Bezpečnost mobilních telefonů GSM

Šifra v GSM prolomena!

V seriálu o bezpečnosti mobilních telefonů GSM (Chip 6 až 9/98) jsme vás seznámili se základními bezpečnostními prvky, které se v GSM používají. Tehdy jsme se zaměřili zejména na klonování SIM karet a upozornili jsme též na možnosti operátora zaznamenávat čas, polohu i otevřené informace přenášené sítí GSM. K této tematice se nyní vracíme při zajímavé příležitosti — došlo totiž k útoku na algoritmus, který se v GSM stará o šifrování éterem přenášených dat.

K ochraně komunikace mezi mobilním telefonem a sítí GSM se používá tajná šifra. Pokud by tento rádiový přenos nebyl šifrován, kdokoliv s příslušným přijímačem by mohl odposlouchávat jakýkoliv mobilní telefon GSM — třeba i telefony ministrů, poslanců nebo představitelů významných společností; postačilo by jen postavit několik přijímačů k důležitým budovám nebo do centra hlavního města. Kdoví, možná tam už jsou — politická a průmyslová špionáž není nic nového. Dnes si však ukážeme, že luštit se dá i ***šifra A5***, kterou používají mobilní telefony asi 200 milionů uživatelů v Evropě i jinde.

Pro lepší přehlednost jsme nové informace rozdělili do dvou částí. V první se zaměříme zejména na klíčové myšlenky popisovaného útoku s hlavním důrazem na pochopení jeho základních principů, příště se soustředíme na podrobnější výklad některých úvah, které se při luštění algoritmu A5 používají.

Finální odhalení

První popis šifry A5, který jsme přinesli už v Chipu 9/98, se dostal na internet na základě podkladů získaných od dr. Shepherda. Britská telefonní společnost BTT mu omylem zapomněla dát podepsat smlouvu o mlčenlivosti, kterou musí podepsat všichni, kdo se se šifrou A5 seznámí — včetně výrobců mobilních telefonů, v jejichž firmwaru je implementována. Než britská tajná služba zasáhla a na Shepherdovu přednášku uvalila utajení, popis unikl na veřejnost. To bylo v roce 1994.

V květnu 1999 Marc Briceno, Ian Goldberg z ISAAC (univerzita v Berkeley) a David Wagner z SDA získali reverzním inženýrstvím přesný popis A5 (přesněji variant A5/1 a A5/2) a kód ověřili vzhledem k oficiálním testovacím hodnotám. Ukázalo se, že dřívější údaje o A5 byly v zásadě správné, jen došlo k upřesnění detailů.

Zkoumání plné verze A5 přivedlo v prosinci minulého roku dvojici luštitelů (Alexe Biryukova a Adiho Shamira) z Weizmannova institutu v Izraeli k objevu lušticí metody. Jejich útok, který si zde popíšeme, umožňuje **nalézt tajný šifrovací klíč k A5 za méně než sekundu pomocí obyčejného PC se 128 MB RAM a dvou 73GB pevných disků**, a to na základě analýzy známé dvouminutové komunikace. Útok byl ověřen na modelovém příkladě.

Šifra A5 a její varianty

Šifra A5, kterou si dnes popíšeme, je tzv. *silnou variantou*, označovanou jako *A5/1*. Vznikla před rokem 1989, byla určena pro západní Evropu a dnes ji používá asi 100 milionů lidí. Pro ostatní státy byla pak určena její zeslabená verze *A5/2*; tu údajně používá dalších cca 100 milionů telefonů GSM v Evropě i jinde.

Obr.1. Anténa běžné buňky GSM. Je to ale opravdu obyčejná buňka, nebo špionážní stanice?

Zatím není nikdo ochoten říci, která šifra se kde používá, a proto jedinou cestou zůstává zpětné inženýrství. Popis A5/2 se na veřejnost zatím nedostal. Dosud se soudilo, že jediným rozdílem oproti A5/1 je záměrné vynulování deseti z 64 bitů klíče Kc, ustaveného pomocí A8 k šifře A5. Jsou zde však určité náznaky, že změn k horšímu je více.

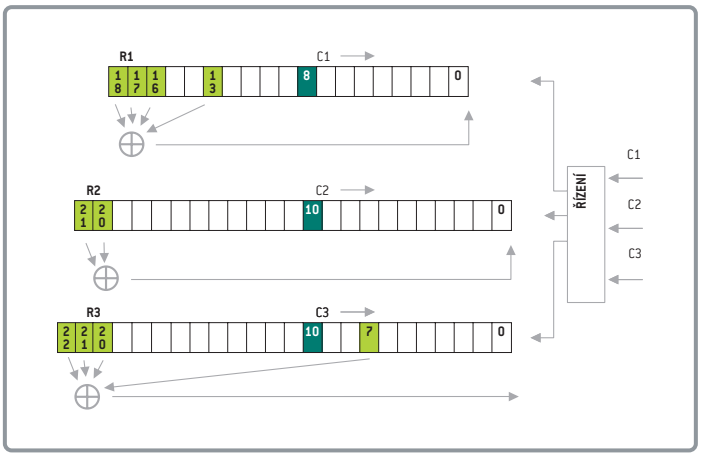
Zajímavé je, že skupina tvořená Bricenem, Goldbergem a Wagnerem uvádí, že **všechny** implementace A5, s nimiž se setkali, měly 10 bitů Kc vynulovaných! Další vzrušení do situace vnesl David Wagner, když v srpnu 1999 na konferenci Crypto'99 prohlásil, že luštění A5/2 vyžaduje řádově pouze 2^{16} operací! Podrobnosti tohoto útoku uvedené skupiny však nejsou známy, a proto nemůžeme posoudit jeho účinnost. Pro země, kde je A5/2 používána, by to však mohl být značný bezpečnostní problém.

Technický popis

(Pro stručnost a přehlednost dalšího výkladu si dovolíme předpokládat znalost základních mechanismů a termínů z oblasti ochrany přenosu GSM, které jsme uvedli v předchozích článcích na toto téma — viz zejména Chip 6/98, str. 148 až 150).

Základem zde prezentované metody je **útok se známým otevřeným textem** *(KPA — Known Plaintext Attack)*. Abychom byli schopni určit příslušný výstup algoritmu A5, musíme znát nějakou dvojici *otevřený text — šifrový text*. Výstup A5, tj. vygenerované heslo, potom získáme jako jejich vylučovací součet (exclusive or): heslo = otevřený text XOR šifrový text.

Dále popsaný útok předpokládá, že jsme pro dané nastavení A5 (tj. hodnotu Kc



Obr. 2. Ověřené schéma stále ještě utajované proudové šifry A5/1

a aktuální číslo rámce TDMA) schopni získat jeho výstup o maximální délce, tj. 228 bitů. Jak ale víme, tato hodnota se v GSM zařízení dělí na 114 b hesla pro *uplink* (kanál od telefonu do sítě) a 114 b hesla pro *downlink* (kanál ze sítě do telefonu). Náš útok tedy předpokládá znalost otevřené podoby přenášených dat jdoucích v určitém okamžiku oběma směry. Pro jednoduchost teď předpokládejme, že jsme schopni KPA v takovémto rozsahu provést, takže pro jedno číslo rámce TDMA zjistíme všech 228 b produkovaných algoritmem A5. Úvahám o případných modifikacích, které by tento požadavek zjemnily nebo odstranily, se budeme věnovat příště.

Popis A5/1

Základem A5/1 jsou tři lineární posuvné registry R1, R2 a R3 o délkách 19, 22 a 23 bitů se zpětnou vazbou (LSFR), jak je vidíte na obr. 2. Pokud označíme bit nejvíce vpravo indexem nula, má registr R1 zpětnovazební bity 18, 17, 16 a 13, pro R2 to jsou bity 21 a 20 a pro registr R3 bity 22, 21, 20 a 7. Prostřední bity registrů (u R1 je to bit 8, u R2 bit 10, u R3 bit 10) jsou určeny pro nelineární krokování a označíme je C1, C2 a C3. Jejich hodnoty určí, který z registrů bude stát a který se posune.

Krokování je velmi jednoduché. Nejprve se vypočte majoritní hodnota C takto: C se rovná nule, jsou-li alespoň dvě z hodnot C1, C2 a C3 nuly, jinak se rovná jedničce (je to zkrátka bit, který v této trojici převládá). Proto se C rovná vždy buď dvěma, nebo třem bitům z trojice (C1, C2, C3). Krokování je definováno tak, že příslušný registr Ri se posune, pokud se hodnota jeho řídicího bitu Ci rovná majoritní hodnotě C (v každém kroku se proto posunou buď právě dva, nebo právě tři registry). Pokud posun nastane, je ze stávajícího stavu vypočtena zpětná vazba Z (například u R2 je to hodnota $Z2 = R2_{21}$ XOR $R2_{20}$) a ta se plní zprava do registru. Tím se zároveň posunou všechny buňky registru o jednu doleva.

Po ukončení tohoto posunu jsou vyčteny nejvyšší bity registrů a jejich XOR vytváří hodnotu hesla v daném kroku. Heslo se pak další operací XOR sloučí s otevřeným textem.

Počáteční naplnění registrů

Nejprve se obsahy registrů vynulují a vypne se nelineární řízení. Všechny registry teď budou krokovat zcela pravidelně. Nyní se připraví 88bitový proud, který je tvořen klíčem Kc, následovaným 22bitovým číslem rámce TDMA. Jako první se z proudu použije nejnižší bit Kc a jako poslední nejvyšší bit TDMA. Následuje 88 kroků, v nichž se do zpětné vazby, jdoucí do nejnižšího bitu registru, „přixoruje" navíc ještě také bit z našeho proudu. Proud je tímto způsobem plněn paralelně do všech registrů.

Protože registry mají jiné zpětné vazby i délky, jejich obsah bude nakonec jiný. Po dokončení tohoto kroku nazveme tento stav *počátečním stavem A5* (resp. jejích registrů). Protože byl vytvořen nezávislými lineárními kombinacemi bitů klíče (nelineární řízení bylo vypnuto), může se reálně dostat do všech 2^{64} možných stavů.

Po úspěšném naplnění se nelineární řízení zapíná a pak následuje 328 kroků, v nichž je produkováno heslo. Jeho prvních 100 bitů se ignoruje, zbývajících 228 bitů h_{101} až h_{328} se už známým způsobem použije pro šifrování přenášených dat.

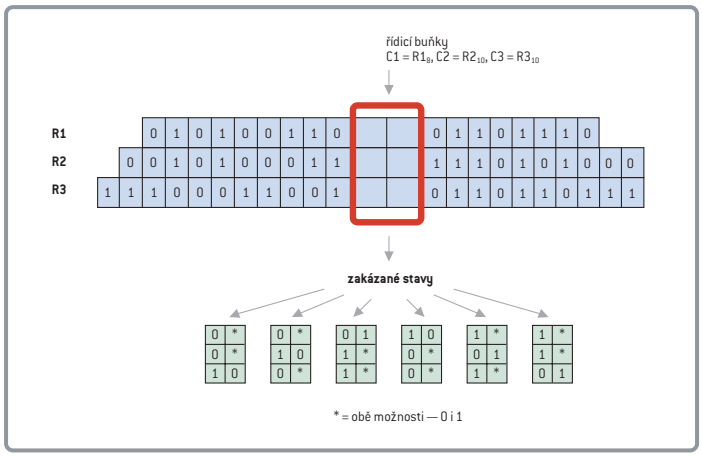
Podstata útoku

Jak se tedy vlastně luští? Celá lušticí metoda má asi 15 klíčových myšlenek, jejichž předběžný popis vydal na 18stránkovou zprávu. Zde z nich popíšeme pouze dvě, které jsou dle našeho názoru opravdu stěžejní. Dnešní popis přitom pojmeme jako obecné seznámení. Na objasnění některých detailů a hlubších souvislostí se potom zaměříme v příštím dílu.

Jak jsme už řekli, je na počátku všeho KPA, který nám umožní získat přímý výstup A5, tak jak byl generován pro dané číslo rámce TDMA. Rozboru úspěšnosti vlastního KPA se budeme věnovat příště. Dnes jen poznamenáváme, že šance na úspěšné provedení KPA v takovém rozsahu, v jakém ho popisovaný útok potřebuje, je v prostředí GSM velmi velká.

„Nejdůležitějším bodem lušticí fáze je nasbírat potřebný počet datových vzorků."

První stěžejní myšlenka se týká principu, podle něhož můžeme ze známé hodnoty výstupu určit vnitřní stav automatu realizujícího funkci A5. To by u kvalitně navrženého kryptosystému samozřejmě nemělo být možné, avšak auto-



Obr. 3. Zakázané stavy v registrech A5/1

rům útoku se to podařilo — nalezli metodu, která s využitím jistého objemu předem vypočtených dat přechod od výstupní posloupnosti k vnitřnímu stavu A5 umožňuje.

Během přípravné fáze lušticího procesu se vygenerují tabulky spojující konkrétní 51bitovou výstupní posloupnost hesla s příslušným vnitřním stavem. Při vlastním luštění je potom v proudu hesla, získaného pomocí KPA, hledán výskyt některé z těchto uložených posloupností. V okamžiku jejího nalezení potom jen nahlédneme do předem vypočtené tabulky a ihned určíme hledaný stav algoritmu A5.

Samo „nahození" A5 do správného vnitřního stavu nám však nestačí, neboť takto bychom byli schopni maximálně doluštit zbývající část komunikace odvysílané v rámci jednoho časového slotu — příští slot bude totiž přenášen v jiném čísle rámce TDMA, a tudíž bude šifrován jiným heslem. My potřebujeme provést u automatu reverzní chod, jímž se dostaneme až k počátečnímu stavu, který vznikl lineárním (neboť řízení hodin bylo vypnuto) sloučením známého čísla rámce TDMA s neznámou hodnotou Kc. Odtud už **přímo určíme tajný klíč Kc** — jeho pomocí pak můžeme snadno luštit jak minulou, tak i veškerou příští komunikaci mezi daným telefonem a sítí GSM. Poznamenejme ještě, že znalost Kc nás ani zdaleka neomezuje pouze na luštění jednoho hovoru. Praktickými testy bylo u jedné z našich sítí ověřeno, že hodnota Kc zde má tak trestuhodně dlouhou životnost, že její případné rozluštění může běžně pokrýt všechny hovory za měsíc!

Za normálních okolností by byl zpětný chod podobného automatu opět velmi složitou záležitostí. Zde se však dostáváme ke **druhé stěžejní myšlence**, která reverzní chod umožňuje. Ta dovedně obrací výhodu nové inicializace A5 s každým dalším rámcem v nevýhodu, neboť v důsledku neustálé reinicializace je cesta od stavu zachyceného k počátečnímu vždy poměrně krátká (maximálně 278 mezistavů).

Krátká vzdálenost od počátečního stavu by sama o sobě také nestačila, kdyby u automatu A5 nebyly pozorovány takzvané *zakázané stavy*. Pro ilustraci se podívejme na obrázek 3. Zde jsme si vystřihli okénko v šíři dvou buněk a přiložili je na registry tak, že vidíme vždy jen řídicí buňku a jejího levého souseda. Pokud budeme nyní v okně sledovat obsah buněk při činnosti A5, nikdy neuvidíme stavy, které jsou na obrázku (hvězdičky znázorňují libovolnou hodnotu).

Těchto „zakázaných" stavů je 24, což představuje 24/64 = 3/8 všech možných stavů tohoto okna! To vede k degradaci původního počtu 2^{64} vnitřních stavů a ke zvláštní stromové struktuře stavů automatu A5. Díky existenci zakázaných stavů je zpětná cesta v A5 nakonec determinističtější, a tudíž schůdnější, než bychom na první pohled očekávali.

Složitost útoku

Stejně jako většina ostatních lušticích metod i tato má fázi přípravnou a fázi vlastního luštění. Během **přípravné fáze** se vytvoří tabulka obsahující 2^{35} stavů automatu A5, která bude během lušticího procesu používána k určení vnitřních stavů. Autorům se podařilo vyvinout metodu, díky níž jsou schopni jednotlivé stavy kódovat pomocí 40bitových řetězců. Výsledná kapacita nutná pro uložení zmíněné tabulky tedy činí zhruba 146 GB; takovýto objem dat je možné uložit například na dva 73GB pevné disky, které jsou už dnes volně dostupné.

Přípravná fáze je náročná nejen na paměť, ale i na čas, neboť pro zkonstruování uvedené tabulky je třeba 2^{38} až 2^{48} operací. Vzhledem k těmto nárokům se přípravná fáze stává vzhledem k potřebným systémovým zdrojům nejnáročnějším krokem celé metody. Velmi závažné ovšem je, že výsledek této fáze (tj. 146 GB tabulek) je naprosto **stejný pro všechny útoky** na algoritmus A5/1 a je použitelný kdekoliv na světě. Pokud by došlo k masovější vlně útoků, lze právem očekávat, že zmíněné dva 73GB disky naplněné potřebnými informacemi se stanou ceněným artiklem průmyslové nebo politické špionáže.

Nejdůležitějším bodem lušticí fáze je nasbírat **potřebný počet datových vzorků**, na kterých jsme schopni provést KPA. Podle stochastických odhadů je na

INFOTIPY:

Web Asociace GSM: ***www.gsmworld.com***
Klonování SIM karet: ***www.scard.org/gsm/***
Ověřený zdrojový kód A5/1:
www.scard.org/gsm/a51.html
Biryukovův-Shamirův útok:
cryptome.org/a51-bs.htm
Bezpečnost GSM: ***jya.com/crack-a5.htm***
Kontakty na luštitelskou trojici:
Marc Briceno (Smartcard Developer Association) ***www.scard.org/gsm/***
Ian Goldberg a David Wagner (skupina ISAAC na univerzitě v Berkeley):
www.isaac.cs.berkeley.edu/isaac/gsm.html
Původní popis A5 a Goličův útok na ni:
jya.com/a5-hack.htm

61procentní úspěšnost vyluštění klíče Kc třeba nasbírat celkem 5 947 836 takových bitů, které jsou tvořeny 228bitovými podřetězci pocházejícími od stejného čísla rámce TDMA. Z toho plyne, že potřebujeme znát obsah celkem 26 087 časových slotů jdoucích v daném rámci TDMA oběma směry. To odpovídá znalosti obousměrné komunikace **v délce dvou minut**. Lze soudit, že uspokojení takového požadavku může být v běžných podmínkách celkem reálné. Více se této problematice budeme věnovat příště.

Časové nároky lušticí fáze jsou dány zejména dobou nutnou pro monitorování datového přenosu. Vlastní práce lušticího počítače se při přístupové době pevného disku menší než 6 ms vejde s přehledem do jedné vteřiny strojového času!

Závěr

O šifře A5 se dosud předpokládalo, že zabrání odposlechu komunikace mezi mobilním telefonem a bázovou stanicí sítě GSM. Dnes už víme, že tuto ochranu lze prolomit. Dále je možné, že existují ještě mnohem efektivnější metody, než jsme dnes ukázali. Navíc oslabená verze A5/2 je podle skupiny luštitelů v Berkeley luštitelná do 15 milisekund! Tyto závěry jsou pro majitele mobilních telefonů samozřejmě znepokojující, a proto vás budeme o novém vývoji v této oblasti neprodleně informovat.

[Vlastimil Klíma | v.klima@decros.cz]
[Tomáš Rosa | t.rosa@decros.cz]

Je tento útok technicky možný?

Bezpečnostní ředitel Asociace GSM James Moran tvrdí, že „nikde na světě nebyla demonstrována schopnost zachytit volání do sítě GSM". Moran říká: „Podle našich znalostí neexistuje hardware, který by byl schopen odposlechu." Myslíme si, že každý trochu zasvěcený technik se tomu musí vysmát. Na trhu totiž existují komerčně dostupné digitální skenery, které umějí zachycovat komunikaci GSM v reálném čase (některá z takových zařízení používají pro testovací účely dokonce i členské organizace Asociace GSM). Dají se ale použít také pro zachycování konverzace u telefonů používajících šifru A5/0 (ta produkuje „nulové heslo", tj. nešifruje), která je údajně použita například v Číně. Ian Goldberg, jeden ze skupiny luštitelů na univerzitě v Berkeley, prohlásil, že pokud ho výrobce těchto zařízení požádá, rád je doplní o možnost dešifrování A5/2 v reálném čase a dešifrování A5/1 ze záznamu.

Protože možnost luštění byla prokázána a algoritmy jsou uloženy v mobilním telefonu, jedinou obranou může být výměna mobilních telefonů. Tato akce se také „výhledově" plánuje — James Moran dokonce řekl, že algoritmus, který tam bude použit, bude poskytnut k veřejnému posouzení. Že by si přece jen uvědomoval vážnost a neudržitelnost situace?