zaměnit a použít TCP transportní protokol, který je spojovaný a navíc velmi spolehlivý. TCP sice nepoužívá kryptografické metody k zabezpečení přenášených dat, ale na aplikační vrstvě je možné použití šifrování nebo jiných zabezpečujících systémů a metod.

TCP/IP se skládá ze čtyř vrstev. Vrstva nejnižší úrovně se nazývá vrstvou síťového rozhraní. Tato vrstva řídí konkrétní přenosové cesty a stará se o příjem a vysílání paketů. Paket je formátovaný blok dat, který obsahuje IP adresu, atributy a data. Pakety jsou zabaleny do rámců, „obálek“, a tyto rámce poté putují po síti. O doručení paketů od odesílatele k příjemci se stará síťová vrstva a jejich přenos zajišťuje transportní vrstva. Nejvyšší vrstvou je vrstva aplikační, která zajišťuje přístup a komunikaci aplikací s transportní vrstvou.

V současném moderním světě se jako jeden z hlavních komunikačních kanálů využívá právě internet. Pomocí internetu lze získávat různé informace, provádět elektronické objednávky, platit za zboží, obchodovat, investovat, komunikovat se státními institucemi a úřady, nebo zasílat e-mailové zprávy. Internet je zdrojem poskytujícím mnoho různých služeb a informací.

Nicméně je na místě také otázka, zda to, co je na internetu, pochází z důvěryhodných zdrojů? Kam nebo komu se dostanou data internetu svěřená? Velkým nebezpečím na internetu jsou nejen lidé, kteří internet zneužívají k podvodným aktivitám, ale dalším slabým článkem je také chování aplikací. Některé aplikace požadují uživatelské údaje, jako je přihlašovací jméno a heslo, ale přitom tyto údaje přenáší nezabezpečeně a data nešifrují. Ta potom putují sítí jako čistý otevřený text, který je snadno zneužitelný.

3.10.2 Bezpečnost dat

Proč se vůbec zabývat bezpečností dat na internetu? O jaká data je zájem, koho mohou útoky postihnout? Kdo by měl zájem o data „obyčejného“ běžného uživatele?

Každý člověk je specifický a má jiné znalosti a známosti. Z pohledu útočníka může jít také o různé druhy zájmu. Níže je uveden výčet nejtypičtějších druhů útoků.

Finanční zainteresovanost

- útoky jsou uskutečňovány s cílem získání bezpečnostních údajů k platební kartě nebo bankovnímu účtu

Konkurence nebo zášť

- dochází zde k útoku na server za účelem jeho zpomalení, nebo úplného selhání, útok je prováděn z důvodu budoucí ztráty zákazníků nebo vydírání
- provádí se zpravidla u společností, jejichž existence závisí na internetu, jako jsou internetoví obchodníci nebo zpravodajské servery

Spamové útoky

- útok je zaměřen na získání seznamu kontaktů a následnou distribuci spamových zpráv

Vyzvědění tajných dat

- útok je cílený za zjištěním utajovaných dat, které mohou být ku prospěchu útočníka

Útok na osobu

- záměrné cílené chování útočníka s cílem poškodit oběť, popřípadě může docházet k vydírání oběti

Zábava a ego

- překonání bezpečnostních systémů čistě ze zábavy, případně si útočník chce dokázat, že on je nepřekonatelný

K poškození či zneužití dat může dojít buď záměrně, nebo neúmyslně.

Neúmyslné hrozby jsou většinou způsobeny chybou v systému, nevědomým jednáním uživatele, lidským selháním, špatným fyzickým zabezpečením mobilního telefonu, hardware při přetížení nebo také špatně napsaným software.

Ty úmyslné jsou způsobeny záměrně s cílem získání dat nebo poškození oběti. Při úmyslném zneužití mohou být získaná data ponechána nepozměněna, nebo jsou změněna, ať už obsahem, nebo v místě paměti. Útočník však využívá výhody jejich znalosti.

3.10.3 Zajištění přístupu

Bezpečnost informací a dat zasílaných přes internet je zajištěna pomocí ověřovacích a kryptografických nástrojů. Mezi nejdůležitější patří identifikace, autentizace, autorizace, zachování integrity dat, auditing, zajištění důvěrnosti dat, neodmítnutelnosti autorství a zachování dostupnosti. Níže je uveden jejich krátký popis, a jakou funkci v oblasti bezpečnosti zastávají.

Identifikace

- slouží k určení, identifikaci, autora / subjektu / objektu

- provádí se na základě shody identifikačních charakteristik se záznamy v databázi
- určuje se pomocí ID čísla zaměstnance, ID karty, biometriky (otisk prstu, apod.)

Autentizace, nebo také verifikace

- ověření, že příslušné údaje o autorovi / subjektu / objektu souhlasí
- ověřuje se na základě znalostí (PIN či vstupní heslo), vlastnění určité věci (například přístupová ID karta) nebo tím, čím autor / subjekt / objekt je (biometrické měření)
- je možné kombinovat výše uvedené metody autentizace

Autorizace

- souvisí s oprávněním určitého uživatele k přístupu či nějaké aktivitě
- uživatelům se na základě identity přiřazují různá oprávnění a přístupy na základě seznamu oprávnění a řízení přístupu

Pro ověření zachování integrity dat se zjišťuje, zdali původní data nebyla změněna.

Důvěrnost dat je zajištěna pomocí šifrování, které zaručí, že nikdo nepověřený důvěrná data nepřečte.

Auditing naopak poskytuje informace o historii činností, to znamená informaci o tom, kdo kdy a co udělal. Tyto informace jsou výhodné pro případné řešení incidentů.

3.11 Problematika ochrany dat

S rozvíjejícími možnostmi techniky a informačních technologií se musí stále častěji myslet na ochranu osobních dat. Každá organizace si vede vlastní databáze, ať už se jedná o zákazníky, obchodní partnery nebo občany státu. Tyto databáze obsahují kompletní informace, počínaje jménem a příjmením, adresou, mobilním telefonem a e-mailem konče. V případě klubových karet obchodníků i souborné statistické údaje o tom, co který zákazník nakupuje, v jakém množství a kdy. Tyto informace lze využít při plánování zásob nebo výroby. U státních organizací a úřadů jsou pak evidována další soukromá data. Všechna tato data poskytují přesný obraz o dané osobě a lze jich snadno zneužít.

„*Osobní data každého občana jsou evidována v mnoha registrech občanů, přes základní školu, databanku řidičských průkazů, zdravotní pojišťovny, různé zájmové kluby až po ty nejneočekávanější případy, jako je například placení televizních poplatků. Policie, úřady a soukromé organizace přímo hamižně shromažďují veškeré možné informace*

o každém občanovi.“[10] Takto vytvořené databáze jsou snadno zneužitelné, ať už se jedná o útok zvenčí nebo zevnitř. Se souhornými daty se dá obchodovat nebo je využít z hlediska marketingových obchodních strategií.

V současnosti jsou technologie mobilních telekomunikací na vysoké úrovni. Za velmi praktické funkce je možné označit určování aktuální polohy mobilního telefonu a vyhledávání v mapách. Lokalizace mobilních telefonů s sebou ale přináší i rizika, uživatel tím vlastně dobrovolně dává svolení ke zjištění informací o tom, kde se právě nachází. Tato informace opět může být využita k lokální marketingové propagaci či útoku na konkrétní osobu, či její majetek.

„*Odposlouchávání v síti GSM je relativně snadné, jestliže uživatel mobilního telefonu volá na pevnou síť. Rozhovor jde z mobilu k základnové stanici, odtud k MSC [Mobile Switching Center] a pak do pevné sítě. V MSC je instalováno odposlouchávací zařízení, které zachytí každý hovor.*“[11] V některých zemích se i dnes stále používají nekódované přenosy v síti GSM. Potom je i odposlech komunikace při volaní z jednoho mobilního telefonu na druhý velmi snadné. Při odposlechu je narušeno uživatelovo soukromí, může docházet k jeho vydírání nebo šikanování, či zneužití jeho citlivých dat.

„*V březnu roku 1996 představil jeden americký podnik svůj odposlouchávací systém pro síť GSM. Zařízení se jmenuje IMSI-Catcher, ale neslouží k odposlouchávání, jak se mnohokrát tvrdilo, umí pouze obstarat informace, které špehování umožní. K odposlouchávání mobilních telefonů potřebujete totiž znát jeho IMSI [Inernational Mobile Subscriber Identity]; to je kód, který je vyslán při navazování spojení. Jestliže telefonujete mobilem, vyšle telefon svůj kód zařízení IMSI- Catcher, které se však musí nacházet poblíž mobilu*“[12] Tak lze následně zahájit odposlech, protože daný přístroj vydá příkaz k nekódovanému přenosu dat.

„*Ačkoliv se tato skutečnost neustále popírá, používají veškeré tajné služby na světě speciální scannery, které reagují na vyslovení určitých slov.*“[13]

---

[10] REISCHL, G., *Sběratelé elektronických dat pod lupou*, úvodem

[11] REISCHL, G., *Sběratelé elektronických dat pod lupou*, s. 17

[12] REISCHL, G., *Sběratelé elektronických dat pod lupou*, s. 17

[13] REISCHL, G., *Sběratelé elektronických dat pod lupou*, s. 21

„Extrémně složité jazykové scannery sledují hovory a automaticky se zapojí, jakmile zaznějí určitá klíčová slova. Tyto „hity" mezi slovy se týkají oblasti obchodu s drogami a zbraněmi nebo terorismu. Jejich seznam je přísně tajný. Jazykový scanner se pravděpodobně uvede do provozu při slově „kalašnikov", ještě mnohem choulostivější než toto slovo jsou však pro agenty BND ruské a čínské výrazy, které jsou rozšířeny mezi ruskou mafií či v čínských Triádách."[14]

Samozřejmě může docházet k oficiálnímu odposlechu osob, ať už vinných nebo nevinných. To se může stát například vyslovením výše zmíněných klíčových slov, ať už z legrace nebo nevědomosti. Pak jsou osoby odposlouchávány z důvodu podezření ze spáchání trestného činu, případně v souvislosti známosti s jinou podezřelou osobou. Ve většině případů jsou tyto odposlechy spíše kratšího trvání. V České republice je pak povinností státního zástupce nebo policejních složek po ukončeném vedení odposlechů odposlouchaného o provedeném odposlechu informovat.

„Důvěrná a tajná sdělení by se neměla posílat faxem, protože i fax lze „napíchnout". Stačí, když se na paralelní přípojku napojí druhý faxový přístroj. To lze udělat jak v domě, kde se fax nachází, tak i v centrále. Pak může každou faxovou zprávu, kterou dostane přístroj A, vytisknout i přístroj B – aniž by to uživatel faxu zpozoroval."[15]

Dále existují statistická sledování přístrojů. *„Systém vyhlásí poplach v případě něčeho neobvyklého, při netypickém chování během telefonátu. Jestliže někdo telefonuje průměrně desetkrát za den a najednou se frekvence jeho volání zvýší na sto. Jestliže náklady na telefon ze dne na den prudce stoupnou, nebo když se z jednoho telefonu vedou nápadně dlouhé hovory. Pomocí časového faktoru lze usuzovat i na možné pirátské kopie SIM-karet. Není možné telefonovat z jednoho mobilního telefonu ve 12 hodin z Hamburku a o hodinu později z Darmstadtu. Ve všech těchto případech se může stát, že se najednou za dveřmi objeví specialisté na boj s podvodníky.*"[16]

Velkým problémem jsou nepochybně databáze, ve kterých se evidují telefonní čísla se jmény majitelů včetně jejich adresy. Pokud se k tomu přidá možnost kontroly mobilního telefonu pomocí GPS a tím i sledování polohy, je soukromí uživatele opět narušeno.

---

[14] REISCHL, G., *Sběratelé elektronických dat pod lupou*, s. 22

[15] REISCHL, G., *Sběratelé elektronických dat pod lupou*, s. 27

[16] REISCHL, G., *Sběratelé elektronických dat pod lupou*, s. 32

3.12 Legislativa

Níže jsou uvedeny nejdůležitější zákony a vyhlášky, které v České republice oblast mobilních komunikací a informační bezpečnosti upravují.

Oblast mobilních komunikací upravuje a vymezuje Zákon 151/2000 Sb., o telekomunikacích. V platnost vešel dne 16. května 2000 a „*upravuje ve věcech telekomunikací:*

a) podmínky pro zřizování a provozování telekomunikačních zařízení a telekomunikačních sítí,

b) podmínky pro poskytování telekomunikačních služeb,

c) výkon státní správy včetně regulace.“[17]

V paragrafu 35 a odstavce a) je uvedeno, že *držitel telekomunikační licence k poskytování veřejné telefonní služby je povinen vést aktuální databázi všech svých účastníků veřejné telefonní služby.*“[18]

Dále se v paragrafu 84 odstavce (1) pojednává o ochraně osobních a zprostředkovacích dat. Je zde uvedeno: „*Právnické nebo fyzické osoby, které vykonávají telekomunikační činnosti, jejich zaměstnanci a jiné osoby, které se podílejí na vykonávání telekomunikačních činností, nesmějí získávat pro jiné než pracovní účely, vyplývající z jejich telekomunikační činnosti, informace o skutečnostech, které jsou předmětem telekomunikačního tajemství ve větší míře, než je pro vykonávání telekomunikačních činností nezbytně nutné.*“[19] Předmětem obchodního tajemství je veškerý obsah neveřejných zpráv, údaje o účastnících komunikace a „*provozní doklady, z jejichž obsahu je zjevný obsah přepravovaných zpráv*“.[20]

---

[17] Systém ASPI [počítačový program]. *Verze 2013 pro Microsoft Windows. Praha: Wolters Kluwer ČR, a. s.* Systém pro práci s právními informacemi

[18] Systém ASPI [počítačový program]. *Verze 2013 pro Microsoft Windows. Praha: Wolters Kluwer ČR, a. s.* Systém pro práci s právními informacemi

[19] Systém ASPI [počítačový program]. *Verze 2013 pro Microsoft Windows. Praha: Wolters Kluwer ČR, a. s.* Systém pro práci s právními informacemi

[20] Systém ASPI [počítačový program]. *Verze 2013 pro Microsoft Windows. Praha: Wolters Kluwer ČR, a. s.* Systém pro práci s právními informacemi

Dalším významným zákonem, a to ve vztahu k elektronické komunikaci, je Zákon č. 127/2005 Sb., o elektronických komunikacích. Tento zákon vešel v platnost 22. února 2005, a „*upravuje na základě práva Evropské unie podmínky podnikání a výkon státní správy, včetně regulace trhu, v oblasti elektronických komunikací*“.[21] V tomto zákoně je dále v paragrafu 75 uvedeno následující: „*Je-li to technicky proveditelné, je podnikatel poskytující veřejně dostupnou telefonní službu prostřednictvím veřejné mobilní telefonní sítě povinen na základě písemné žádosti Policie České republiky a na její náklady pro účely trestního řízení znemožnit na požadovanou dobu, nejdéle však na dobu povoleného odposlechu, provozování koncového mobilního telekomunikačního zařízení (mobilní telefonní přístroj) ve veřejné mobilní telefonní síti, který umožňuje šifrování, kódování nebo jiný způsob utajení přenášené zprávy účastníkem.*“[22]

Zákon č. 141/1961 Sb., o trestním řízení soudním, se v celé sedmé části věnuje odposlechu a záznamu telekomunikačního provozu.

V červnu loňského roku byl tehdejší vládě předložen návrh na nový zákon o kybernetické bezpečnosti a v lednu letošního roku vláda České republiky *“schválila Návrh zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Tento návrh zákona připravil a předložil Národní bezpečnostní úřad. Návrh zákona bude předložen k dalšímu legislativnímu projednávání v Parlamentu České republiky.*“[23]

---

[21] Systém ASPI [počítačový program]. *Verze 2013 pro Microsoft Windows. Praha: Wolters Kluwer ČR, a. s.* Systém pro práci s právními informacemi

[22] Systém ASPI [počítačový program]. *Verze 2013 pro Microsoft Windows. Praha: Wolters Kluwer ČR, a. s.* Systém pro práci s právními informacemi

[23] Zpracováno dle *http://www.govcert.cz/cs/legislativa/legislativa/*

4. PRAKTICKÁ ČÁST

V této části je popsán analyzovaný mobilní telefon, jeho výrobce a použitý operační systém. Detailně jsou pak rozebrány různé druhy a metody útoků a hrozeb, a s tím spojená rizika související s daným mobilním telefonem. Ke každému druhu útoku nebo hrozby jsou uvedena konkrétní řešení, včetně doporučení pro uživatele nebo návodu k nastavení bezpečnostních prvků na mobilním telefonu.

4.1 Analyzovaný přístroj

Pro účely této práce slouží jako pokusné zařízení mobilní telefon HTC Wildfire S A510e s operačním systémem Android verze 2.3.3 Gingerbread. Jeho parametry jsou následující:

„Rozměry

- *Rozměry 101,3 x 59,4 x 12,4 mm*
- *Váha 105 g*

Displej

- *Rozlišení displeje 320 x 480 px*
- *Barvy 256 000*
- *Plně dotykový TFT 3,2"*

Rozhraní

- *Bluetooth*
- *WiFi*

Datové přenosy

- *GPRS, EDGE, UMTS / 3G, HSDPA, HSUPA*
- *EDGE třída 10*
- *GPRS třída 10*
- *Max. počet aktivních timeslotů 5*
- *GPRS speed UL 2*
- *GPRS speed DL 4*

Prohlížeč internetu

- *WAP*

Podporované sítě

- *WCDMA 850/900/1900/2100 MHz; GSM 850/900/1800/1900 MHz*

Napájení

- *Délka hovoru (max - hod): 7*
- *Pohotovostní režim (max - hod): 360*
- *Baterie Li-on 1230 mAh*
- *Doba nabíjení (hod.): 2*

Audio a video

- *Podporované formáty audia*
- *Přehrávání:.aac, .amr, .ogg, .m4a, .mid, .mp3, .wav, .wma (Windows Media Audio 9)*
- *Záznam:.amr*

Podporované formáty videa

- *Přehrávání:.3gp, .3g2, .mp4, .wmv (Windows Media Video 9)*
- *Záznam:.3gp*

Konektivita

- *3,5 mm stereo audio jack*
- *Standardní micro-USB (5-pin micro-USB 2.0)*
- *HSDPA až 7,2 Mbps*
- *WiFi: IEEE 802.11b/g/n*
- *Bluetooth Bluetooth® 3.0 s FTP/OPP pro přenos souborů*
- *A2DP pro bezdrátová stereo sluchátka*
- *PBAP pro přístup k telefonnímu seznamu z autosoupravy*

Snímače

- *G-Sensor*
- *Digitální kompas*
- *Snímač přiblížení*
- *Snímač světla prostředí"*[24]

---

[24] Zpracováno dle *http://www.o2.cz/osobni/techzona-mobilni-telefony/htc-wildfire-s.html?tab=techinfo*

4.1.1 Výrobce HTC

Společnost HTC Corporation byla založena v roce 1997, ale až v roce 2006 vstoupila na trh mobilních telefonů a tabletů. Zpočátku vyráběla společnost HTC přístroje pouze pro mobilní operátory, až později se zaměřila na produkci pod vlastní značkou. Mobilní zařízení HTC jsou osazena operačními systémy Android a Windows Phone.

4.1.2 Operační systém Android

Mobilní operační systém Android byl vytvořen společností Google Inc., po akvizici společnosti Android Inc. v roce 2005 a je jedním z nejrozšířenějších mobilních operačních systémů. V roce 2013 bylo celosvětově aktivováno více než jeden bilion mobilních telefonů a/nebo tabletů právě s operačním systémem Android.

Architektura Androidu se skládá z operačního jádra, knihoven, virtuálního stroje, vrstvy pro přístup k aplikačním službám a základní aplikační vrstvě. Operační jádro slouží jako pomyslná vrstva mezi hardware a ostatním software. Je postaveno na Linuxu, čímž je zajištěna přenositelnost na různá zařízení. V další vrstvě architektury jsou knihovny. Jedná se o soubory ve strojovém kódu, které obsahují souhrn dostupných funkcí a procedur pro propojení s programem, nebo bežícím procesem. Další vrstva obsahuje virtuální stroj Dalvik, který zajišťuje překlad Java kódu. Pak následuje vrstva aplikačního frameworku, která zajišťuje podporu pro programování a vývoj systémových aplikací. Nakonec je zde základní aplikační vrstva, která slouží běžným uživatelům a obsahuje předinstalované aplikace z výroby nebo uživatelem stažené aplikace z Google Play. Google Play jsou webové stránky, nazvané market, poskytující ke stažení různé aplikace pro platformu Android.

Ve srovnání s dalšími operačními systémy pro mobilní telefony, jako jsou Apple iOS, Window Phone nebo Blackberry, je Android častěji a snadněji napadnutelný a také nejméně bezpečný. To je dáno několika fakty. V první řadě, Android je otevřený operační systém. To znamená, že je jeho zdrojový kód veřejně přístupný, lze si jej prohlížet a v případě dodržení určitých podmínek také upravovat. Dále jsou veřejně k dipozici informace o komplexním řešení operačního systému, pro testování a vývoj aplikací je k dispozici speciální vývojářský nástroj Software Development Kit. Velmi riziková z hlediska bezpečnosti je možnost získání administrátorských oprávnění, tzv. root telefonu. Pokud jsou na mobilním telefonu získána oprávnění uživatele „root“, původní

bezpečnostní nastavení již nejsou funkční a v případě instalace škodlivého software nelze zabránit neoprávněné manipulaci s daty.

Dalším důvodem častějšího útoku na systém Android je také fakt, že je to aktuálně nejrozšířenější mobilní operační systém.

4.1.3 Statistické údaje

Podle statistických údajů za rok 2013 zveřejněných analytickou společností IDC z 27. ledna 2014 se za rok 2013 prodala jedna miliarda kusů mobilních telefonů, respektive smartphonů. Podíl na trhu za rok 2013 byl 31,3 % smartphonů od společnosti Samsung, poloviční podíl zaujímala značka Apple a daleko za nimi s přibližně stejným 5 %tním podílem smartphony značek Huawei, LG a Lenovo. Za rok 2013 se celkem prodalo o 38,4 % smartphonů, resp. o 278,9 milionů kusů přístrojů, více než v roce 2012.

Dále podle statistik stejné společnosti z 12. listopadu 2013 zaujímal mobilní operační systém Android vedoucí pozici na trhu, a to s 81 % podílu. Jen za třetí čtvrtletí se prodalo 261,1 milionů kusů mobilních telefonů (smartphone), z čehož na 211,6 milionech z nich byl nainstalován operační systém Android. V porovnání se stejným obdobím přechozího roku, kdy Android ukrojil 74,9 % podílu na trhu, a dalšími čtvrtletními statistikami společnosti IDC je možno konstatovat, že jeho podíl na trhu stále roste.

4.2 Bezpečnost dat

4.2.1 Škodlivý software

Uživatelé osobních počítačů všeobecně znají problematiku škodlivého software, malware a virů, které mohou napadnout jejich počítače. Většina si také svůj počítač proti takovému software chrání alespoň instalací antivirového programu. Avšak jen málokterý uživatel mobilního telefonu chrání svůj přístroj vhodným antivirovým programem nebo jiným komplexním ochranným systémem.

Co může takový škodlivý software způsobit?

- volání a posílání SMS zpráv za velmi vysoký volací tarif
- zcizení osobních dat z telefonu
- vzdálené nahlížení do mobilního telefonu
- změny a úpravy systémových aplikací
- blokování paměťové karty
- posílání spamových zpráv podle lokalizace

O soukromá data z mobilních telefonů je velký zájem, počty nových škodlivých programů a sofware rychle narůstají. Níže jsou některé z nich blíže popsány.

Program, který pomocí internetu odesílá data z počítače, aniž by o tom sám uživatel věděl, se jmenuje spyware. Mezi druhy spyware patří například ty, které nabízejí při práci na internetu obtěžující reklamní informace, dále takové, které sledují stisky klávesnice nebo existují i takové, které umožňují autorovi spyware vzdálený přístup do napadeného počítače. Ochranu proti spyware zajišťují antispyware programy, které škodlivé programy dokáží spolehlivě nalézt, blokovat a odstraňovat. Jsou obsaženy v komplexním antivirovém systému, ale není na škodu mít nainstalovaný speciální antispyware program. To proto, že každý antivirový nebo antispyware program může obsahovat různé virové databáze. Dalším škodlivým software jsou nevyžádaná sdělení šířená přes internet, většinou komerčního rázu. Nazývají se spam, nebo také „junk mail“. Dříve se do spamu řadily pouze e-maily s reklamním sdělením, v současnosti jsou však postižena také diskusní fóra a další druhy internetové komunikace. Program, který chrání uživatele před nevyžádanou poštou, se nazývá antispam.

Oba výše uvedené ochranné programy se instalují do počítačů, tabletů, a v současnosti už i do mobilních telefonů, buď pod jedním antivirovým systémem, případně zvlášť jako jednotlivé programy. V případě stálého připojení do internetové sítě, se programy automaticky aktualizují a poskytují tím nejvyšší možnou ochranu. V případě občasného připojení do internetové sítě se jejich aktualizace provádí v čase připojení a podle rychlosti připojení probíhá aktualizace různě dlouhou dobu. Pak je vhodné před další prací na internetu počkat na stažení a instalaci všech aktualizací.

Jiný škodlivý software, který je velmi specifický, je trojský kůň. Ten po instalaci do systému sbírá a odesílá data. K útoku pomocí trojského koně může dojít prostřednictvím instalace neznámé a neověřené aplikace, kterou si uživatel instaluje sám, případně dojde k nevědomému nainstalování škodlivého programu odkliknutím odkazu obdrženého v SMS. Uživatel vůbec netuší, že si s vybranou aplikací nainstaloval také trojského koně, avšak ten mezitím odesílá ukradená data svému tvůrci. Poměrně čerstvým příkladem útoku trojského koně je útok na Tibetské a Ujgurské aktivisty a obhájce lidských práv, který odhalili experti ze společnosti Kaspersky Lab. Škodlivý malware s trojským koněm, speciální „ušitý na míru“ pro systém Android, byl zaslán účastníkům konference v příloze e-mailu s odkazem na Světovou Ujgurskou konferenci (World Uyghur Conference)

konanou 22. března 2013. Podle expertů z Kaspersky Lab se jednalo o vůbec první útok zaměřený na smartphony se systémem Android.

Novým a zajímavým způsobem možného infikování je malware z března 2013, který se umí přesunout z Androidu do počítače poté, co je telefon k počítači připojen. Další novinkou jsou také podvodné e-mailové zprávy typu „potvrzení objednávky“. Do inboxu uživatele je doručen e-mail, který slouží jako potvrzení nikdy neprovedené objednávky. Vypadá jako klasický potvrzovací e-mail, na konci kterého je vložena věta s odkazem „Pokud chcete objednávku změnit nebo zrušit, klikněte na tento odkaz“. Žádné další kontaktní údaje nejsou uvedeny a společnost ani nelze dohledat v rejstříku existujících firem. Pokud uživatel v okamžiku překvapení klikne na odkaz, pravděpodobně neunikne instalaci škodlivého software do svého mobilního telefonu.

Řešení

Bránit se proti obdržení či nainstalování škodlivého software, malware či virů lze pomocí antivirových systémů, případně speciálních antispyware a antispam programů. Pro mobilní telefon analyzovaný v této práci je vybrán antivirový systém avast! Free Mobile Security, který je zdarma ke stažení na oficiálních webových stránkách.

Obrázek č. 9 Antivirový software

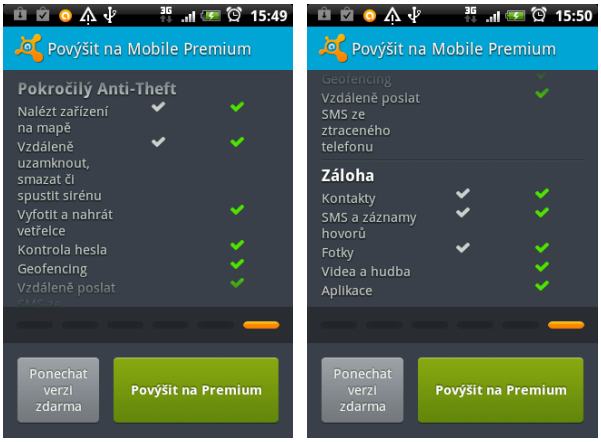
Zdroj: zpracováno dle *vlastní zdroj*

Tento antivirový systém nabízí ochranu před malware a podvodnými aplikacemi, umí filtrovat příchozí hovory a SMS nebo varovat před nebezpečnými webovými stránkami. Byl testován nezávislou organizací AV-Test a vyhodnocen jako jeden

z nejlepších antivirových systémů pro platformu Android. Lednový test v roce 2014 ukázal, že Avast odhalil více než 98,7 % hrozeb.

Pro nainstalování antivirového systému je nutné akceptovat a povolit aplikaci přístupy zobrazené na obrázku níže. Pokud jsou tyto přístupy akceptovány, jsou vlastně aplikaci povolena veškerá práva k ovládání daného telefonu.

Obrázek č. 10 Povolení práv a přístupu aplikace

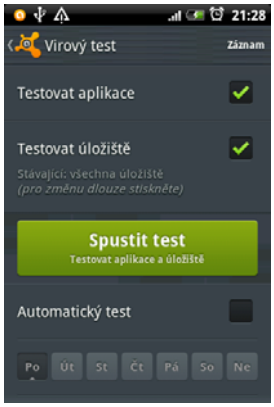


Zdroj: zpracováno dle *vlastní zdroj*

Po stažení a úspěšné instalaci antivirového programu je následně nutné odsouhlasit licenční ujednání, které je dostupné jen v anglickém jazyce a souhlasit s ochranou osobních údajů. Po schválení je již aplikace připravena k použití.

Nyní je vhodné telefon nechat zkontrolovat pomocí virového testu. Při vůbec první kontrole mobilního telefonu je doporučeno provést kompletní test, tedy včetně úložiště.

Obrázek č. 11 Virový test



Zdroj: zpracováno dle *vlastní zdroj*

Mezi funkcemi zahrnutými v nainstalované verzi je také například správa aplikací. Ta nám po vybrání dané aplikace poskytuje informace o systémových zdrojích jako je velikost, zda je aktuálně využívaná paměť (běžící aplikace), nebo kdy byla aplikace naposledy použita. Nainstalované aplikace je možné vytřídit na aktuálně běžící nebo všechny aplikace. Nakonec jsou k dispozici informace o datových přenosech, kde je na výběr kontrola pro aktuální den, měsíc nebo rok.

Dále je obecně doporučeno nestahovat neznámé a neověřené aplikace a neklikat na odkazy v obdržených SMS nebo e-mailech, ale také nenavštěvovat nevhodné internetové stránky s podezřelým obsahem.

Mimo výše uvedené je na místě upozornění na (ne)instalaci antivirového programu Android Defender, což je falešný antivirus, který po instalaci zablokuje telefon a poté po uživateli telefonu požaduje výkupné.

4.2.2 Phishing

Proč je phishing zahrnutý do samostatné kapitoly? Protože je extra nebezpečný! A mnohdy tak nenápadný, že si uživatel nemusí vůbec všimnout, že se stal jeho obětí.

Phishing je forma útoku s cílem získání přístupových údajů do bankovního on-line účtu uživatele, k bankovním kartám nebo informacím z bankovního účtu. Phishingový útok je prováděn metodou falešné identity známé webové stránky, respektive banky uživatele. Uživatel obdrží e-mailovou zprávu, naprosto nerozeznatelnou od klasické, běžně doručované bankovní korespondence. V ní je vyzván, zpravidla pomocí varovné zprávy, aby kliknul na uvedený odkaz ve zprávě. Ten ho přesměruje na formulář, kde uživatel zadá svoje přihlašovací údaje. Tento formulář je naprosto věrohodně vypadající, ale po vložení a odeslání údajů tyto údaje putují přímo k útočníkovi. Jinou formou útoku je umístění formuláře přímo do textu e-mailu. Další prováděnou metodou je útok na server banky. V tomto případě je po zadání korektní webové adresy banky v prohlížeči uživatel přesměrován na falešné, ale identicky vypadající, stránky. V tuto chvíli opět uživatel po zadání svých údajů odesílá svá data tvůrci spamu.

Řešení

Je vhodné vytvořit a používat několik e-mailových účtů, minimálně ale dva. Jeden k soukromým a druhý k veřejným účelům. Privátní e-mail by měl sloužit jen ke komunikaci s rodinou a přáteli a dále ke komunikaci s bankami nebo jinými finančními

institucemi. Adresu na privátní e-mail není dobré veřejně sdělovat, naopak je nutné její název střežit a nazadávat při registraci u obchodníků nebo do jiných registračních formulářů při zakládání různých služeb internetu. Pokud musí být privátní adresa uvedena například na webových stránkách uživatele jako kontaktní údaj, je lepší emailovou adresu napsat ve formátu jmeno-zavinac-seznam.cz, protože takto uveřejněná adresa se obtížněji hledá automatickými vyhledávači nebo tvůrci spamových zpráv. Tvůrci spamu také často odhadují formu e-mailové adresy, takže je vhodnější vytvořit e-mailový účet v kombinaci s dalšími znaky, písmeny nebo čísly, ne pouze ze jména a příjmení.

Veřejná e-mailová adresa pak tedy slouží ke všem ostatním úkonům na internetu, nežli jsou ty privátní. Čím častěji svou adresu na internetu uživatel sdílí, tím vetší je riziko, že se dostane na seznam spamu. A to poměrně rychle.

Pokud se chce uživatel vyvarovat vykradenému účtu, rozhodně by neměl odpovídat na spamové zprávy obdržené v e-mailu a ani je dál přeposílat dalším příjemcům. Dalším trikem tvůrců spamu je možnost zakliknutí „nepřeji si, aby mi byly tyto e-maily dále zasílány“. Ve chvíli, kdy na daný odkaz uživatel klikne, odešle svou e-mailovou adresu na seznam příjemců spamu.

Je také doporučeno nastavení si spamových filtrů v e-mailové schránce nebo zajištění spamového klienta, který veškeré zprávy tohoto typu zachytí a do emailu uživatele doručí pouze ty nepodezřelé.

Na závěr je uvedeno doporučení ohledně vyhledávače. Měl by být vždy aktualizovaný a uživatel by měl kontrolovat adresu webové stránky, na kterou je přesměrováván. V souvislosti s mobilními telefony je tuto kontrolu obtížnější provádět, vzhledem k tomu, že se nezobrazuje celá adresa přesměrovávané webové stránky. Nešikovným řešením je také zkracování webových adres, jako se to děje nejen u mobilních telefonů, ale například také u sociálních sítí, kde je pak pod zkrácenou verzí ukryt mnohem delší odkaz na falešné webové stránky.

4.2.3 Firewall

Dalším bezpečnostním prvkem je firewall. Jedná se o síťové zařízení, které kontroluje informace přicházející z internetu, respektive vnějších a cizích sítí. Podle nastavení firewall informace a data buď zablokuje, nebo jim umožní projít do počítače, respektive do mobilního telefonu. Firewall tedy brání přístroj uživatele před útočníky a škodlivým software, je pomyslnou zdí mezi lokální sítí a ostatními sítěmi. Dále firewall

dokáže zabránit rozesílání škodlivého software do dalších přístrojů připojených do internetové sítě.

Řešení

V této práci analyzovaný mobilní telefon neumožňuje ve své původní softwarové verzi nastavení firewallu. Firewall ale lze také nastavit prostřednictvím antivirového systému, ale k tomuto úkonu je potřeba, aby měl daný telefon práva uživatele „root".

Root ve své podstatě umožňuje administrátorská práva pro uživatele, která v původním stavu zařízení nejsou uživateli přístupná. Rootování telefonu jinými slovy znamená přepsání originálního software telefonu a možnost měnit chování samotného operačního systému. Pokud se provede root, současně se u nainstalovaných aplikací zobrazí nabídka SuperUser. Ta umožňuje přehled a přidávání nebo odebírání root práv, které instalované aplikace požadují.

Následující obrázek ukazuje chybové oznámení antivirového systému při pokusu o nastavení firewallových opatření na mobilním telefonu.

Obrázek č. 12 Zamítnutí firewallu

Zdroj: zpracováno dle *vlastní zdroj*

Co je root mobilního telefonu a je vůbec přínosný?

V případě rootovaného telefonu je možné s výše uvedeným antivirovým systémem firewall nastavit. To samé platí i pro další specifické firewall aplikace dostupné na Google Play, jako jsou například Droid Wall nebo Android Firewall. Avšak pokud dojde k rootu mobilního telefonu, není už možné na daný telefon uplatnit reklamaci.

4.2.4 Šifrování

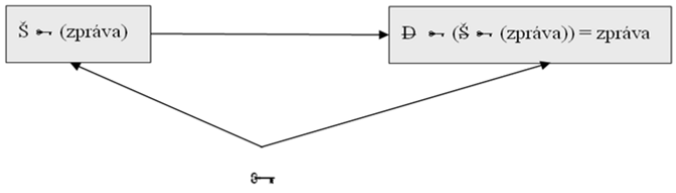
Šifrovací, jinak také šifrový nebo kryptografický, systém je systém používaný ke změně otevřeného textu na text nesrozumitelný pro kohokoliv jiného kromě příjemce. Otevřený text je původní text zprávy před zašifrováním. „*Pokud nějaký šifrový systém použijeme na zpracování nějaké zprávy, tak říkáme, že zprávu šifrujeme, nebo že jsme ji zašifrovali. Osoba, která šifrování provádí, se nazývá šifrant nebo šifrér.*“[25]

Vhledem k rozdílu mezi pojmy šifra a kód je nutné poznamenat následující. „*Pomocí šifry nebo přesněji šifrovacího systému se odesílatel a adresát snaží utajit obsah zprávy před nepovolanou osobou. Smyslem kódu není zprávu utajit, ale upravit ji tak, aby ji bylo možné dále příslušným technickým prostředkem zpracovávat, např. přenést nějakým kanálem. Kódovaná zpráva může být na základě znalosti příslušného kódování převedena zpět do původního tvaru.*“[26]

V otevřených sítích, kde nejsou přenosové kanály bezpečné, je rozumné přenášené údaje zabezpečit. Například pomocí kryptografie. Ta se používá mimo jiné k ověření identifikace a autentizace, autorizace, zachování integrity dat, auditingu, zajištění důvěrnosti dat, neodmítnutelnosti autorství a zachování dostupnosti.

Šifrování je dvojího typu. Symetrické šifrování se zakládá na jednom tajném šifrovacím klíči. Ten si musí oba účastníci před začátkem vzájemné komunikace vyměnit a nesmějí ho sdílet s nikým dalším. Poté odesílatel před odesláním zprávu zašifruje tajným klíčem a příjemce přijatou zprávu dešifruje stejným tajným klíčem.

Obrázek č. 13 Symetrické šifrování



Zdroj: zpracováno dle DOSTÁLEK, L. a kol., Velký průvodce infrastrukturou PKI a technologií elektronického podpisu

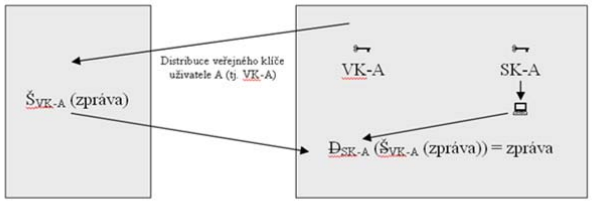
---

[25] VONDRUŠKA, P., *Kryptografie, šifrování a tajná písma*, s. 11

[26] VONDRUŠKA, P., *Kryptografie, šifrování a tajná písma*, s. 15

Při asymetrickém šifrování se používá dvojice klíčů, kterou tvoří veřejný a soukromý klíč. Asymetricky je možné šifrovat dvěma způsoby, a to s odlišným použitím páru klíčů.

Obrázek č. 14 Asymetrické šifrování



VK-A: veřejný klíč uživatele A
SK-A: soukromý klíč uživatele A
ŠVK-A: šifrování veřejným klíček uživatele A
DSK-A dešifrování soukromým klíčem uživatele A

Zdroj: zpracováno dle DOSTÁLEK, L. a kol., Velký průvodce infrastrukturou PKI a technologií elektronického podpisu

První varianta je šifrování veřejným klíčem a dešifrování soukromým klíčem. V tomto případě musí příjemce nejdříve vygenerovat soukromý klíč, který si uschová, a veřejný klíč, který může nezabezpečeně zaslat komukoliv, s kým chce komunikovat. Odesílatel tedy zprávu zašifruje veřejným klíčem příjemce a pouze příjemce může zprávu dešifrovat svým soukromým klíčem.

Použitím druhé varianty se data zašifrují privátním klíčem odesílatele a dešifrují veřejným klíčem odesílatele. Obdobně jako v první variantě odesílatel generuje dva klíče. Zašifruje zprávu svým soukromým klíčem, s tím rozdílem, že dešifrovat zprávu může kdokoliv, kdo vlastní veřejný klíč odesílatele.

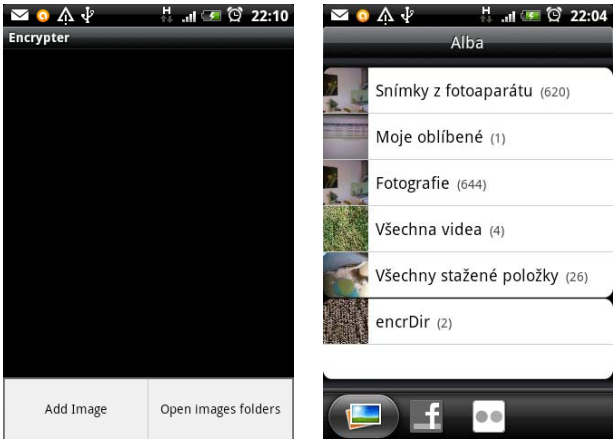
Dále v souvislosti s šifrováním existuje funkce hash. Jedná se o jednocestnou funkci, která z jakkoli dlouhého textu vytvoří krátký řetězec, otisk. Tento otisk může být spočten pomocí starších a slabších algoritmů, jako je MD-5 s velikostí výstupu 16 bytů, nebo SHA-1 s velikostí výstupu 20 bytů. Také lze použít jakýkoliv z novějších algoritmů, například SHA-256 nebo SHA-2. Tyto algoritmy jsou mnohem silnější a rozsáhlejší, a proto vypočtou otisk o větší velikosti výstupu než MD-5 nebo SHA-1.

Řešení

Na Google Play marketu jsou k dispozici různé šifrovací aplikace nabízející šifrování SMS zpráv, e-mailů nebo obrázků. Zde vybraná aplikace Encrypter - image crypt je velmi jednoduchá a intuitivní. Po jejím nainstalování vyskočí okno pro zadání přístupního hesla a po jeho nastavení je možné aplikaci začít využívat. Do nabídky aplikace se uživatel dostane přes stisknutí androidovského tlačítka menu, kde následně vybere *add image* z galerie obrázků. Po vybrání obrázek zašifruje pomocí příkazu encrypt. Dále je možné nastavení úrovně 1 – 3 pro šifrování obrázku, kde nejvyšší je úroveň tři a ta je také nejsložitější na dešifrování případnými útočníky. Aplikace defaultně používá šifrování první úrovně.

Po prvním zašifrování obrázku se automaticky vytvoří v galerii složka encrDir, jak je zobrazeno na obrázku níže.

Obrázek č. 15 Aplikace Encrypter a její úložiště



Zdroj: zpracováno dle *vlastní zdroj*

V této složce jsou uloženy všechny zašifrované obrázky. Pokud uživatel chce obrázky dešifrovat, musí tak učinit opět přes aplikaci Encrypter. Pres *add image* vybere úložiště encrDir a konkrétní obrázek, dlouze podrží prst na zvoleném obrázku a po naskočení okna s nabídkou vybere *decrypt*. Poté je požádán o zadání hesla, které po prvotním spuštění nastavil. Pokud je heslo zadané správně, obrázek se dešifruje na původní formu a je opět takto uložen do složky encrDir. Na obrázcích níže jsou vidět původní nezašifrovaná fotografie a zašifrovaná fotografie.

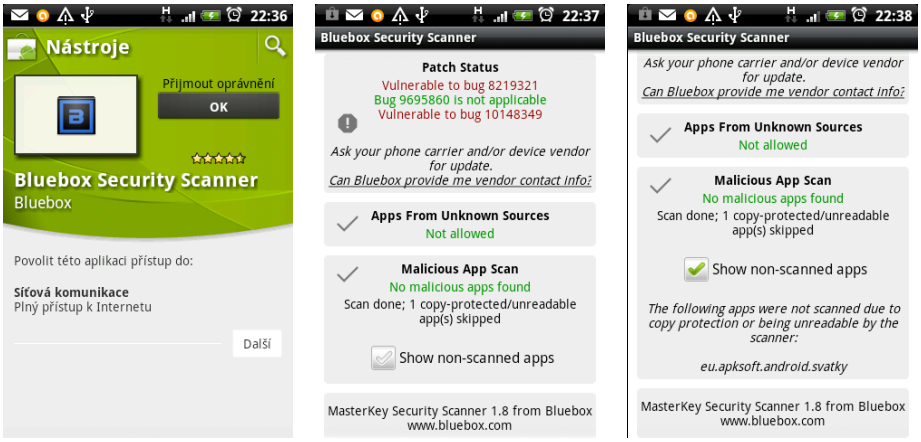
Obrázek č. 16 Nezašifrovaná a zašifrovaná verze fotografie

Zdroj: zpracováno dle *vlastní zdroj*

4.2.5 Bezpečností díry v Androidu

Případné chyby ve zdrojovém kódu umožňuje odhalit například aplikace Bluebox Security Scanner. Po jejím nainstalování a zavedení na mobilním telefonu se automaticky spustí kontrola.

Obrázek č. 17 Výsledky kontroly zdrojového kódu



Zdroj: zpracováno dle *vlastní zdroj*

Řešení

Dle výsledků kontroly aplikace Bluebox Security Scanner nejsou na mobilním telefonu žádné aplikace nainstalované z neznámých zdrojů nebo škodlivý software. Scanner vynechal kontrolu jedné aplikace, která je chráněna proti kopii nebo je nečitelná.

V tomto případě se jedná o *aplikaci eu.apksoft.android.svatky*. Nyní je vhodné překontrolovat tuto aplikaci pomocí již nainstalovaného antivirového systému, který dokáže zobrazit souhrnné informace o tom:

- jaké systémové zdroje tato aplikace využívá
- jaké jsou datové přenosy v souvislosti s aplikací, a to zpětně až jeden rok
- jaká jsou potenciálně nebezpečná oprávnění, kterými aplikace disponuje

Antivirový systém neodhalil žádné potenciální nebezpečí, dostupné informace o datových přenosech aplikace zobrazily 0.0 MiB, tedy aplikace neodesílá žádné podezřelé množství dat do nebo z telefonu. Ani antivirový test neodhalil, že by tento software byl škodlivého rázu.

Pomocí internetového vyhledávače a čísel uvedených po kontrole telefonu by mělo být možné nalézt výše uvedené chyby a následně zjistit, zda byla chyba opravena a jaká je případná náprava.

Chyba č. 8219321 a 10148349

Dle vývojářů aplikace Bluebox Security Scanner umožňují obě tyto chyby ve zdrojovém kódu přidání škodlivého kódu do APK souboru, a to v čase mezi ověřováním podpisu a samotnou instalací aplikace.

Pro zajištění a ověření původu, a tím i bezpečnosti aplikací, musí být prověřena jejich identita. To je obecně zajištěno pomocí vystaveného certifikátu certifikační autoritou, kterým jsou aplikace podepsány a následně distribuovány na Google Play marketu. Při instalaci aplikace dochází k prověřování identity, ale chybou ve zdrojovém kódu je, že jsou během instalace vkládány dva názvy aplikace. U jednoho názvu je systémem kontrolován kryptografický podpis a druhý slouží k provedení samotné instalace aplikace. Po instalaci aplikace je současně na mobilním telefonu nainstalován škodlivý software, díky němuž útočník získává plný přístup k systému, k veškerým datům uživatele a nakonec plnou kontrolu nad daným mobilním telefonem.

Chyba č. 9695860 (ZIP vulnerability)

Tato chyba není v tomto případě relevantní.

Společnost Google oficiálně nepotvrdila výše uvedené chyby ve zdrojovém kódu dané verze operačního systému, na které poukázali vývojáři aplikace Bluebox Security Scanner. Než bude případná oficiální záplata k dispozici, je vhodné vyhýbat se stahování a instalování aplikací z nevěrohodných nebo podezřelých zdrojů. V každém

případě je všeobecně doporučeno stahovat a instalovat aplikace pouze přes oficiální market Google Play, kde jsou všechny aplikace počátečně i průběžně kontrolovány.

4.2.6 Aplikace htcloggers

Aplikace HTCLoggers.apk je předinstalována na vybraných mobilních telefonech HTC se systémem Android a slouží jako kontrolér přihlášení. Aplikace umožňuje sběr informací, jako jsou data o poloze, vytáčená čísla, systémové výpisy nebo SMS zprávy. Tato data jsou následně umístěna do jediného souboru a jakákoliv další uživatelem naistalována aplikace na postiženém přístroji, která požádá o přístup k internetu, může všechny tyto údaje získat a odeslat. O přístup k internetu běžně žádá každá aplikace, která se do internetové sítě připojuje, ale také každá další aplikace, která zobrazuje reklamy.

Kromě přístupu k osobním údajům uživatele je možné získat informace o systému, používané síti včetně IP adresy nebo činnosti procesoru. Je také umožněno sledovat běžící procesy, paměť, stav baterie včetně informace o nabíjení, a mnoho dalších systémových informací.

Řešení

Dle oficiálního prohlášení vydala společnost HTC záplatu ve formě over-the-air aktualizace s doporučením jejího okamžitého stažení.

4.2.7 Fyzické zabezpečení

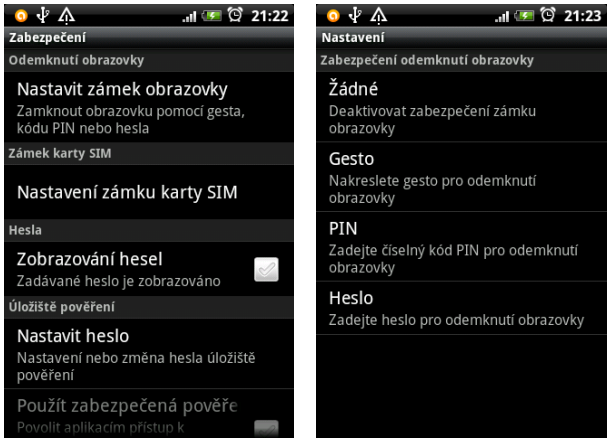
Pokud je telefon snadno fyzicky přístupný, může do něj útočník během krátké chvíle nainstalovat software pro odposlech či nahrávku nebo i „jen“ ukrást soukromá data. V případě ztráty nebo odcizení mobilního telefonu je u fyzicky přístupného telefonu jeho obsah snadno k dispozici. Pokud by obyčejné zadání PINu, nebo gesta, pro odemčení obrazovky mohlo zabránit ukradení soukromých fotografií, SMS zpráv, nebo v horším případě zneužití dat z navázaných webových aplikací na mobilním telefonu, pak je to to nejjednodušší, co může uživatel udělat. Zloděj má u nezabezpečeného mobilního telefonu příliš snadný přístup k datům, do e-mailu a k bankovnímu nebo jinému finančnímu účtu uživatele.

Řešení

Uživatel by neměl nikdy na veřejnosti nechávat svůj telefon bez dozoru, i kdyby to měla být jen pouhá minuta. Mělo by být nastaveno heslo nebo gesto pro odemknutí

displeje. To je možné provést v základním nastavení telefonu pod záložkou *Zabezpečení / Nastavit zámek obrazovky*, kde je následně nabídnuta možnost uzamčení telefonu pomocí gesta, PINu nebo hesla.

Obrázek č. 18 Nastavení zámku displeje



Zdroj: zpracováno dle *vlastní zdroj*

V souvislosti s odposlechem je doporučeno neotevírat MMS zprávy od neznámých odesílatelů a rovnou je vymazat. Pokud má uživatel podezření, že je jeho telefon odposloucháván, měl by jej resetovat do továrního nastavení. To, že je přístroj nějakým způsobem odposloucháván, se pozná mimo jiné také na měsíčním vyúčtování. Odchozí zprávy, ale i telefonní hovory, jsou většinou účtování dvakrát, to když útočníkovy chodí zprávy v kopii, či notifikace o telefonním hovoru, případně zapojení útočníka do „konference“ probíhaného hovoru. Dalším náznakem odposlouchávání je nestandardní zvuk při uskutečňování hovoru, nebo dokonce šum a cvakání v průběhu hovoru.

4.2.8 Ztracený nebo ukradený mobilní telefon

Pokud dojde ke ztrátě nebo zcizení mobilního telefonu, existuje velké riziko zneužití dat v daném přístroji. Pro vzdálenou správu a ovládání mobilního telefonu přes počítač, a to nejen v případě ztráty nebo zcizení, ale také pro v případě zapomenutí mobilního telefonu doma nebo v zaměstnání, slouží Aplikace HTCSense, která je dostupná na oficiálních webových stránkách HTC. S touto aplikací je možné přesměrování hovorů nebo SMS na jiný mobilní telefon nebo telefon nechat vyzvánět, telefon tehdy vyzvání i v případě ztlumeného zvuku. Dále je možné pomocí aplikace mobilní telefon přibližně lokalizovat na mapě nebo telefon uzamknout a nastavit zprávu ve formě krátkého vzkazu

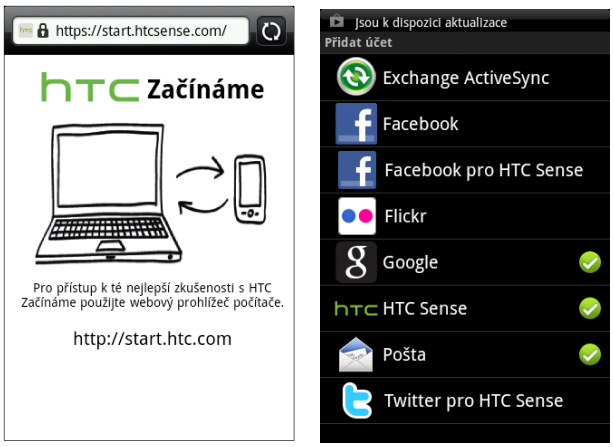
a telefonního čísla, na které je možné v případě nálezu zavolat. Pokud nálezce na telefonu poklepe na zobrazené telefonní číslo ve vzkazu, je umožněno z daného přístroje na toto číslo zavolat. V nejhorším případě je k dispozici funkce kompletního vymazání paměti telefonu včetně paměťové karty. Tato funkce je nevratná a smazaná data není možné následně obnovit.

Řešení

Nejprve je nutné povolit funkci hledání telefonu. To se provede přes *Nastavení / Umístění / Hledání telefonu*. Poté se vytvoří registrace účtu na https://www.htcsense.com, nebo přes daný mobilní telefon. Při registraci je požadováno zadání e-mailové adresy, mobilního čísla a odsouhlasení podmínek použití. Po vytvoření je potřeba v účtu ještě nastavit konkrétní model mobilního telefonu a služby, jaké uživatel bude využívat.

Pokud dojde k registraci přes mobilní telefon HTC Wildfire S, je ve fázi výběru modelu telefonu zobrazena následující obrazovka.

Obrázek č. 19 Registrace a přidaný účet HTCSense



Zdroj: zpracováno dle *vlastní zdroj*

V tuto chvíli není možné dokončení registrace mobilního telefonu jinak, než přes webový prohlížeč počítače. Tam dochází k zádrhelu, protože v internetové aplikaci není model telefonu HTC Wildfire S v nabídce podporovaných přístrojů. Mobilní telefon byl s funkcí HTCSense distribuován, proto byl v této souvislosti vznesen dotaz na výrobce a opravdu bylo následně potvrzeno, že mobilní telefon HTC Wildfire S nelze v aplikaci HTCSense vybrat a tím jej k účtu přiřadit.

Nezbývá než vyhledat podobnou aplikaci, která bude na daném mobilním telefonu dostupná. Na Google Play marketu je k dispozici ke stažení zdarma například aplikace Lookout Mobile Security, která má dobré uživatelské reference. Aplikace umožňuje vysledování pozice, vyzvánění na mobilním telefonu nebo také pořízení a zaslání fotografie, včetně lokalizace, na předem zvolenou e-mailovou adresu. Dále je možné pomocí této aplikace provádět jak antivirovou kontrolu mobilního telefonu, tak zálohu kontaktů z telefonu do počítače.

4.2.9 Nedostatečně vyspělé technologie

Další hrozbou, která je v povědomí lidí málo rozšířená, je používání nedostatečně vyspělých technologií.

Jednou z možných hrozeb v této oblasti je používání starých SIM karet, které využívají šifrování DES. Toto šifrování se považuje za velmi nespolehlivé, používá klíč jen o délce 64 bitů. Dnes je dokonce možné šifru DES prolomit nejdéle do 24 hodin.

Také zabezpečení sítí operátorů poskytujících mobilní služby je velmi důležité. Mezi velmi jednoduše zabezpečené sítě patří síť GSM, v níž lze pomocí cenově a snadno dostupného hardware zachytit komunikaci a speciálním software dešifrovat. Může zde docházet k odposlouchávání uživatelů, sledování jejich polohy či krádeže identity.

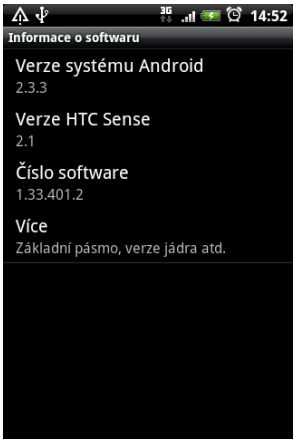
Řešení

Na straně operátů by měla být prioritou snaha o zvýšené zabezpečení jejich sítí. V roli uživatele je řešením mít vždy aktualizovaný software a používat nejnovější možné a dostupné technologie. Proto se doporučuje zajištění, případně zakoupení, novější SIM karty u poskytovatele.

V souvislosti s aktualizacemi software je níže uvedený postup jak zjistit, zda jsou k dispozici aktualizace a jak si je na mobilní telefon nainstalovat.

Na mobilním telefonu se provede zjištění aktuální verze operačního systému přes *Nastavení / Info o telefonu / Informace o softwaru*.

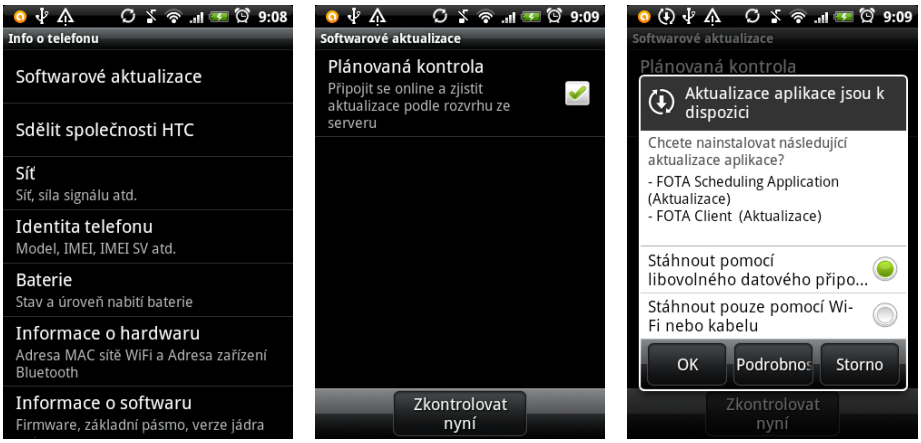
Obrázek č. 20 Zobrazení informací o software



Zdroj: zpracováno dle *vlastní zdroj*

Nyní je možné zjistit, zda jsou pro danou verzi dostupné aktualizace, a to připojením telefonu do internetové sítě přes *Nastavení/ Bezdrátová připojení / Mobilní síť* a následně v *Nastavení / Info o telefonu / Softwarové aktualizace / Zkontrolovat nyní*. Poté vyskočí obrazovka s vypsanou nabídkou dostupných aktualizací.

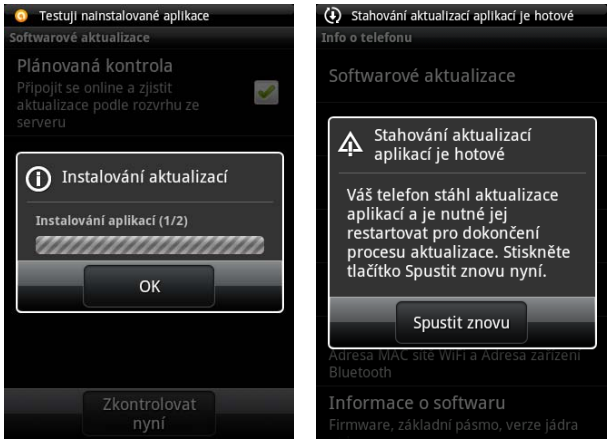
Obrázek č. 21 Softwarové aktualizace



Zdroj: zpracováno dle *vlastní zdroj*

Poté je možnost výběru ze dvou variant stažení aktualizace, popřípadě instalaci aktualizace odmítnout. Po stažení aktualizací je nutné mobilní telefon restartovat, až poté bude možné aktualizace nainstalovat.

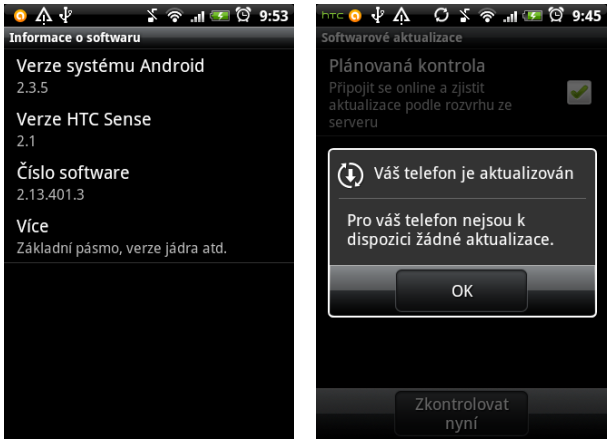
Obrázek č. 22 Průběh aktualizací



Zdroj: zpracováno dle *vlastní zdroj*

V tuto chvíli se verze systému Android změnila z 2.3.3 na 2.5.5 a číslo software z 1.33.401.2 na verzi 2.13.401.3 a po provedení kontroly softwarové aktualizace již nejsou žádné další k dispozici.

Obrázek č. 23 Výsledky aktualizací



Zdroj: zpracováno dle *vlastní zdroj*

4.2.10 Finanční služby

Bankovní instituce v České republice již běžně nabízejí mezi svými službami také mobilní finanční služby, respektive mobilní bankovnictví. Služba poskytuje vzdálenou správu bankovního účtu prostřednictvím aplikace té dané bankovní instituce. Pomocí mobilního telefonu si uživatel může ověřit zůstatek na účtu, zadat nebo zrušit jednorázové

a trvalé příkazy k platbě, případně povolit nebo zrušit inkaso. Aplikace bank jsou dobře zabezpečené, z tohoto hlediska se není prakticky čeho obávat.

Další poměrně mladou finanční službou je Google Wallet. Jedná se o aplikaci nainstalovanou do mobilního telefonu, pomocí níž lze zaplatit účet na podporovaných terminálech obchodníků. Aplikace funguje jako platební a věrnostní karta a současně dokáže zobrazovat okolní obchodní nabídky. Finance lze v aplikaci Google Wallet spravovat dvěma způsoby. Prvním je uložení bezpečnostních údajů z karty přímo do aplikace. Ale tím je samozřejmě povolen neomezený přístup k příslušnému bankovnímu účtu. Druhou možností je uložení určité částky, respektive kreditu, na účet aplikace a s jeho disponibilním zůstatkem platby hradit.

Řešení

Mobilní bankovnictví je velmi dobře zabezpečené, ale i tak je při užívání všech finančních aplikací nutná obezřetnost. Na prvním místě by mělo být výborné fyzické zabezpečení mobilního telefonu a hned poté nainstalování kvalitního antivirového systému.

Mobilní telefony využívající aplikaci Google Wallet by měly mít zabudovaný NFC čip. Mezi dostupné NFC telefony na českém trhu patří například Nokia Lumia 925, Blackberry Q5, Sony Xperia Z1 Compact, Samsung GALAXY S4 Mini nebo HTC ONE (M7). Poslední tři mobilní telefony využívají operační systém Android. HTC Wildfire S nemá NFC čip zabudovaný, takže službu Google Wallet nepodporuje.

4.2.11 QR kódy

Jak QR kódy fungují a proč jsou nebezpečné?

QR kódy jsou založeny na principu rychlého stažení dat do mobilního telefonu, ať už se jedná o kontaktní údaje, odkaz na webové stránky nebo rovnou údaje k platbě přes bankovní převod. Data se do mobilního telefonu stáhnou pomocí načtení QR kódu speciální čtečkou. Čtečka QR kódu není běžně v mobilním telefonu nainstalovaná, takže pokud uživatel chce QR kód načíst, je potřeba nejdříve čtečku do mobilního telefonu nainstalovat. QR kódy ale mohou obsahovat kromě praktických informací také škodlivý software, který je nevědomě uživatelem do mobilního telefonu nainstalován. Mezi těmito škodlivými programy může být malware, viry a další software podobného typu.

Obrázek č. 24 QR kód

Zdroj: zpracováno dle *http://smobil.cz/cz/qr-kody/popis/*

Řešení

U QR kódu je možnost kontroly, zda škodlivý software obsahují, velmi obtížná. Proto je lepší do mobilního telefonu tyto kódy nenačítat. V případě načítání QR kódů je nutností mít nainstalovaný kvalitní antivirový systém.

4.3 Útoky na uživatele

Bezpečnost uživatele je mnohem důležitější, než předcházení rizika zneužití citlivých dat. Proto je tato kapitola věnována takovým útokům, které jsou vedeny se záměrem poškodit konkrétní osobu.

Dle informačního portálu Policie České republiky se kyber útoky člení do následujících kategorií:

- Kyberšikana
- Kyberstalking a stalking
- Sexting
- Kybergrooming

Níže jsou jednotlivé kategorie blíže popsány, uvedeny důsledky souvisejících útoků a nasledně stanovena doporučení na možná řešení konkrétní dané problematiky. Dále jsou v této kapitole rozepsána aktuální témata z oblasti bezpečnosti sociálních sítí, sledování komunikace na internetu, hrozby software pro rozpoznávání tváře či snímání otisků a podvodné telefonáty či SMS s cílem obohacení se na úkor uživatele.

4.3.1 Kyberšikana

V tomto případě útočník využívá informačních technologií k různým druhům činnosti zaměřené na konkrétní osobu s cílem jejího poškození, znemožnění, ublížení nebo zastrašování. Rozhodně to není kompletní výčet, který lze do oblasti kyberšikany zahrnout.

Útoky kyberšikany jsou prováděny pomocí internetu, mobilních telefonů, e-mailu, sociálních sítí, chatu a dalších komunikačních kanálů.

V oblasti telefonické kyberšikany se jedná zejména o vydírání přes mobilní telefon, obtěžování, sledování a neustálé prozvánění mobilního telefonu oběti nebo zasílání urážlivých, nemravných nebo zastrašujících SMS zpráv.

Oběť si někdy není ani vědoma, že se již jedná o kyberšikanu. Útočníci mají většinou stejný profil jako u klasické šikany, nebo se jimi naopak stanou dřívější oběti kyberšikany. Kyberútoky nelze z hlediska načasování a místa předem odhadnout, o to více jsou nepříjemné a oběť se nemá možnost před nimi nikam schovat. Útočníci kyberšikany mohou vystupovat, a mnohdy i v komunikaci vystupují, anonymně a oběť je v takovém případě vystavena pocitu neřešitelnosti daného problému. Je přesvědčena, že útočníka nelze nijak identifikovat a najít. Útočníci kyberšikany se na základě anonymity stávají mnohem agresivnějšími, než by v reálném světě byli. Z pocitu neodhalitelnosti zkoušejí a používají stále horší nátlak na oběť, a pokud má kyberútočník k dispozici publikum, účinek útoku má na oběť o to větší dopady.

Je velmi složité šikanování na oběti odhalit, a to právě proto, že zde dochází k psychické újmě, ne fyzické. Oběť velmi často trpí v tichosti, a pokud není kyberšikana včas odhalena, může se stát, že oběť situaci nezvládne a tato situace může dospět k tak smutnému činu jako je sebevražda.

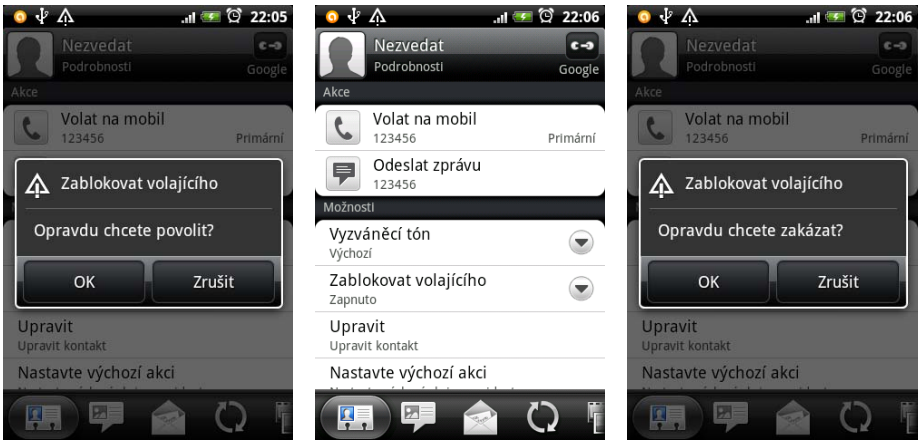
Řešení

V České republice jsou zřízeny asistenční linky pro oběti internetové kriminality a dále anonymní formuláře, přes které je možné po vložení e-mailového kontaktu zaslat krátký popis dané situace. Výše uvedených kontaktních míst lze využít také v případě, že jde pouze o podezření, že je nějaká osoba šikanována pomocí prostředků informačních technologií. Jak telefonní číslo na asistenční linku, tak kontaktní formulář lze najít na internetových stránkách Policie České republiky.

Na mobilním telefonu HTC Wildfire S je nastavení blokace telefonního čísla jednoduché. Po otevření uloženého kontaktu ve složce *Lidé* je v možnostech kontaktu volba *Zablokovat volajícího*. Po potvrzení blokace jsou všechny hovory z tohoto čísla blokovány a u položky *Zablokovat volajícího* je uvedeno *Zapnuto*, jak je uvedeno na obrázku níže. U blokovaného telefonního čísla je možné zpětně tuto blokaci odebrat. Pokud je blokace čísla nastavena, útočníkovi se ozve vyzváněcí tón a následně obsazovací

tón. Avšak telefon, který má blokaci nastavenou, vůbec nevyzvání. Zmeškané hovory od blokovaných čísel jsou ukládány do příslušné hlasové schránky.

Obrázek č. 25 Blokace volajícího

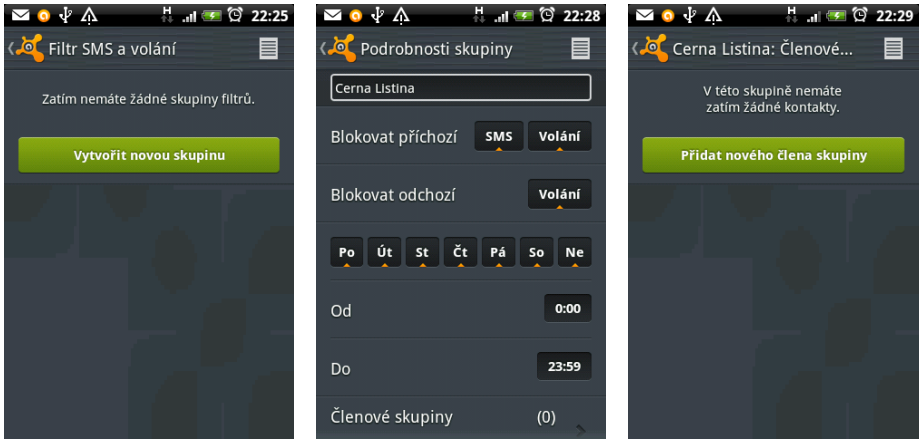


Zdroj: zpracováno dle *vlastní zdroj*

Toto základní nastavení je velmi užitečné, ale nastavitelné jen pro konkrétní telefonní číslo. Pokud se útočník pokusí kontaktovat oběť přes jiné telefonní číslo, toto nastavení nebude funkční a útočník tak může dál pokračovat s šikanováním oběti.

Chce-li uživatel nastavit blokaci také pro textové zprávy, je tu možnost použití antivirového systému. Přes funkci *Filtr SMS a volání* může uživatel přidat novou skupinu přes *Vytvořit novou skupinu*. V následně otevřeném okně může skupinu pojmenovat a nastavit co je požadováno, aby bylo po danou skupinu blokováno a v které dny a čas. Do skupiny přidají vybranná telefonní čísla pomocí funkcí *Členové skupiny* a *Přidat nového člena skupiny*.

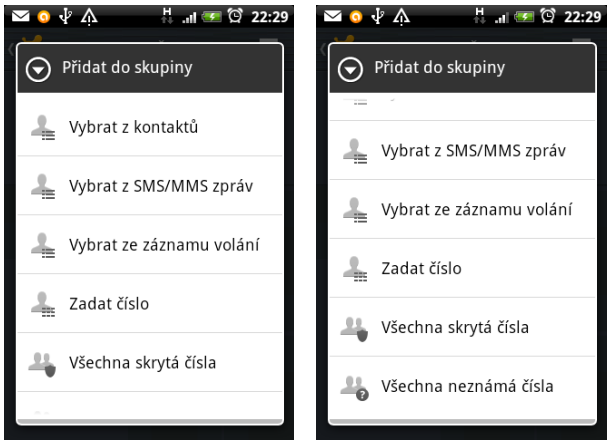
Obrázek č. 26 Nastavení filtru SMS a volání



Zdroj: zpracováno dle *vlastní zdroj*

Antivirový systém umožňuje blokaci jak čísel konkrétních, tak všech skrytých nebo neznámých, jak je vidět na obrázcích níže.

Obrázek č. 27 Možnosti filtrování a blokace skupin



Zdroj: zpracováno dle *vlastní zdroj*

Co se týká nastavení blokace MMS zpráv, je nutné do mobilního telefonu nainstalovat speciální aplikaci. Přes market Google Play je k dispozici mnoho blokačního software. Jedněmi z těch lépe hodnocených aplikací jsou BlackList a aFirewall call and sms blocker, které umí blokovat příchozí hovory, SMS a MMS pro vybraná telefonní čísla, neznámá nebo private čísla. Lze také vytvořit povolené skupiny a na takto nastavený mobilní telefon se dovolají a dopíší pouze vybrané kontakty.

Velkou nevýhodou je, že uživatel musí při instalaci blokačního software povolit práva zobrazená na následujícím obrázku. První obrázek náleží aplikaci BlackList a druhý obrázek ukazuje nutná práva pro chod aplikace aFirewall call and sms blocker.

Obrázek č. 28 Práva blokačního software

Zdroj: zpracováno dle *vlastní zdroj*

V tomto případě je doporučena obezřetnost a instalaci takového software s potenciálně nebezpečným oprávněním pečlivě promyslet.

Přeje-li si uživatel ještě více zvýšit soukromí mobilního telefonu, lze provést nastavení zamezení identifikace telefonního čísla. Nejprve je nutné aktivovat službu u daného operátora a ve druhém kroku nastavit službu v mobilním telefonu přes *Menu / Nastavení / Volat / Další nastavení / ID volajícího*, kde je možná volba mezi *Výchozím nastavením sítě*, *Skrytým číslem* nebo *Zobrazením čísla*.

4.3.2 Kyberstalking

V tomto případě dochází k obtěžování oběti nevyžádanými SMS nebo telefonními hovory. Kyberstalker stupňuje obsah zpráv a formu svého jednání v závislosti na stádiu kyberstalkingu. Nejprve jsou zprávy nebo hovory pozitivní a milé, s postupem času začínají být nepříjemné, otravující, vydírající a vyhrožující. Jako ukázku své síly útočník používá prostředků, jako jsou fyzické sledování, ničení majetku nebo usmrcení domácích mazlíčků oběti. Dále využívá telekomunikačních prostředků k prokázání znalosti oběti například ve formě zpráv o tom, že danou oběť vidí, ví co má na sobě nebo co právě dělá.

V dalších případech se útočník snaží snížit důvěryhodnost oběti jejím pomlouváním v jejím okolí, případně šířením nepravdivých informací o oběti.

Řešení

Od roku 2010 se změnou trestního zákona stal v České republice stalking trestnou činností. Bránit se stalkingu lze především blokováním telefonních hovorů a veškerých zpráv od útočníka. Dále zde platí ignorovat útočníka a v případě nouze či ohrožení kontaktovat tísňové linky nebo policii.

4.3.3 Sexting

Jedná se o zasílání pornografického materiálu prostřednictvím internetu nebo přes mobilní telefony. Účastníci sextingu jsou si známi, většinou se jedná o přítele a přítelkyni, zpravidla v mladistvém věku. Zasílají si nahé fotografie, fotografie citlivých míst nebo videa se sexuálním podtextem. K problému dochází v okamžiku rozchodu, kdy se jeden z partnerů začne mstít a tyto citlivé materiály zveřejní, ať už ve formě přeposlání na jiný mobilní telefon nebo prostřednictvím sociálních sítí či serverů pro sdílení videí.

Útočníci nemusí spadat do skupiny přítel a přítelkyně, ale mohou to být kamarádi, popřípadě spolužáci, kteří se k pornografickému materiálu dostali přemluvením oběti nebo krádeží takového materiálu.

Řešení

Už jen samotné posílání a sdílení pornografického materiálu je nelegální činností, což si ale mnoho účastníků sextingu vůbec neuvědomuje. V České republice jsou takové případy řešeny individuální nebo občansko-právní cestou.

Předejít sextingu a následnému trestnímu stíhání lze jedině dostatečnou informovaností.

4.3.4 Kybergrooming

Kybergrooming je útok za účelem manipulace oběti a následného přemluvení k osobní schůzce. Pokud osobní schůzka proběhne, dochází k sexuálnímu zneužití nebo mučení oběti. Útočníkem je často pedofil a obětí dítě nebo mladistvá osoba.

Útočník se nejprve snaží dostat do přízně oběti, naslouchá jejím problémům a snaží se dostat do role osoby, která oběti rozumí. Snaží se oběť izolovat od jejího okolí manipulací a cíleným našeptáváním oběť proti svému okolí postavit. Vždy se ale pokouší

udržet celý vztah v naprostém utajení. Pomocí obdarovávání a vybudování psychické závislosti oběti na útočníkovi se útočník snaží přemluvit oběť k osobní schůzce, kde poté následuje sexuální zneužití nebo fyzické týrání oběti.

Řešení

Při řešení problematiky kybergroomingu je velmi důležitý výborný vztah rodičů s dětmi a velmi dobrá informovanost potencionálních obětí.

4.3.5 Sociální sítě

Lidé se dobrovolně registrují do sociálních sítí, většinou pod vlastním jménem a poskytují internetu ve větší či menší míře své osobní údaje. Sociální sítě pak nejsou nic jiného než obrovskou databází lidí se jmény, adresami, vzájemnými vztahy a komunikací, vše doplněno aktuální fotodokumentací. Pokud se navíc uživatelé na svůj účet připojují přes mobilní telefon, riziko zneužití soukromých dat se tím jen zvyšuje.

Kromě získání osobních informací z databází sociálních sítí se tu také naskýtají hrozby spojené s akceptací falešných přátel. Útočníci si za účelem získání dat určité osoby (oběti), vytvoří na sociální síti falešný účet. Následně zkouší být akceptováni alespoň jednou osobou z okruhu oběti, což jim umožní přístup k informacím buď přímo oběti nebo jejích přátelů. Pokud najdou přítele oběti, který ještě nemá na sociální síti účet, tak si tento falešný účet vytvoří, s nímž je následně velmi jednoduché být obětí na seznam přátel akceptován.

Ztráta dat, případně nechtěné změny na účtu oběti, souvisejí s ukradeným nebo zneužitým přístupovým heslem. Nevhodné statusy psané útočníkem, znemožnění oběti před ostatními přáteli nebo uveřejnění urážlivých fotografií může u osob se sníženou či nestabilní psychikou vést k závažným problémům.

Řešení

Už jen tím, že uživatel dobrovolně poskytuje své osobní informace jako je jméno, datum narození, informace o zaměstnání, e-mail a mobilní telefon do relativně přístupné sítě, se vystavuje riziku zneužití těchto dat. Na sociální síti ale navíc zveřejňuje veškeré vazby a známosti, nebo svou vztahovou situaci. I toto je velké odhalení soukromí a pro mnoho lidí mají tato data potenciální užitek a jsou prostředkem zneužití. A nakonec fotografie veškerého druhu, počínaje detailními fotografiemi domova včetně jeho vybavení, svých dětí a domácích mazlíčků, automobilů nebo závodních kol konče, jsou

přesným obrazem toho, co uživatel vlastní, kde je to umístěno, kdy a jakým způsobem je to používáno.

Nejbezpečenějším řešením by bylo sociální sítě vůbec nevyužívat, ale to je v dnešní době, zejména mezi mladistvými, nemyslitelné. Nezbývá než postavit útočníkovi do cesty překážky ve formě kvalitního mobilního antivirového programu a dále neakceptovat mezi své přátele cizí osoby. Pokud jsou akceptovány osoby, které jsou známy, je lepší jejich opravdovou identitu prověřit i jinou cestou, například osobním kontaktem. Dále je doporučeno minimalizovat vkládání soukromých informací a fotografií na sociální sítě.

4.3.6 Sledování internetové komunikace

Nedávno uveřejněné informace v tisku poukazují na existenci utajené operace tajných složek, kde dochází ke sledování internetové komunikace a přímému sběru informací. Osobní data jsou vedena o uživatelích na celém světě v databázích vybraných gigantických společností a tajné složky mají údajně neoficiální přístup do těchto databází přes zadní vrátka. Zadní vrátka v systému znamená vložení specifik do systému, které po zadání určitých vstupních dat umožňují projít skrze bezpečností mechanismy systému. Mohou se tak snadno získat soukromé informace o jakékoliv osobě v jakýkoliv čas a bez nutnosti předložení soudního příkazu.

Řešení

Proti takovému sběru osobních dat se nelze nijak chránit. Pokud uživatel ve svém mobilním telefonu používá připojení k internetu, jeho data jsou patrně nějakým způsobem vedena a uchovávána. Jak snadno přístupná tato data opravdu jsou, to lze jen těžko odhadnout.

4.3.7 Rozpoznávání tváře a snímače otisku prstu

Moderní technologie přináší mnoho dobrého, ale mnohdy také něco velmi nebezpečného. Alespoň co se ochrany osobních údajů a osobnosti týče.

Novodobé technologie přišly například s detektory a rozpoznávači tváře. Ano, je to velmi praktická pomůcka pro policii, která díky takovému softwaru dokáže vyhledat a sledovat pomocí propojeného městského bezpečnostního kamerového systému konkrétní osobu. Ale už také na sociálních sítích je možné během přidávání nových fotografií jen potvrdit automaticky nabídnuté označení osob na vkládané fotografii. To je provedeno pomocí detekčního rozpoznávacího software a porovnávání dat v dané databázi. Ovšem na

druhou stranu, uživatel nemusí být na fotografii vůbec označen, ale i tak je ho možné v dané databázi nalézt.

Dalším diskutovaným tématem jsou nepochybně také snímače otisku prstů. Dnes je lze najít na moderních počítačích nebo přenosných zařízeních, včetně mobilních telefonů. Otázkou zůstává, jsou-li tato data v bezpečí jak před výrobcem, tak před případnými útočníky.

4.3.8 Podvodné telefonáty

Podvodné telefonáty jsou velkým nebezpečím a to především proto, že se dají jen velmi špatně odhalit. Scénář je většinou následující. Na mobilní telefon zavolá operátor neznámé společnosti, zabývající se výzkumem veřejného mínění. Rozhovor je natáčen. Operátor požádá volaného, zda je ochoten zodpovědět následujících pár otázek. Tyto otázky jsou sestaveny tak, aby rozhovor mohl být následně změněn, resp. zfalšován, ku prospěchu volajícího. Volaný, pokud na zodpovězení otázek přistoupí, může být tímto způsobem zneužit například tím, že se „zaváže k úvěru“, k „dlouhodobému odběru určitého zboží nebo materiálu“ nebo v lepším případě jen „potvrdí objednávku“. A to právě proto, že byl daný rozhovor nahráván a následně pozměněn. Odpovědi volaného zůstaly stejné, ale otázky operátora se změnily.

Řešení

Pokud uživatel obdrží hovor od kohokoliv ze společnosti, kterou nezná, a hovor neočekává, je doporučeno rozhovor ihned ukončit a na žádné otázky neodpovídat.

4.3.9 Dobíjecí SMS

V posledních několika měsících se v České republice rozšířila nekalá finta v podobě dobíjecích SMS, příběh je vždy dost podobný. Uživatel obdrží SMS s nějakým kódem. Následuje další SMS s prosbou o zaslání či potvrzení dobíjecího, přihlašovacího či jiného kódu, který byl na daný přístroj „omylem“ zaslán. Někdy naopak útočník napřímo zavolá s velmi zkroušeným a nešťastným hlasem, jindy zavolá dokonce dítě. Ve chvíli, kdy úživatel kód potvrdí nebo přepošle, bude mu na jeho měsíční účet připsána různě vysoká finanční částka. U operátora je bohužel většina reklamací tohoto typu neuplatnitelná.

Dalším chytákem podobného rázu je nalákání k zaslání kreditu výměnou za nahou fotografii. Tento následně zaslaný kód opět neslouží k ničemu jinému, než k vymámení peněz z oběti.

Řešení

Uživatel by neměl odesílat a ani potvrzovat žádné kódy obdržené prostřednictvím SMS z neznámých telefonních čísel. Dále by též neměl odpovídat na inzeráty typu „*ty mi zašleš .. a já ti pošlu kredit..*“.

4.4 Špionážní software

Pomocí špionážního software se útočník může dostat k různým informacím a datům. Špionážní software je buď nainstalován přímo do mobilního telefonu, nebo je pomocí speciálního hardware a software daný telefon odposloucháván na dálku.

První varianta je poměrně snadno dostupná, protože na trhu již existuje mnoho špionážních aplikací. O to hůře je ale realizovatelná. Daný software, jako je například aplikace SpyAndroid LITE, je potřeba nainstalovat na sledovaný přístroj, což se provádí jen velmi težko, snad jen s výjimkou telefonů členů rodiny. Špionážní software se používá pro kontrolu dětí, nastavení různých omezení při procházení webových stránek, ale také pro vyhledání polohy, kde se zrovna dítě nachází. V horším případě je software instalován do mobilních telefonů partnerů nebo manželů, a to za účelem potvrzení nevěry nebo kontroly partnera. Kromě výpisu hovorů, jejich délky, SMS zpráv, monitorování chatu nebo pohybu na sociálních sítích, je možné kontrolovat také výpis adresáře nebo sledovat fotogalerii. Některé špionažní aplikace umožňují navíc odposlech okolí telefonu, odposlech hovoru živě nebo dokonce pořízení fotografie vzdáleným příkazem.

Další variantou je odposlech na dálku pomocí počítače s anténami, přijímačem a software, který dokáže vyhledat mobilní telefony v určitém dosahu. Radiový signál je zachytáván, nahráván a dekódován a poté je příslušný mobilní telefon odposloucháván. Podle typu zařízení a software je možné odposlouchávat i více než jeden přístroj. Na druhou stranu je tato technologie závislá na pohybu odposlouchávaného telefonu a proto také náročná z hlediska technického provedení.

Pochopitelně jakákoliv forma odposlechu je nelegálním zásahem do soukromí odposlouchané osoby.

Řešení

Bránit se proti nainstalování špionážního software lze fyzickým zabezpečením přístupu do mobilního telefonu. Pokud uživatel mobilní telefon někomu půjčuje, měl by zvážit případnou kontrolu, co na telefonu dotyčný provádí. Má-li uživatel podezření, že je

již špionážní software na telefonu nainstalovaný, je doporučeno uvést daný přístroj do továrního nastavení.

V případě odposlechu na dálku existují různé technické prostředky a technologie na ochranu místnosti nebo přístrojů, počínaje generátory bílého šumu a konče různými rušičkami radiového signálu. Co se softwarového zabezpečení mobilního telefonu týče, řešením je instalace šifrovacího software, který zašifruje jak probíhající telefonní hovor, tak textové zprávy nebo přenos souborů. Data jsou chráněna přímo v mobilním telefonu, pak na cestě mezi telefonem a BTS stanicí, ale také před monitorováním komunikace na ústředně operátora. Data nelze dešifrovat v reálném čase hovoru, ale ani zpětnou analýzou. Na českém trhnu dostupný šifrovací software je například SILENTEL, který je se systémem Android a mobilními telefony HTC plně kompatibilní.

5. SHRNUTÍ A ZÁVĚR

5.1 Shrnutí

V této práci byl analyzován mobilní telefon HTC Wildfire S A510e s operačním systémem Android verze 2.3.3 Gingerbread.

První kapitola se zaměřila na řešení bezpečnost dat. Nejprve bylo zjištěno, že na mobilním telefonu není nainstalovaný žádný antivirový systém, který by ho chránil před útoky z internetu a případnými viry. Byl proto nainstalován antivirový systém. Po kontrole virového testu nebyl odhalen žádný škodlivý software. Následně byla na mobilním telefonu nainstalovaná aplikace, která umožňuje šifrování fotografií přímo v mobilním telefonu. Zpětně dešifrovat fotografie bylo poté možné jen s použitím znalosti hesla, které bylo původně při instalaci aplikace zadáno. Dále bylo zjištěno, že mobilní telefon nesplňuje požadavek na aktualizovaný software. K dispozici byl firmware over-the-air, který byl stáhnut a nainstalován. Také došlo k aktualizaci systému na verzi 2.3.5. Dále byl mobilní telefon testován na chyby ve zdrojovém kódu. Byla provedena kontrola aplikací, tedy zda jsou nějaké aplikace nainstalovány z neznámých zdrojů nebo je-li nainstalován jakýkoliv škodlivý software. Kontrola neodhalila žádné nebezpečné aplikace, ovšem byla vynechána kontrola jedné, která byla chráněna proti kopii nebo byla nečitelná. Tato aplikace byla následně prověřena antivirovým systémem, který neodhalil žádné potenciální nebezpečí. Dále byly aplikací pro kontrolu zdrojového kódu odhaleny dvě chyby. Vzhledem k tomu, že se společnost Google k těmto chybám ještě oficiálně nevyjádřila a nevydala k dispozici žádnou opravu, bylo v tomto případě pouze uvedeno doporučení ohledně stahování a instalování aplikací pouze přes oficiální market Google Play. Dále bylo zjištěno, že je mobilní telefon snadno fyzicky přístupný, proto na něm bylo nastaveno gesto pro odemknutí displeje. Pro případ ztráty, nebo zcizení, mobilního telefonu, měl být nastaven účet a registrován daný mobilní telefon v aplikaci HTCSense, přes kterou je možné vzdáleně spravovat registrovaný přístroj. Bylo ovšem zjištěno a ověřeno přes oficiální zdroje, že analyzovaný mobilní telefon není s touto funkcí aplikace kompatibilní, přestože by teoreticky kompatibilní měl být. Dále bylo upozorněno na možné varianty zneužití peněžních prostředků v případě používání finančních aplikací, jako je mobilní bankovnictví nebo platby přes terminál z mobilního telefonu. Na závěr byly zmíněny možné hrozby QR kódů.

V další kapitole byly uvedeny hrozby vázající se na uživatele. Detailněji byly popsány kyberútoky, konkrétně kyberšikana, kyberstalking a stalking, sexting a kybergrooming. V jejich souvislosti byla uvedena doporučení chování uživatele pro omezení vzniku útoků, případně jejich řešení. Bylo také vzpomenuto na potenciální nebezpečí spojená se sociálními sítěmi, softwarem pro rozpoznávání tváře nebo snímači otisku prstů. Na závěr kapitoly byly popsány aktuální postupy u podvodných telefonátů nebo dobíjecích SMS zpráv.

Poslední kapitola praktické části byla věnována technikám odposlechu a metodám, jak se takovému odposlechu bránit.

Celkové náklady na řešení v této práci byly nulové, veškerý testovaný a použitý software byl k dispozici bezplatně ke stažení.

5.2 Závěr

V teoretické části práce byly popsány principy fungování mobilních telefonů, internetové a mobilní komunikace, ale také úvod do problematiky ochrany dat a příslušné legislativy. V praktické části byla pak analyzována související bezpečnostní rizika. Na základě zjištěných poznatků bylo uvedeno doporučení pro minimalizaci těchto rizik a/nebo navrhnuto konkrétní zabezpečení včetně volby, zavedení a nastavení vhodného bezpečnostního software, doplněné grafickým návodem.

Vytyčený cíl práce splnila. Může se stát nejen návodem, ale také upozorněním na nebezpečí, která s používáním mobilních telefonů úzce souvisí. Mnohé hrozby si uživatelé mobilních telefonů vůbec neuvědomují, a je proto důležité, aby o nich byli dostatečně a průběžně informováni.

Trendem současnosti je shromažďování čím dál více funkcí a různorodých dat do mobilního telefonu, ať už se jedná o fotoaparát, přenosnou mobilní kancelář nebo různé aplikace pro elektronickou komunikaci či každodenní zábavu. Dnes již spolu lidé sedící pouze pár metrů od sebe komunikují především pomocí internetu a telekomunikačních technologií a osobní kontakt je pomalu na ústupu. Pokud bude v budoucnu probíhat většina komunikace v elektronické formě, prioritním cílem musí být zaručení její bezpečnosti a soukromí.

6. SEZNAM POUŽITÝCH ZDROJŮ

6.1 Soupis bibliografických citací

Literatura

PROCHÁZKA, David. *Mobilní telefony: příručka pro stávající i budoucí majitele mobilu.* 1. vydání. Olomouc: Rubico, 2000. 104 s. ISBN 80-85839-57-1.

REISCHL, Gerald. *Sběratelé elektronických dat pod lupou.* 1. vydání. Praha: Euromedia Group; Knižní klub, 2001. 254 s. ISBN 80-242-0514-9.

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma.* 1. vydání. Praha: Albatros nakladatelství, a.s., 2006. 400 s. ISBN: 80-00-01888-8.

Počítačové programy

Systém ASPI [počítačový program]. *Verze 2013 pro Microsoft Windows. Praha: Wolters Kluwer ČR, a. s.* Systém pro práci s právními informacemi. [cit. 2014-01-18].

Elektronické zdroje

ACCESS SERVER. Mobilní sítě. In: *Access.feld.cvut.cz* [online]. 28. srpna 2004 [cit. 2013-12-15].
Dostupné z WWW: <http://access.feld.cvut.cz/view.php?cisloclanku=2004072801>

NÁRODNÍ CENTRUM KYBERNETICKÉ BEZPEČNOSTI ČR. Legislativa. In: *Národní centrum kybernetické bezpečnosti ČR* [online]. 2. ledna 2014 [cit. 2014-01-29].
Dostupné z WWW: <http://www.govcert.cz/cs/legislativa/legislativa/>

O_2. Parametry HTC Wildfire S. In: *Telefónica Czech Republic, a.s.* [online]. [2014]. [cit. 2014-01-23].
Dostupné z WWW: <http://www.o2.cz/osobni/techzona-mobilni-telefony/htc-wildfire-s.html?tab=techinfo>

PETERKA, Jiří. Báječný svět počítačových sítí. Část XXVII: Pevná telefonní síť a její využití pro přenos dat. In: *eArchiv.cz* [online]. 2011 [cit. 2013-11-30].
Dostupné z WWW: <http://www.earchiv.cz/b07/b0700001.php3>

PETERKA, Jiří. Kam směřují mobilní sítě? In: *eArchiv.cz* [online]. © 2011 [cit. 2013-12-26].
Dostupné z WWW: <http://www.earchiv.cz/b07/b0200003.php3>

SERVIS-SONYERICSSON. Pohled do historie. In: *Servis mobilních telefonů Sony Ericsson, Sony, iPhone, Samsung, Nokia, LG, ZTE a Huawei* [online]. © 2009–2014 [cit. 2013-11-30].
Dostupné z WWW: <http://www.servis-sonyericsson.cz/zajimavosti.html>

6.2 Seznam zdrojů obrázků

Literatura

DOSTÁLEK, Libor, VOHNOUTOVÁ, Marta, KNOTEK, Miroslav. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2. aktualizované vydání. Brno: Computer Press, a.s., 2009. 542 s. ISBN 978-80-251-2619-6.

PROCHÁZKA, David. *Mobilní telefony: příručka pro stávající i budoucí majitele mobilu.* 1. vydání. Olomouc: Rubico, 2000. 104 s. ISBN 80-85839-57-1.

Elektronické zdroje

MEYERS, Justin. From Backpack Transceiver to Smartphone: A Visual History of the Mobile Phone. In: *WonderHowTo* [online]. 2012. [cit. 2013-11-25].
Dostupné z WWW: <http://smartphones.wonderhowto.com/inspiration/from-backpack-transceiver-smartphone-visual-history-mobile-phone-0127134/>

MOLNÁR, Jiří. Úvod do sítě 3. generace. In: *Umts.wz.cz* [online]. [cit. 2013-12-10].
Dostupné z WWW: <http://www.umts.wz.cz/Mob_radio_site_3G/uvod_do_site_3G.htm>

PETERKA, Jiří. Kam směřují mobilní sítě? In: *eArchiv.cz* [online]. © 2011 [cit. 2013-12-26].
Dostupné z WWW: <http://www.earchiv.cz/b07/b0200003.php3>

SMOBIL. O QR kódech. In: *Seznam.cz na mobil*. [online]. © 1996–2014. [cit. 2014-02-25].
Dostupné z WWW: <http://smobil.cz/cz/qr-kody/popis/>

WIKIPEDIA. File: DynaTAC8000X.jpg. In: *Wikipedia, the free encyclopedia* [online]. 2008. [cit. 2013-11-30].
Dostupné z WWW: <http://en.wikipedia.org/wiki/ File:DynaTAC8000X.jpg>

WIKIPEDIE. Soubor: Mobile phone evolution.jpg. In: *Wikipedie, Otevřená encyklopedie* [online]. 3. 12. 2006. [cit. 2013-11-30].
Dostupné z WWW: <http://cs.wikipedia.org/wiki/ Soubor:Mobile_phone_evolution.jpg>

WIKIPEDIE. Soubor: Vlnova delka.png. In: *Wikipedie, Otevřená encyklopedie* [online]. 24. 6. 2005. [cit. 2013-12-03].
Dostupné z WWW: <http://cs.wikipedia.org/wiki/Soubor:Vlnova_delka.png>