Chyba karty SIM – náhoda, či úmysl?

Časovaná bomba

Čtenáře jistě příliš nepřekvapí novinová zpráva o novém počítačovém viru, který se ve formě elektronické pošty nebo jinak šíří internetem a zanechává za sebou jen spoušť v podobě zničených datových souborů, uklepaných magnetických hlav pevných disků, zničených budičů sběrnic, které byly destruktivním exekučním kódem viru nejprve nastaveny jako výstupní, a to proti sobě, aby je pak jimi protékající zvýšený proud zničil.

Říká se, že takové viry jsou výsledkem činnosti frustrovaných jedinců, kteří si tak léčí svoji bolístku způsobenou vyhazovem ze zaměstnání či jiným ústrkem okolní společnosti, která je dozajista ztělesněním dobra samého, a proto je chování autorů virů nanejvýš zavrženíhodné. Jde však o chování stejně tak zavrženíhodné, implementuje-li vir do svého produktu nějaká společnost, jejíž produkty nakupují zákazníci, a ještě za to zaplatí? Že to není možné? A že by techniku vhodně zkonstruovaného viru nemohla použít i nějaká velká společnost? Ptáte se proč? No třeba proto, že si tím v budoucnosti zajistí další příjem od svých zákazníků, kteří již používají její produkt. A nic na celé věci nezmění ani fakt, že se nejedná o počítačový vir v klasickém smyslu toho slova, ale o specifickou “chybu” v SIM kartě jednoho z našich provozovatelů sítě GSM, která způsobí, že po jisté době dojde v kartě k zablokování její důležité části tak, že ji nelze dále používat ani k telefonování, ani ke komunikaci pomocí SMS zpráv, ani k přihlášení mobilního telefonu k síti GSM. To vše samozřejmě bez varování, bez ostychu, nekompromisně. A ptáte se, kdy a za jakých okolností se to stane? Podle této hypotézy k tomuto jevu dojde pravděpodobně u SIM karet Radiomobilu zakoupených v zimě 1998/1999 a novějších (testy jsme prováděli na několika kartách TWIST) po přibližně 90 000 hovorech příchozích či odchozích, odeslaných či přijatých SMS zprávách, přechodech z jedné provozní oblasti do druhé, zjištění kreditu ap. Je lhostejno, která z uvedených eventualit nastala jako poslední. Všechny se pěkně sčítají, a když je jich kolem 90 000, SIM karta vám zamává na rozloučenou. Není bez zajímavosti, že se tato SIM karta s “chybou” chová jako trojský kůň: totiž ještě rádi si ji do svého mobilního telefonu v dobré víře strčíme. Navíc bavíme-li se o mobilních telefonech, jak napovídá nadpis (a těm pozorným z vás jistě neušla aféra s autentifikačním algoritmem obsaženým v SIM kartách GSM telefonů v dubnu 1998), rázem se před námi otevírá prostor, ve kterém je možné takovýto přístup velmi elegantně využít. Provozovatel sítě by tak prostě vydal karty, které mají díky specifické “chybě” jen omezenou životnost. Zákazníci by pak časem tyto karty museli vyměnit. Byl by to jejich problém a velmi pravděpodobně by taková výměna nebyla zadarmo. Díky viru, své časované bombě, má provozovatel mobilní sítě jistotu, že časem prodá zákazníkům jiné karty, a řeší tím díru v zabezpečení sítě. A kdože to platí? No kdo jiný než zákazník! “Vždy o důvod víc, proč být s námi.” Ano vážení, velmi to tu zavání globalizací. A co víc, stavěním rovnítka mezi to, co režim reálného socialismu označoval jako lid, konzumní společnost spotřebitelskou veřejností a tupým stádem, které ve finále zaplatí řešení problémů provozovatele služeb GSM. Takže nebuďme tupí a dávejme si pozor! Ale popořádku.

Na samém začátku našeho krátkého povídání si dovoluji čtenáře odkázat na sérii článků v časopise Chip, jejichž autory jsou Vlastimil Klíma a Tomáš Rosa: Když se řekne SmartCard, Není všechno zlato..., GSM pod tlakem klonování, Karta a její klíč, Důvěrnost a šifra v GSM, Šifra v GSM prolomena. Zkratky a terminologie použité v tomto povídání jsou stejné jako v uvedených článcích.

Dne 13. dubna 1998 bylo Asociací vývojářů čipových karet oznámeno, že byl nalezen efektivní útok na autentifikační algoritmus GSM, algoritmus nazývaný A38, jenž je spojením dvou klíčových algoritmů zabezpečení celého systému GSM, algoritmu A3 generujícího autentifikační odezvu SRES a algoritmu A8, který generuje klíč pro šifrování hovoru Kc. Prováděcí kód byl přečten metodou zpětného inženýrství z čipu SIM karty a zveřejněn. Jedná se o COMP128. Oba algoritmy mají společné vstupy RAND, což je náhodné číslo, které dodá GSM síť na začátku procesu autentifikace mobilní stanice a Ki, což je identifikační klíč SIM karty, který je pro každou kartu unikátní, a víceméně společný výstup SRES´_Kc. Kc převezme mobilní telefon a je jedním ze vstupů do algoritmu A5 a SRES je odesláno do sítě GSM ke kontrole autenticity uživatele. Útok z dubna 1998 předpokládá vlastnictví modulu SIM a znalost jeho PIN1, popř. PUK1 k získání přístupu k autentifikační funkci na SIM kartě (je to funkce INS=0x88 s P1=0x00, P2=0x00, P3=0x10 s datovou částí RAND). Výsledek pak obdržíme aplikací instrukce getResponse (INS=0xC0 s P1=0x00, P2=0x00, P3=0x0C). Úvodní byte příkazů pro GSM SIM je vždy CLA=0xA0. Cílem útoku je (jak jinak) určit klíč Ki, který nelze běžným způsobem přečíst. Dělá se to tak, že se hledají tzv.

kolize, stejné výsledky SRES´_Kc pro různá čísla RAND. Přitom RAND se zadávají tak, že se zadává vždy "stejné" číslo, v němž se mění pouze 1 nebo 2 B, a to tak, že při hledání 0. a 8. byte klíče Ki měníme pouze 0. a 8. byte RAND a poznamenáváme si výsledky SRES´_Kc. Najdeme-li dva stejné výsledky, máme nyní dvě čísla RAND a k nim dohledáme při znalosti algoritmu COMP128 (viz zmíněné články) prostým vyzkoušením opět všech 65536 možností příslušné dva byte klíče Ki. A tak postupujeme s 1. a 9. až se 7. a 15. bytem. To, že kolize nastávají v míře tak hojné, je slabou stránkou algoritmu COMP128. Měl bych zde asi napsat, že Ki je dlouhý 128 b stejně jako RAND. Výsledek SRES´_Kc je dlouhý 96 b, ale při použití algoritmu COMP128 zůstává posledních 10 b nulových.

Podívejme se nyní blíže na komunikaci mezi kartou SIM a útočníkem, jenž se snaží zjistit klíč Ki. Vypadá to asi takto:

CLA, INS, P1,P2,P3	Data	SW1, SW2	Poznámka
A0 88 00 00 10	00 kk kk kk kk kk kk kk 00 kk kk kk kk kk kk kk	9F 0C	RAND
A0 C0 00 00 0C	dd dd dd dd dd dd dd dd dd dd dd dd 00	90 00	SRES´_Kc
A0 88 00 00 10	00 kk kk kk kk kk kk kk 01 kk kk kk kk kk kk kk	9F 0C	
A0 C0 00 00 0C	dd dd dd dd dd dd dd dd dd dd dd dd 00	90 00	
A0 88 00 00 10	00 kk kk kk kk kk kk kk 02 kk kk kk kk kk kk kk	9F 0C	
A0 C0 00 00 0C	dd dd dd dd dd dd dd dd dd dd dd dd 00	90 00	
	*** atd. ***		
A0 88 00 00 10	00 kk kk kk kk kk kk kk FF kk kk kk kk kk kk kk	9F 0C	
A0 C0 00 00 0C	dd dd dd dd dd dd dd dd dd dd dd dd 00	90 00	
A0 88 00 00 10	01 kk kk kk kk kk kk kk 00 kk kk kk kk kk kk kk	9F 0C	
	*** atd. až do nalezení kolize ***		

kk v tabulce označuje konstantní byte dd v tabulce označuje proměnný byte

V tomto duchu pak komunikace pokračuje, jak je popsáno výše. Lze říci, že takováto komunikace sama o sobě jasně naznačuje, že se s největší pravděpodobností jedná o útok. Číslo RAND se totiž mění jen v 1 nebo ve 2 B, zbytek čísla zůstává stejný. Tuto větu nechť laskavý čtenář nezapomene, neboť se k ní při popisu naší hypotézy ještě vrátím. Není pravděpodobné, že by GSM síť postupně zasílala mobilní stanici takovouto posloupnost čísel RAND. Teoreticky by ke kolizi a tím k určení 1/8 klíče Ki mělo dojít po 23 170 dotazech. Celý klíč by pak mělo být možno určit po 185 360 dotazech vyslaných do karty. Potud tedy krátká rekapitulace jednoho z nejproblematičtějších míst zabezpečení sítí GSM, které používají algoritmus A38 na bázi COMP128, a aféry, která přes jistou bagatelizaci ze strany sdružení operátorů, které tehdy prohlásilo, že se vlastně "nic moc nestalo", jistě mocně zacloumala situací kolem důvěryhodnosti GSM.

Před časem jsme s kolegy nahlíželi na problém kolizí v COMP128 a debatovali o tom, jak kartu zabezpečit před takovým jednoduchým útokem, který je výše popsán, a testovali dostupné moduly SIM karet, ponejvíce propadlé karty TWIST. Zjistili jsme, že některé vykazují neobvykle krátkou dobu života při "trápení" výše uvedeným způsobem. Nedalo nám to a "utrápili jsme k smrti" ještě nejednu novou SIM kartu, kterou jsme však již museli řádně zaplatit. Zde jsme došli k výsledku přibližně 90 000 volání funkce RunA38 (INS=0x88, P1=0x00, P2=0x00, P3=0x10). Poté karta při volání funkce RunA38 vrátí SW1=0x94, SW2=0x08 (dle normy ISO7816 "vybraný datový typ souboru neodpovídá příkazu", dle GSM11.11 doslova "- file ID not found, - pattern not found"), a při následném pokusu o přečtení výsledku getResponse (INS=0xC0, P1=0x00, P2=0x00, P3=0x0C) obdržíme chybovou hlášku SW1=0x6F, SW2=0x00, což podle ISO7816 i GSM11.11, která

předepisuje chování SIM karty GSM, značí “technical problem with no diagnostic given” – blíže nespecifikovaný technický problém. Nyní vznikla právem domněnka, že SIM karta pozná útok, který je proti ní veden, a oprávněně zhatí útočníkovi jeho nekalé plány. Proto byl připraven pokus se simulací, kde nebyla komunikace vedena výše uvedeným způsobem komunikace s větou, kterou jste si měli zapamatovat shora, kdy je z kontextu komunikace jasně vidět útok. Byla prováděna tak, jak se odehrává v běžném provozu, včetně občasného provedení RESET, jako když telefon po vypnutí znovu zapnete, se zápisy do souborů s klíčem Kc, který pak využívá algoritmus A5 k šifrování, LOCI pro update aktuální polohy mobilního telefonu, a karta opět nevydržela více. A potom byl uspořádán poslední pokus, kdy číslo RAND bylo voleno náhodně, a tedy se vlastně o žádný útok nejednalo. Tento pokus se nejvíce přibližoval skutečnému provozu, neboť čísla RAND zadávaná do karty měla statisticky náhodné rozložení (volání funkce Random() z Pascalu 7.0 firmy Borland) jako při autentizaci v síti. A karta to zase po cca 90 000 pokusech vzdala. A to vede k vyslovení hypotézy, že některé karty společnosti Radiomobil, a. s., jsou zatíženy touto “chybou”. Náš vzorek je statisticky malý, neboť jsme vyzkoušeli deset kusů. Ale chování bylo vždy stejné. Jen na kartě vydané stejnou společností ještě před aférou s COMP128 se uvedená vlastnost neprojevila. Karta pracovala spolehlivě i po 250 000 pokusech. Buďme optimisty a domnívejme se, že uvedená vlastnost je možná míněna v dobrém, aby z karty nebylo možno určit klíč Ki. Odpovídalo by tomu i omezení karty na 90 000 autentifikací, což je přibližně polovina z těch teoretických 185 360 autentifikací, kterých by bylo třeba k určení klíče Ki. Ale proč je toho dosahováno tímto způsobem? Zde se opět odvolávám na tu výše uvedenou větu, tento typ útoku lze snadno rozeznat a na platformě čipové karty implementovat. Takže je tu vůbec optimismus na místě? Je-li popsaná hypotéza platná, pak operátor jasně udělal ze svého problému problém svých zákazníků. Řekněte sami, koupili byste si auto, které se po 90 000 ujetých km zastaví a je ho třeba vyměnit s odůvodněním výrobce, že to je pro vaše dobro, abyste se nezabili ve starém voze? Radiomobil má dnes okolo 1 000 000 zákazníků. Kdyby 1/2 z nich měla takto “vylepšenou” kartu, přiteče časem při ceně vyměněné karty 400 Kč do pokladničky Radiomobilu, a. s., 200 000 000 Kč. A kdy by se tak mohlo stát? Při stovce autentifikací denně to vychází na 2,4 roku života karty. Každý nevolá jako o závod, tak se dá tušit, že nejdříve budou postiženi ti nejčastěji telefonující, tedy manažeři, a ti, kteří používají telefon zhusta a hodně se přitom pohybují. Zbylé úvahy jsou na laskavém čtenáři.

Tomáš Voliňský