APEK

Agencija za pošto in elektronske komunikacije Republike Slovenije
Stegne 7, p. p. 418
1000 Ljubljana
telefon: 01 583 63 00, faks: 01 511 11 01
e-naslov: info.box@apek.si, http://www.apek.si
davčna št.: 10482369

Republika Slovenija
Državni zbor
Komisija za nadzor obveščevalnih in varnostnih služb
Šubičeva ul. 4
1000 Ljubljana

Številka: 3824-29/2012/8
Datum: 25.9.2012

Vaša št.: 200-15/12-26

Zadeva: Poročilo v zvezi z varnostjo GSM omrežij

Dne 16.7.2012 smo prejeli vašo prošnjo za posredovanje poročila v zvezi z varnostjo GSM omrežij, kot gradivo za obravnavo na nadaljevanju 4. nujne seje KNOVS. V nadaljevanju vam posredujemo pojasnila in odgovore na vaša vprašanja. V **prilogi 1** tega poročila je tudi bolj podrobna predstavitev delovanja mobilnega sistema GSM z vidika zaupnosti in tajnosti elektronskih komunikacij (registracija uporabnika, šifrirni algoritmi itd.).

Povzetek odgovorov operaterjev na poziv agencije

Agencija za pošto in elektronske komunikacije je pozvala vse operaterje mobilnih GSM omrežij (Telekom Slovenije d.d., Tušmobil d.o.o. in Si.mobil d.d.), da se izjavijo v zvezi sumom, da je na radijskem vmesniku GSM omrežja (Um vmesnik) možen vdor v vsebino komunikacije z uporabo odprtokodne programske kode, ki je javno dostopna na svetovnem spletu in strojno opremo cenovnega razreda 1.000,00 EUR.

Telekom Slovenije d.d. (v nadaljevanju: Telekom) je v svojem odgovoru uvodoma opozoril na dva varnostna vidika, ki jih ne gre enačiti ali zamenjevati: zaščita vsebine komunikacije in zaščita identitete uporabnikov. Pri zaščiti vsebine komunikacije gre za potencialno možnost zlorabe zaupnosti komunikacije na radijskem vmesniku (komunikacija med mobilnim terminalom in bazno postajo). V zvezi s tem se je operater izjavil, da omejitve zaradi tehnoloških danosti GSM sistema in globalno standardiziranega sistema, na katere operaterji nimajo vpliva, predstavljajo največjo potencialno ranljivost omrežja GSM. V nadaljevanju je Telekom povedal, da globalno gledano, vsa omrežja in terminali podpirajo šifrirni algoritem A5/1, kakšna polovica terminalov oz. omrežij pa podpira tudi algoritem A5/3, ki je v primerjavi z A5/1 močnejši. Telekom je pojasnil, da v svojem omrežju na radijskem vmesniku Um uporabljajo šifrirni algoritem A5/1 in tam kjer je možno, tudi A5/3. Kot razlog, zakaj v celotnem omrežju nimajo implementiranega algoritma A5/3, so navedli, da imajo v omrežju tudi 10 let stare bazne postaje, ki ne podpirajo nadgradnje in posledično uporabe šifrirnega algoritma A5/3. V zvezi z nadgradnjo starih baznih postaj (na algoritem A5/3) je Telekom izpostavil tudi smiselnost teh posodobitev z vidika prihodnosti sistema GSM, saj se bliža leto 2013, ko bodo potekle odločbe o dodelitvi radijskih frekvenc za GSM.

Si.mobil d.d. (v nadaljevanju: Simobil) se je izjavil, da v svojem omrežju na radijskem vmesniku Um uporabljajo šifrirni algoritem A5/3 za tiste terminale, ki ta algoritem podpirajo in A5/1 za vse ostale. Šifrirni algoritem A5/3 je implementiran v celotnem omrežju Simobila.

Tušmobil d.o.o. (v nadaljevanju: Tušmobil) se je izjavil, da v svojem omrežju na radijskem vmesniku Um uporabljajo le šifrirni algoritem A5/1.

Stanje v državah članicah EU

Agencija je raziskala, kako imajo to področje urejeno druge članice EU. Zato je agencija zaprosila nacionalne regulatorje držav članic, da odgovorijo na naslednja vprašanja:

1. Katere šifrirne algoritme (A5/x) uporabljajo mobilni GSM operaterji na Um vmesniku v vaši državi?
2. Ali ste operaterjem naložili obveznost oz. izdali priporočilo v zvezi zagotavljanjem varnosti na radijskem vmesniku Um?
3. Če ste naložili obveznost ali izdali priporočilo, kateri šifrirni algoritem (A5/x) ste določili?

Agencija je prejela odgovore 11 nacionalnih regulatorjev, ki so v **prilogi 2** tega poročila. Devet regulatorjev je poročalo, da operaterji v njihovih državah, uporabljajo šifrirni algoritem A5/1, od teh je v dveh državah v uporabi tudi A5/0, to se pravi komunikacija brez šifriranja. Dva regulatorja sta poročala, da podatkov nimajo. Noben od regulatorjev, ki so odgovorili na našo anketo, ni poročal, da je v celotnem omrežju v implementiran šifrirni algoritem A5/3.

Anketirani regulatorji so poročali, da niso naložili noben regulatorni ukrep v zvezi s šifrirnim algoritmom.

V spodnji tabeli je primerjava med stanjem v Sloveniji in drugimi državami članicami EU.

	EU*	**Slovenija**
Šifrirni algoritem A5/1	Da	Da
Šifrirni algoritem A5/3	delno	Mobitel (delno), Simobil (v celem omrežju), Tušmobil (ne)
Regulatorni ukrep v zvezi s šifrirnim algoritmom	-	-

* - članice EU/EEC in R Hrvaška

Stališče agencije v zvezi varnostjo GSM omrežij slovenskih operaterjev

Na osnovi odgovorov slovenskih GSM operaterjev in nacionalnih regulatorjev, agencija ugotavlja, da slovenski operaterji GSM omrežij (Telekom, Simobil in Tušmobil) zagotavljajo slovenskim uporabnikom primerljivo stopnjo zaupnosti in tajnosti komunikacij ter zaščito prenosa podatkov, kot jo imajo uporabniki v drugih državah, članicah EU.

GSM omrežje je mobilno omrežje druge generacije (2G), ki je načrtovano v 90 letih prejšnjega stoletja. Specifikacija GSM standarda iz leta 1993 (GSM 02.09[1]) opredeljuje več področij varnosti, med drugim tudi način zagotavlja zaupnosti podatkov in signalizacije. GSM specifikacija podpira do sedem različnih (A5) šifrirnih algoritmov. Izbira algoritma je odvisna od razpoložljive strojne in programske opreme tako na strani omrežja, kot na strani uporabnika (mobilnega terminala). Ko je pokazala naša anketa, najbolj uporabljen šifrirni algoritem v evropskih mobilnih omrežij je A5/1.

V času ko je omrežje bilo načrtovano in implementirano, je bilo to eno od najbolj naprednih omrežij, tako z vidika storitev kot varnosti. Procesorska moč, ki so jo imeli navadni uporabniki na voljo pred dvajsetimi leti, ni zadostovala za razbijanje standardiziranih GSM šifrirnih algoritmov v realnem času. Vse več pa je znanstvenih člankov[2], da bi procesorska moč današnjih računalnikov zadoščala za razbijanje GSM šifrirnega algoritma A5/1. Kljub temu, da agencija nima trdnega dokaza, da je razbijanje šifrirnega algoritma A5/1 v realnem času možna (za govorno storitev), se tudi agenciji to ne zdi nemogoče. Operaterji imajo na voljo tudi druge varnostne ukrepe, ki skupaj s šifrirnim algoritmom A5/1 lahko zmanjšajo varnostna tveganja.

---

1 3GPP TS 02.09 (http://www.3gpp.org/ftp/Specs/html-info/0209.htm)

2 *Security Research Lab: Decrypting GSM phone calls (https://srlabs.de/decrypting_gsm/), Black Hat (2008): Intercepting GSM traffic (http://www.blackhat.com/presentations/bh-dc-08/Steve-DHulton/Presentation/bh-dc-08-steve-dhulton.pdf), Quirke J. (2004): Security in the GSM system (http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.108.1509&rep=rep1&type=pdf) itd.*

Agencija bo v okviru nadzora priporočila operaterjem, da proučijo te možnosti in jih implementirajo.

Vlaganja v nove tehnologije, ki bi preprečila nezakonite vdore v GSM omrežja (2G)

Razvoj mobilnih omrežij je šel naprej in operaterji predvsem vlagajo in uvajajo omrežja naslednjih generacij (3G, 4G), ki so odpravila varnostna tveganja omrežij druge generacije (GSM). Za omrežja naslednjih generacij (3G, 4G) lahko z veliko gotovostjo trdimo, da procesorska moč in orodja, ki jih imajo navadni uporabniki na voljo danes, ne zadostujejo za razbijanje šifrirnih algoritmov in drugih varnostnih ukrepov. Zato od operaterjev omrežij GSM (2G) lahko pričakujemo največ, da ta omrežja vzdržujejo in z manj ali več standardiziranimi oz. lastnimi rešitvami[3] odpravljajo ranljivosti mobilnega omrežja GSM.

Skratka, danes operaterji (in standardizacija) ne vlagajo veliko v tehnologijo 2G (GSM). Operaterji vlagajo danes predvsem v omrežja naslednjih generacij (3G in 4G). Z vlaganjem v omrežja 3G in 4G se odpravljajo šibkosti 2G, ki se bo enkrat, podobno kot omrežje prve generacije (NMT), ukinilo. Zato, kakšnih novih tehnoloških, standardiziranih rešitev ali nadgradenj omrežja GSM ni pričakovati. Ne gre pa pozabiti na nova varnostna tveganja (npr. spletne prevare), ki jih globalnost, dostopnost in nove storitve prinašajo.

Pristojnost za nadzor

Agencija je pristojna za izvajanje nadzora pri vseh operaterjev, ki so prisotni in ponujajo storitve elektronskih komunikacij na ozemlju Republike Slovenije. Na obmejnem področju, zaradi fizikalnih lastnosti razširjanja radijskih valov, lahko slovenski uporabniki uporabljajo tudi mobilne storitve tujih operaterjev, kljub temu, da so na ozemlju R Slovenije, vendar gre v tem primeru za storitev gostovanja. Agencija ne izvaja nadzora nad tujimi operaterji, ki so s signalom prisotni na ozemlju R Slovenije.

Agencija bo v nadaljevanju postopka nadzora na lokaciji posameznih operaterjev preverila navedbe operaterjev. V primeru, da bo operater v celem omrežju na vmesniku Um zagotavljal šifrirni algoritem najmanj A5/1, bo agencija s sklepom ustavila postopek nadzora in jim priporočila, da implementirajo še druge ukrepe, ki skupaj s šifrirnim algoritmom A5/3 zmanjšujejo varnostno tveganje. V postopku nadzora bomo pregledali in ocenili primernost metodologije za oceno varnostnih tveganj, analizo tveganj in ukrepov. Postopke nadzorov, ki jih agencija vodi proti trem operaterjem (Telekom, Simobil in Tušmobil), bomo zaključili predvidoma v prvi polovici oktobra.

Na morebitna dodatna vprašanja vam bomo odgovorili v čim krajšem času. Prosimo vas, da se pri tem sklicujete na našo opravilno številko.

Pripravil:
Albin Poljanec
pooblaščena oseba agencije

po pooblastilu št. 0202-1/2012/22 z dne 24.9.2012
Mark Pohar
Namestnik direktorja

Priloge: Kot izhaja iz besedila
Vročiti: Naslovniku priporočeno

Vložiti: tu

---

[3] *Uporaba mehanizma frekvenčnega skakanja, zapolnjevanje sporočil z naključnimi biti, pogostejša izmenjava šifrirnih ključev itd.*

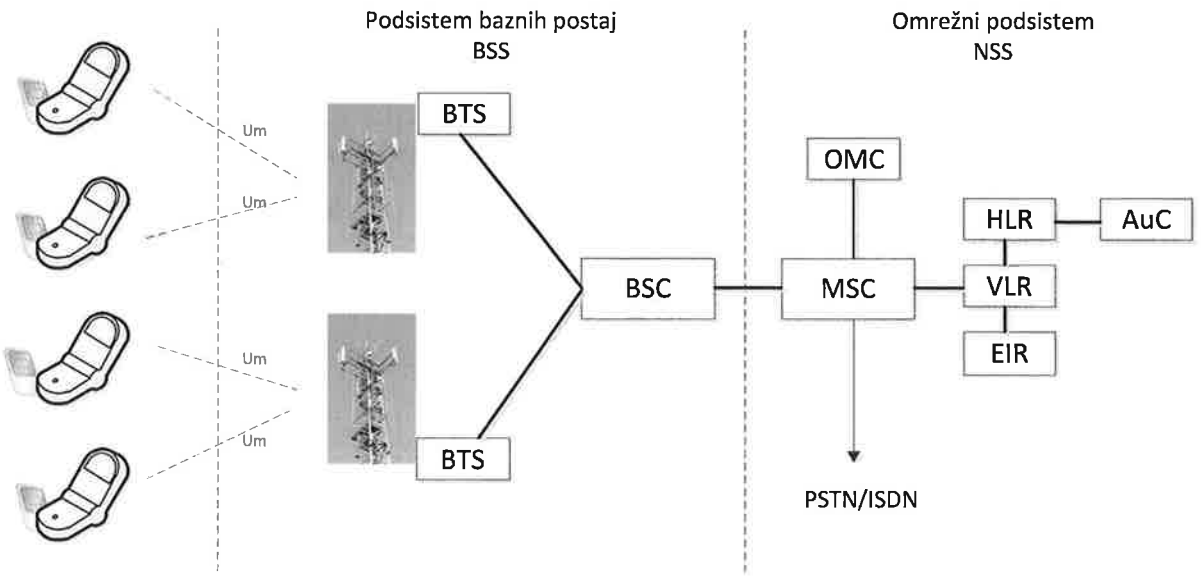
Priloga 1 (3824-29/2012/7)

Gradniki omrežja GSM z vidika zagotavljanja tajnosti in zaupnosti komunikacij

GSM (Global System for Mobile Communications) je standard, katere specifikacije so bile razvite leta 1990 in predstavljajo drugo generacijo mobilnih celičnih omrežij. Čeprav tehnologija obstaja že 20 let, se navkljub napredkom in novim tehnologijam zaradi svoje zanesljivosti še vedno uporablja kot primarna tehnologija za omogočanje govornih storitev.

GSM omrežje se stoji iz treh glavnih delov:

- Mobilna postaja (angl. Mobile Station - MS): ta vključuje mobilen terminal in modul SIM (angl. Subscriber Identification Module), ki omogoča identifikacijo naročnika in šifriranje podatkov.
- Podsistem baznih postaj (angl. Base Station Subsystem - BSS): upravlja in nadzira radijsko povezavo z mobilnim terminalom. BSS je sestavljen iz množice baznih postaj (angl Base Transceiver Station - BTS) ter nadzornika baznih postaj (angl. Base Station Controller – BSC). En BSC pokriva večje število BTS.
- Omrežni podsistem (angl. Network Subsystem - NSS) in omrežni preklopni podsistem (Network and Switching Subsystem - NSS): centralni del inteligence, ki s pomočjo mobilnega komutacijskega centra (Mobile service Switching Center - MSC) omogoča vzpostavitev, vzdrževanje in podiranje klicev ter zagotavlja upravljanje storitev in overjanje uporabnikov.
  Pomemben del omrežnega podsistema so tudi registri, v katerih se hranijo ključni podatki o naročniku:
  - Register domačih naročnikov (angl. Home Location Register – HLR)
    Baza vsebuje vse podatke o naročniku (IMSI, MSISDN, MSRN) in njegovih storitvah, vključno z zadnjo lokacijo naročnika
  - Register gostujočih naročnikov (angl. Visitor Location register - VLR)
    Ta je običajno del komutacijskega centra (MSC) in vsebuje podatke o gostujočih uporabnikih na območju določenega MSC
  - Register opreme (angl Equipment Identity Register – EIR)
    Podatkovna baza, ki vsebuje seznam vse dovoljene opreme v omrežju
  - Avtentikacijski oziroma overitveni center (angl. Authentication Center – AuC)
    Vsebuje kopijo tajnega šifrirnega ključa, ki se uporablja za overjanje in šifriranje radijskega kanala



Povezava med mobilnim terminalom (MS) in bazno postajo (BTS) je zagotovljena preko radijske povezave oziroma radijskega vmesnika (Um), povezava med BSS in NSS pa poteka po fiksnem omrežju. V skladu z GSM standardom je vsa komunikacija med bazno postajo in BSS šifrirana, standard pa določa različne šifrirne mehanizme. Ker gre na radijskem delu komunikacije za skupni medij, lahko vsi terminali v določeni celici (področju pokrivanja BSS) sprejmejo vsa sporočila, ki jih pošilja BSS, dešifrirajo pa jih le tisti terminali, katerem je sporočilo namenjeno.

Naročnikovo identiteto v omrežju predstavlja pametna kartica SIM, ki je dejansko manjši mikroprocesor s tremi vrstami pomnilnika (ROM, RAM, EEPROM).

- ROM vsebuje operacijski sistem, aplikacije in varnostne algoritme A3 in A8, ki omogočajo overjanje naročnika in šifriranje govora in podatkov. Šifriranje temelji na identiteti naročnika (angl. International Mobile Subscriber Identity – IMSI) in varnostnega šifrirnega ključa)
- RAM se uporablja za medpomnenje prenesenih podatkov in izvršilne funkcije
- EEPROM vsebuje
    - Identiteto naročnika (IMSI in PIN)
    - Klicne številke (IMSI in MSISDN)
    - Šifrirne ključe Ki in informacije, ki se nanašajo na omrežje (začasno dodeljeno številko TMSI in lokacijsko informacijo – LAI)
    - Identifikacijo terminala (angl. International Mobile Equipment Identity - IMEI)

Na SIM kartici so vprogramirane vse potrebne funkcije in šifrirni ključ, ki omogoča overjanje naročnika in šifriranje govora in podatkov. Kopija šifrirnega ključa se nahaja tudi v AuC registru. SIM kartica na podlagi vhodnih podatkov izvaja tudi generiranje novih šifrirnih ključev, s katerimi se zaščiti komunikacija. Praviloma so podatki na SIM kartici zapisani na način, ki preprečujejo nepooblaščeno branje in spreminjanje teh podatkov. SIM kartica je zaščitena s PIN (angl. Personal Identification Number) varnostno kodo. Uporabnik lahko sam spremeni varnostno PIN kodo oziroma je celo nima nastavljene, kar predstavlja varnostno tveganje. Preizkusi so pokazali, da lahko ob ustrezni programski in strojni opremi ter poznavanju šifrirnih ključev tudi brez SIM kartice zajemamo (in analiziramo) promet, ki se generira na radijskem vmesniku.

Terminal se lahko prijavi (oz. uporablja) v omrežje le, če je uspešno izvedena faza overjanja. GSM ima vgrajenih več varnostnih funkcij, ki omogočajo zasebnost uporabnika.
Te vključujejo:

- Overjanje registriranega naročnika (ali predplačnika) v omrežje
- Zaupnost podatkov in signalizacije
- Zaupnost uporabnika (zagotavljanje anonimnosti)

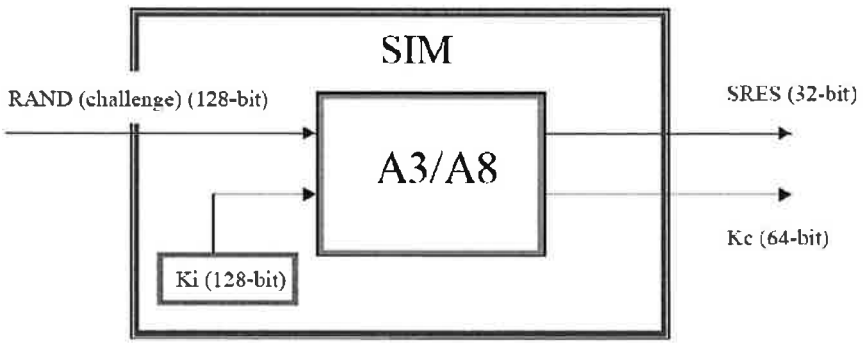
Overjanje in registracija uporabnika v omrežje

Ko operater vključi v omrežje novega naročnika, mu dodeli pametno SIM kartico, ki med drugim vsebuje unikatno mednarodno petnajstmestno indentifikacijsko številko IMSI (angl. International Mobile Subscriber Identity) in pripadajoči skrivni overitveni ključ Ki. IMSI je sestavljena iz kode države (293), kodo mobilnega omrežja (40, 41, 070..) in identifikacijske številke naročnika (xxx). Zaradi dodatne varnosti se v omrežju uporablja tudi t.i. začasna številka TMSI, ki je pogojena na trenutno lokacijo naročnika. Overitveni ključ Ki je skrivni 128-bitni ključ, ki ga proizvajalec preda operaterju ob predaji SIM kartice. Ključ Ki se nahaja samo na SIM kartici in njegova kopija v overitvenem centru (AuC). Ključ Ki je praviloma hranjen v AuC v šifrirani obliki in se uporablja za generiranje overitvenega trojčka, ki se na podlagi zahteve iz HLR generira v AuC in služi za overjanje in proces šifriranja podatkov. Trojček je sestavljen iz treh povezanih vrednosti:

- naključnega 128-bitnega števila (RAND)
- 64-bitnega šifrirnega ključa Kc, ki temelji na GSM A8 algoritmu in je rezultat izračuna z vhodnima parametroma števila RAND in skrivnega ključa Ki
- SRES (angl. Signed RESsponse) 32-bitnega ključa, ki temelji na GSM A3 algoritmu in je rezultat izračuna z vhodnima parametroma RAND in skrivnega ključa Ki

A3 in A8 algoritma se uporabljata za generiranje SRES in Kc vrednosti, ki predstavljata t.i. overitveni trojček. Oba algoritma sta shranjena v AuC in SIM kartici naročnika.

Ko terminal prižgemo, terminal pošlje na radijski vmesnik proti bazni postaji svojo IMSI identifikacijo ter zahtevek za overitveni trojček. Zahtevek za overjanje se iz BTS prenese na BSC, ta pa pošlje zahtevek v HLR register. HLR preko MAP protokola pošlje overitveni zahtevek do AuC. AuC na podlagi IMSI številke poišče pripadajoč tajni šifrirni ključ. Ker je Ki ključ shranjen v bazi v šifrirani obliki se pred izvedbo overitvenega trojčka predhodno z DES (angl. Data Encryption Standard) algoritmom izvede še dešifriranje ključa. AuC najprej generira 128-bitno naključno vrednost (RAND), ki se jo pošlje preko omrežja (MSC/VLR) tudi do mobilnega terminala oziroma SIM kartice. RAND in vrednost Ki sta vhodna podatka za algoritma A3 in A8. Implementacija algoritmov A3 in A8 je neodvisna od proizvajalcev opreme in operaterjev. Večina operaterjev za A3 in A8 uporablja algoritem COMP128. COMP128 proizvede 128-bitno vrednost, pri čemer prvih 32-bitov (z A3) predstavlja vrednost SRES in 54 bitov dolg sejni ključ Kc (A8) . H ključu Kc se doda še 10 ničel, s katerimi dobimo končno 64 bitno vrednost sejnega ključa Kc, ki se ne spremeni, dokler ne pride do ponovnega overjanja. Običajno AuC hkrati generira pet overitvenih trojčkov. COMP128 naj bi vseboval pomanjkljivosti, saj naj bi praksa pokazala, da je mogoče v določenem primeru iz ne tako velikega števila parov RAND-SRES izračunati vrednost Ki.

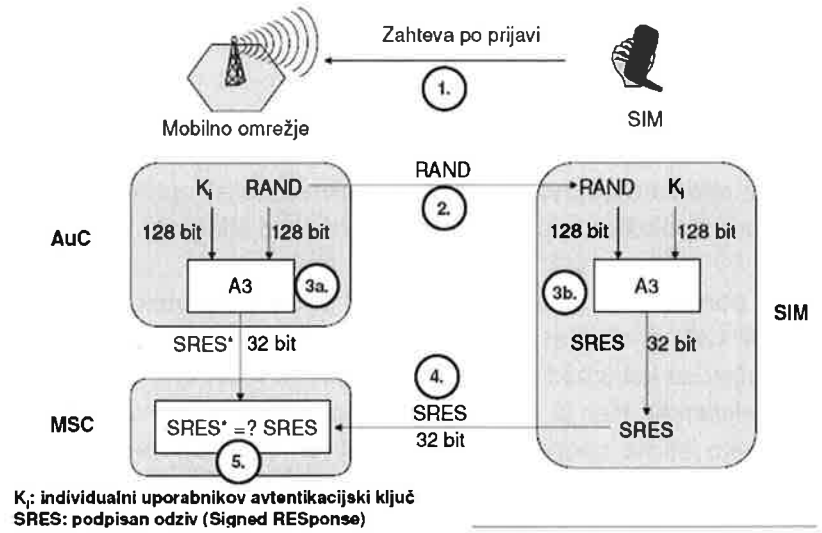


AuC generiran trojček (SRES, RAND in Kc) kot odgovor na overitveni zahtevek pošlje nazaj do HLR, HLR pa ga pošlje do MSC. MSC shrani vseh pet overitvenih trojčkov v register gostujočih uporabnikov (VLR). Ko se jih porabi, se izvede ponovna zahteva za generiranje novih.

Mobilni terminal prav tako uporabi iz MSC prejeto RAND vrednost in s pomočjo svojega Ki ključa in preko A3 algoritma izračuna svojo SRES vrednost ter jo pošlje nazaj do MSC. Ker je RAND ob vsakem overjanju drugačen, se spreminja tudi SRES vrednost. Overjanje uporabnika oz. njegove SIM kartice v omrežje je uspešna, če MSC ugotovi, da sta SRES vrednosti, ki sta bili izračunani v AuC in v mobilnem terminalu, enaki.

V primeru selitve naročnika na drugo celico, ki spada pod drugo lokacijsko področje (LAI), se postopek overjanja ponovi, vendar se za overjanje ne uporablja identifikacijsko številko IMSI, temveč začasno mobilno številko imenovano TMSI (angl. Temporary Mobile Subscriber Identity).

Ta se shrani na SIM kartico in prepreči, da bi morebitni prisluškovalec pridobil identiteto uporabnika (zagotavlja anonimnost naročnika). TMSI številka (ki se ohrani četudi se terminal ugasne) se namesto IMSI uporablja pri naslavljanju terminala vse dokler ne zamenja lokacijskega področja. V tem primeru se TMSI spremeni, skozi omrežje pa se druga številka praviloma pošlje v šifrirani obliki, kar onemogoča sledenju naročnika. Povezava med IMSI in TMSI je shranjena v VLR registru.



Vir: LTFE

Zaupnost podatkov in signalizacije

V GSM omrežju je zaupnost pogovorov in signalizacije, ki se prenašajo kot podatki na radijski poti med mobilnim terminalom in bazno postajo zagotovljena s šifriranjem (SMS sporočila se prenašajo v okviru signalizacijskih podatkov). Šifriran je pogovor in vsi pripadajoči podatki, ki se prenašajo preko signalizacije, vključno z IMSI in IMEI, razen v času prve vzpostavitve povezave (vključitev terminala) terminala z omrežjem. Za šifriranje podatkov se uporablja algoritem A5. Obstaja sedem možnih različic algoritma A5 in osma z odprtimi podatki.

V praksi se največ uporabljajo naslednji A5 algoritmi, ki omogočajo šifriranje govora, podatkov in signalizacije:

- A5/0: ne omogoča šifriranja
- A5/1: je originalni A5 algoritem, ki se uporablja v Evropi
- A5/2: (je šibkejši algoritem, ki je bil namenjen za izvoz in se uporablja v ZDA
- A5/3 (temelji na algoritmu Kasumi 3GPP TS 55.216) je močnejši šifrirni algoritem, ki je bil razvit s sodelovanjem GSMA Security Group in 3GPP (angl. 3rd Generation Partnership Project)

Govori se, da so bili razbiti že vsi prvi trije algoritmi (ter menda tudi zadnji A5/3). Od leta 2009 je razvit (3GPP TS 55.226- Relase 6) še močnejši A5/4 algoritem, ki prav tako temelji na algoritmu Kasumi, vendar uporablja daljše *KLEN* ključe.

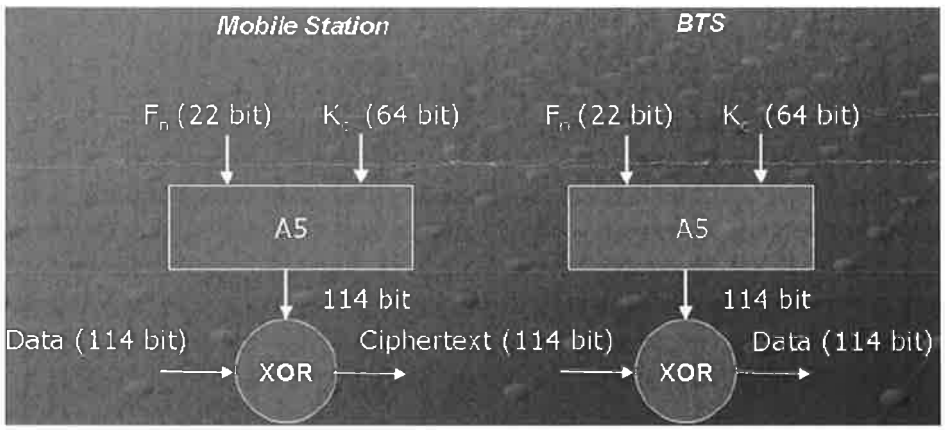
Kot je pokazalo testiranje in tudi javna objava rezultatov slovenskih raziskovalcev, mobilni operaterji v Sloveniji trenutno uporabljajo naslednja šifriranja:

- Mobitel: A5/1

- Tušmobil: A5/1
- Simobil: A5/3 (v času testiranja je uporabljal A5/0)

Začetek šifriranja komunikacije med mobilnim terminalom in bazno postajo po uspešnem overjanju pride z ukazom iz GSM omrežja. V praksi to pomeni, da operater mobilnega omrežja na podlagi razpoložljive strojne in programske opreme sam izbere stopnjo šifriranja oz. vrsto (A5) šifrirnega algoritma. Stopnja šifriranja govora in podatkov pa ni pogojena samo s tehničnimi lastnostmi omrežja, temveč tudi z lastnostmi mobilnega terminala. Operater ima možnost, da nastavi zahtevnejši šifrirni algoritem, v kolikor pa ga terminal ne podpira, omrežje poskusi z naslednjim slabšim šifriranjem. Operater ima praviloma vse mobilne terminale zavedene v svojem registru opreme (EIR). Ker je večino terminalne opreme subvencionirane, lahko operater ob pomoči registra EIR z relativno gotovostjo presodi, kakšen delež opreme podpira določen šifrirni algoritem in v skladu z razpoložljivo opremo primerno nastavi šifriranje.

Za šifriranje govora, podatkov in signalizacije se kot vhodni podatek v A5 algoritem uporabi z algoritmom A8 (COMP128) izračunan sejni ključ Kc in trenutna številka 22-bitnega TDMA okvirja (F_N). 114-bitni tok ključev se kot izhod iz A5 algoritma preko XOR vrat sešteva z vhodnimi podatki (govor, podatki, signalizacija). Ker je sejni ključ Kc pogojen z začetnim overjanjem, se v praksi lahko zgodi, da se lahko isti Kc uporablja tudi več dni (ali dalj) zapored oziroma se spremeni ob naslednjem overjanju.



Vir: http://www.gsm-security.net/gsm-security-papers.shtml

Različni raziskovalci poročajo, je primarni algoritem za šifriranje podatkov (A5/1) ob ustreznem znanju in opremi možno zlomiti. Ključen podatek, s katerim se lahko razbije algoritem, je skrivni ključ Ki. Najbolj nevaren napad je pridobitev podatkov neposredno iz SIM kartice. Raziskovalna skupina Smartcard Developer Association in ISAAC je ugotovila pomanjkljivost v COMP128 algoritmu, ki omogoča pridobitev tajnega ključa Ki iz SIM kartice. Napad je izvedljiv tako fizično neposredno na kartici s pomočjo bralnika kartic in računalnika kot tudi preko radijskega vmesnika.

Dešifriranje podatkov, šifriranih z algoritmom A5/1, je mogoče izvesti z ustreznim znanjem in opremo tudi preko radijskega vmesnika. Profesionalne naprave, ki bi jih lahko uporabile različne službe, to zanesljivo omogočajo. Hekerski pristopi pa so se v praksi izkazali kot bolj ali manj uspešni, pri dešifriranju podatkov. V prvem primeru je oprema dostopna praviloma le državnim organom, v drugem primeru pa je potrebno imeti ustrezno računalniško programsko in strojno opremo, ki jo je mogoče prosto pridobiti na trgu. Potrebujemo univerzalni radijski sprejemnik (Universal Software Radio Peripheral - USRP), ki zna sprejemati radijski signal iz GSM omrežja ter specifično programsko opremo, ki izvaja analizo signalov (odprtokodni GNU radio). Za

dešifriranje podatkov, ki se jih zajema iz radijskega vmesnika, lahko morebitni vsiljivec uporabi t.i. mavrične tabele. Gre za tabele s predizračunanimi vrednostmi delov šifrirnih ključev, ki omogočajo hitrejšo kriptoanalizo sprejetih podatkov (npr. program Kraken) in hkrati zahteva za računalnik manj procesorskega časa. Za drugi primer seveda velja, da zahteva tudi znanje programiranja, kot dobro poznavanja delovanja GSM omrežja.

Pripravil:

Urban Kunc

	Q1: Which ciphering algorithm (A5/x) for protecting an air interface has been primarily used by the mobile operators in your country?	**Q2: Have you imposed any obligation org guidelines regarding securing an air interface?**	**Q3: If so, which one did you impose?**
EU	A5/1 any operator deploying 3GPP Release 6 on can use A5/3, this algorithm is not currently deployed by operators.	No.	
EU	For GSM networks, the A5/1 algorithm has primarily been used.	No, privacy of communications is a matter of data protection. Therefore, the competent authority is primarily the Data Protection Commission. To our knowledge, there are no guidelines regarding securing an air interface.	N/A.
EU	As far as we know, the three GSM operators use A5/1 for ciphering their air interface.	We do not impose any specific obligations regarding securing the air interface. They are obliged to follow the 3GPP GSM specifications, so the use of A5/1 will fulfill this obligation.	
EU	Ciphering algorithms (as well as authentication algorithms) are secret. To our knowledge, at least 3 of the 4 main mobile operators use the same ciphering algorithm, A5-1.	No	N/A
EU	Our authority doesn't deal with security questions regarding GSM network systems so we don't possess the appropriate information you've required. Therefore we cannot give you proper answers to these questions.		
EU	A5/0 and A5/1	Today is not any specific legislation regarding to securing an air interface for GSM networks	
EU	The ciphering algorithm depends on the version of a mobile telecommunications system that was purchased and implemented by a given operator. For older equipment this was a 5/1 version (with a simplified ersion 5/2 or even 5/0, i.e. without ciphering). Currently operators are migrating to 5/3. For UMTS UEA0, UEA1. It is also important to remember that the applicable ciphering algorithm depends on a mobile terminal as the terminal is involved in ciphering.	There are no requirements as regards ciphering – the relevant ETSI standards are applied, 3gpp etc.	See left.
EU	It must be emphasised that NRA has not thoroughly surveyed the encryption protocols employed by mobile phone operators. Hence, the material presented here is anecdotal at best. It is the belief of NRA that all operators employ A5/1 in their algorithm suite. As far as we know, none of the operators have enabled the use of A5/2. It is our belief that the implementation of A5/2 has been removed in the mobile terminals since 2007. None of the operators have forced encryption to be taken off completely (A5/0) on a regular basis, but may opt to temporarily activate it during periods of exceptionally heavy loads. According to the information available to NRA, A5/3 has been tested since 2009 but the availability of A5/3 throughout the network is not known. Same applies to A5/4. The adoption of the more modern algorithms is limited both by high investment costs in BSS (stronger encryption requires modern equipment in the base station infrastructure) and by the limitations set by older mobile terminals.	Not as such. According to Communications Market Act , section 128, the networks must be planned, built and maintained in a manner that "the protection of privacy, information security and other rights of users and other persons are not endangered". This provision has, however, not been interpreted in a way that would make it necessary to regulate the implementation of encryption algorithms in the networks. NRA encourages end users to protect their privacy and corporate secrets by utilising suitable protective measures, including encryption. The national legislation does not prohibit the use of strong encryption. In the end, however, it is a matter of productisation on the service providers' side and a matter of risk management on end users' side. NRA also acknowledges that no end user should rely solely on the protections provided by the carrier network. For any serious data protection need, use of end-to-end encryption is required.	N/A
EU	We didn't impose any obligation in terms of the algorithm.		
Izven EU	Ciphering algorithm for protecting an air interface primarily used by mobile operators is A5/1	There are no any obligations or guidelines regarding securing an air interface.	n/a
EU	A5/1	No	

Pripravil:

Albin Poljanec