ANALYSIS OF SIM CARDS FOR GSM PHONES

Juraj ONDRUŠ, Master Degree Programme (4)
Dept. of Information Systems, FIT, BUT
E-mail: xondru06@stud.fit.vutbr.cz

Supervised by: Dr. Daniel Cvrček

ABSTRACT

The paper analyses properties of SIM cards and the communication between SIM cards, GSM cell phones and GSM networks (network providers). The analysis should give an idea about the processes taking place when e.g. a mobile is turned on, or when one reads an SMS message.

1 ÚVOD

SIM karty jsou součástí GSM systému od jeho prvního návrhu. Při definici standardů GSM se pamatovalo na to, aby telefony bylo možné vyrábět masově a aby bylo snadné jim přiřadit telefonní číslo. Médiem, které nese informace o telefonním čísle, je SIM karta. První karty, s označením GSM fáze jedna, nebyly vybaveny některými funkcemi, které jsou pro dnešní karty zcela běžné, neuměly například ukládat SMS zprávy. Ty sice byly standardem podporovány, ale bylo je možné uložit jen do paměti samotného telefonu nebo jen dočasně zobrazit na jeho displeji.

Vzhledem ke stále se zlepšujícím parametrům moderních čipových karet se stala reálnou možnost vložit informace několika SIM karet do jedné fyzické čipové karty a některé mobilní telefony dokonce práci s takovými SIM kartami podporují. Naprosto opačnou motivací je vytvoření kopií SIM karty např. pro telefony vestavěné do aut.

2 CO JE SIM KARTA

Karta SIM (***S**ubscriber **I**dentification **M**odul*) je procesorová karta. Obsahuje tedy vlastní mikroprocesor, který je ovládán řídícím programem. Tím může být specializovaný program, virtuální stroj (např. Java virtual machine), nebo plnohodnotný operační systém.. Tento mikroprocesor pak zpřístupňuje přes datové rozhraní karty právě ty informace ze své paměti, které telefon v danou chvíli vyžaduje pro svou činnost. Telefon je tedy vždy tou aktivní stranou, zatímco karta funguje jako periferie.

Všechny karty, ať už čipové, magnetické nebo jen plastové, jsou normalizovány. Normám podléhají rozměry, mechanické vlastnosti, magnetické vlastnosti u magnetických karet i množina příkazů, kterým karty rozumějí. Hlavní normou je ISO 7816, která má šest

částí, z nichž však jen tři jsou pro GSM karty důležité. Prvá definuje rozměry a mechanické vlastnosti, druhá karty s elektronickými čipy, jejich umístění a rozměry, třetí pak elektrické signály a komunikační protokoly.

Karta se skládá z mikroprocesoru (typicky 8-bitového, nebo 16-bitového, ale může už být i 32-bitový) a pamětí (EEPROM, ROM, RAM), příp. specializovaného koprocesoru (např. pro kryptografické operace). Jedná se o mikroprocesor bez periferií. Se svým okolím komunikuje sériově přes jeden datový vodič. Mikroprocesor potřebuje napájení Vcc, zdroj signálu RESET, kterým se uvádí do výchozího stavu, zdroj hodinového signálu – vstup CLK, už zmíněný datový vstup DATA pro přenos informací z/do karty, a zem GND. Historicky je definován ještě vstup programovacího napětí Vpp. Ten však již na moderních SIM kartách nebývá připojen. Celkem tak dostáváme 5 vodičů rozhraní, kterým karta komunikuje se světem.

V paměti najdeme v prvé řadě operační systém, který je uložen v ROM paměti (její velikost bývá od 8 do 256KB). Odsud je řízen mikroprocesor. V ROM paměti jsou také uloženy informace o výrobci, systému souborů, někdy i kryptografické algoritmy a pod. Kromě toho najdeme v paměti (tentokrát EEPROM – může mít až ke 100 kB, nejnovější dokonce několik MB) prostor k uložení dat o účastníkovi, např.: SMS zprávy, telefonní seznam fixní a časté volby, číslo IMSI (***I**nternational **M**obile **S**ubscriber **I**dentification*), kterým se účastník k síti přihlašuje, bezpečnostní klíč Kc, pomocí něhož je šifrován hovor na cestě mezi telefonem a BTS (základnovou stanicí).

3 KOMUNIKAČNÍ PROTOKOLY

Komunikační protokoly definují způsob komunikace, strukturu přenášených dat a příkazů. Protokol T1 dodržuje zásady komunikace *data-link* (anebo *link-level*) popsaných v *OSI* (Open system Interconnect), protokol T0 je jednodušší. Komunikace probíhá na podnět telefonu, telefon zadá požadavek, případně zašle potřebná data, karta přijme požadavek zkontroluje správnost dat, vykoná požadované operace a výsledek pošle zpátky. Nad protokoly T0 a T1 je definován aplikační protokol pomocí tzv. APDU (*application protocol data units*). Základní sada APDU je definována již v původním standardu ISO 7816-4, ale každá aplikace přirozeně definuje další specifické příkazy.

Po připojení napájecího napětí (zapnutí telefonu) mezi vývody Vcc a GND karta očekává událost RESET. Jelikož telefon neví, jestli je RESET definován fyzickým signálem 0 V, nebo 5 V, tak nejprve nastaví RESET do stavu 0, které podrží po dobu 40 000 hodinových cyklů (vstup CLK) a očekává reakci karty. Když karta neodpoví, udělá totéž ještě ve stavu 1. Karta na událost RESET reaguje vysláním tzv. ATR sekvence (***A**nswer **T**o **R**eset*). Je to sled bytů obsahujících komunikační parametry a informace o výrobci/typu. Neohlásí-li se karta, telefon ji odmítne. Jestliže karta reaguje, je nadále na vývodu RESET ustálena ta hodnota, při které nastala událost ATR. Data přitom karta vysílá asynchronně. Data jsou přenášena sériově, po START-bitu je přeneseno osm datových bitů, následovaných sudou paritou a následuje STOP-bit. Základní rychlost komunikace na datovém rozhraní je 9600 bitů za vteřinu pro karty s vnitřním zdrojem hodin, nebo CLK/372 u karet, které vyžadují externí zdroj hodin. Pro korektní chování je tedy třeba, aby frekvence na CLK byla mezi 3,5-4 MHz.

4 PŘÍSTUP K SOUBORŮM

Karta všechny informace ukládá do speciálních souborů, které jsou rozděleny do adresářů. Většina těchto souborů je chráněna určitou úrovní zabezpečení (0-15), tyto úrovně jsou v kartě předem naprogramovány a tudíž se nedají měnit, lze do nich pouze vstupovat. Běžný uživatel má přístup pouze k prvním třem úrovním.

Každý účastník má přiděleno unikátní číslo IMSI (**I**nternational **M**obile **S**ubsciber **I**dentification), které je uloženo na SIM kartě a sestaveno tak, že je ve všech GSM sítích na světě zajištěna jeho jedinečnost. *IMSI* se používá v okamžiku, kdy mobilní telefon žádá o přihlášení do GSM sítě, tedy vždy po zapnutí telefonu. Aby si GSM síť dokázala prověřit, že dané *IMSI*, které v okamžiku přihlášení od mobilního telefonu obdržela, skutečně přísluší té správné SIM kartě, je na ní uloženo ještě jedno číslo, které je ovšem tajné a nedá se ze SIM karty přečíst. Toto číslo, kterému se říká *Ki* (identifikační klíč) se spolu s náhodným číslem, které síť do karty pošle, zpracuje *autentizačním algoritmem* (A3, COMP128,…). Výsledek, kterému se říká *SRES* (**S**igned **Res**ponse), mobilní telefon pošle zpět síti a ta porovná, zda je shodný s tím, který si pro kontrolu spočítala sama. Na základě porovnání těchto dvou výsledků je pak karta přijata nebo odmítnuta.

5 KLONOVÁNÍ SIM KARET

Klonovaní SIM karty je jednoduše řečeno, vytvoření karty se stejnou identitou, jakou má originál. Z výše uvedeného plyne, že k tomu potřebujeme dvě věci: *IMSI* a *Ki*. *IMSI* je v kartě chráněno kódem PIN1 a po jeho zadání nám nic nebrání toto číslo přečíst. U *Ki* je situace složitější. Operační systém SIM karty, nám tento klíč nesdělí. Je ovšem možné zlomit algoritmus *COMP128* a klíč vypočítat. V dalším kroku je třeba IMSI a Ki přenést do nějakého zařízení, které se jako SIM karta bude chovat, v ideálním případě do nějaké prázdné SIM karty, která tak získá identitu originálu. Funkci karty celkem dobře může zastoupit počítač PC, nebo i jiný, vybavený softwarem pro simulaci SIM karty. Vytvoření kostry SIM karty v mikrokontroléru integrovaném v čipové kartě pak s sebou přináší zajímavý efekt. V programu karty je možné pamatovat na možnost změny IMSI a Ki a získat tak více karet v jedné. Jednotlivé identity lze pak jednoduše vázat např. na zadaný PIN, jehož volbou pak je možné mezi uloženými účty přepínat.

6 ZÁVĚR

Po úvodní analýze komunikace SIM karet s telefony a otestování získaných poznatků na skutečných SIM kartách se budeme dále věnovat vytvoření aplikace, která umožní vytvoření klonu SIM karet na programovatelných kartách (např. Java karty).

LITERATURA

[1] http://mobil.idnes.cz/mob_tech.asp?r=mob_tech&c=A011010_0042218_mob_tech

[2] http://mobil.idnes.cz/mob_tech.asp?r=mob_tech&c=A011012_0042288_mob_tech

[3] http://www.jecny.cz/