Bezpieczeństwo sieci bezprzewodowych GSM

Karta SIM, usługi bezpieczeństwa, uwierzytelnianie, algorytm A3/A8, poufność oraz integralność

Patryk Kaniewski

2021-05-10

Outline

Rozwiązanie problemów z GSM

Wstęp

W tej prezentacji zostaną przedstawione rozwiązania bezpieczeństwza sieci komórkowych.

- Ogólne idee bezpieczeństwa sieci bezprzewodowych
- Problemy 2G (GSM)
- Rozwiązania problemów z GSM

Bezpieczeństwo

Bezpieczeństwo systemów teleinformatycznych

Ogół technik, procesów i praktyk stosowanych w celu ochrony sieci informatycznych, urządzeń, programów i danych przed atakami. W informatyce mówimy głownie o procesie bezpieczeństwa, zaczyna sie on od projektowania i implementacji dobrych praktyk, i trwa poprzez życie produktu poprzez stałe wsparcie (komercyjne lub społeczności).

Ograniczenia sieci bezprzewodowych:

W porównaniu do sieci przewodowych, sieci bezprzewodowe (takie jak sieci komórkowe) mają dużo problemów:

- Otwarty dostęp - nie ma fizycznego oddzielenia które zwiększa zaangażowanie osoby atakującej
- Złożoność systemu - system składa sie z wielu elementów urządzenia końcowe <-> anteny <-> sieć wspierająca

Ograniczenia sieci bezprzewodowych (kont.):

Problemy w części rozwiązane

- Ograniczenia przepustowości - bardziej wydajne rozwiązania powoduja wiekszy popyt na urządzenia podłaczone do sieci (IoT)
- Niestabilość sieci bezprzewodowych - zakłocenia powodują straty i potrzeba jest retransmisji

Problemy rozwiązane:

- Ograniczona moc obliczeniowa
- Ograniczenia poboru mocy

Zagadnienia bezpieczeństwa

- Autoryzacja
- Integralność
- Poufność
- Bezpieczeństwo urządzenia

Autoryzacja

Telefon komórkowy znajduje się w kieszeni każdej osoby, a podróż przez granice a nawet oceany jest w zasięgu wiekszej liczby osób

- Urządzenie musza współpracować z sieciami różnych krajów aby zapewnić wysoką jakość usługi
- Osoby niebędące abonentami takiej sieci nie powinny mieć dostępu

Integralność

Wysyłając czy otrzymując wiadomość użytkownik musi być pewny że dotarła ona w całości a jednocześnie nic nie zostało do niej dołączone.

- Sieć musi zapewnić jakiś mechanizm sprawdzania czy dana wiadomość jest poprawna
- Sieć musi zapobiec podszywaniu się pod innego użytkownika

Poufność

Często używamy sieci bezprzewodowej do wysyłania informacji poufnej, oczekujemy również prywatności nawet w sytuacjach w których zajmujemy się zwykłymi danymi

- Sieć musi zapewnić że nasze prywatne wiadomości nie dostaną sie w niepożądane ręce
- Idealnie nawet dostawca usługi nie może tych wiadomości podejrzeć (End-to-End)

Bezpieczeństwo urządzenia

Urządzenia klienckie stają się coraz bardziej zaawansowane

- Nawet jeżeli systemy takie jak Android oferuja mniejszy dostęp do sprzętu fizycznego nadal są narażone na ataki
- Słabe praktyki bezpieczeństwa u producentów urządzeń mogą pozostawiać dużą liczbę urządzeń niezabezpieczonych

DOS

Atak na sieć lub urządzenie poprzez wysyłanie dużej ilości wiadomości który zagłusza inne prawdziwe wiadomości lub całkowicie blokuje urządzenie

DDOS

Atakujący posiadający botnet urządzeń może wykonać ataki wielkiej skali które mogą zablokować całą sieć. W sytuacjach kryzysowych, duża liczba użytkowników może również wywołać podobny efekt

Jamming

Atak miejscowy na infrastrukture, polega on na zagłuszeniu jednej lokalizacji. Jedyną ochroną przed tego typu atakami jest droga legalna.

Nieautoryzowany dostęp

Do systemu podłączane są urządzenia które nie zostały wprowadzone przez operatora takiej sieci, mogą służyć do innych ataków lub jako forma nielegalnej "konkurencji"

Nasłuch

Atakujący ma dostęp do danych wysyłanych przez taką sieć. Tracimy wtedy prywatność takiej sieci gdyż wszystkie informacje są dostępne do atakującego. Jest to zwykle "cichy" atak, ofiara zwykle nie jest świadoma że sieć jest złamana

Message forgery

Niezabezpieczona komunikacja jest podatna na ataki w których atakujący podszywa się pod innego użytkownika sieci i może wysyłać i/lub modyfikować wysłane wiadomości

Message Replay

Nawet w niektórych zabezpieczonych sieciach atakujący może zapisać wiadomości i odtworzyć takie wiadomości w innym czasie aby uzyskać pożądany efekt

Rozwiązanie problemów z GSM

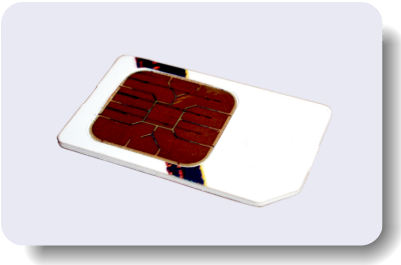
Otwarte pytanie

Ile komputerów jest w twoim telefonie?

"Karta SIM"

UICC

Mówiąc o karcie SIM, mowimy tak naprawde o UICC (Universal Integrated Circuit Card) która zapewnia usługi SIM (CSIM/USIM itp.). UICC jest to SoC który zawiera własny procesor, RAM, oraz ROM, i posiada specjalne programy którę udostępniają różne funkcje sieci komórkowej.



SIM

Jest to SoC (System on a Chip) przeznaczony do bezpiecznego (fizycznego) przechowywania danych oraz zapewniania pewnych usług:

- IMSI
- klucz prywatny (K_i)
- dwa hasła (PIN1 & 2 i PUK)
- numer seryjny (ICCID)
- dane sesji (np. LAI - location area identity)
- dane użytkownika (np. książka telefoniczna)

K_i

- Jest to 128bitowa wartość używana w autoryzacji w sieciach GSM. K_i jest przechowywane również poprzez operatora sieci w jego wewnętrznych systemach. Jest to zastosowanie PSK (pre shared key) gdzie klucz jest dostarczany przez inne medium do drugiego urządzenia.
- Karta SIM utrzymuje ten klucz fizycznie bezpieczny poprzez udostępnienie jedynie funkcji która otrzymuje dane od urządzenia i zwraca odpowiednio podpisany wynik

IMSI

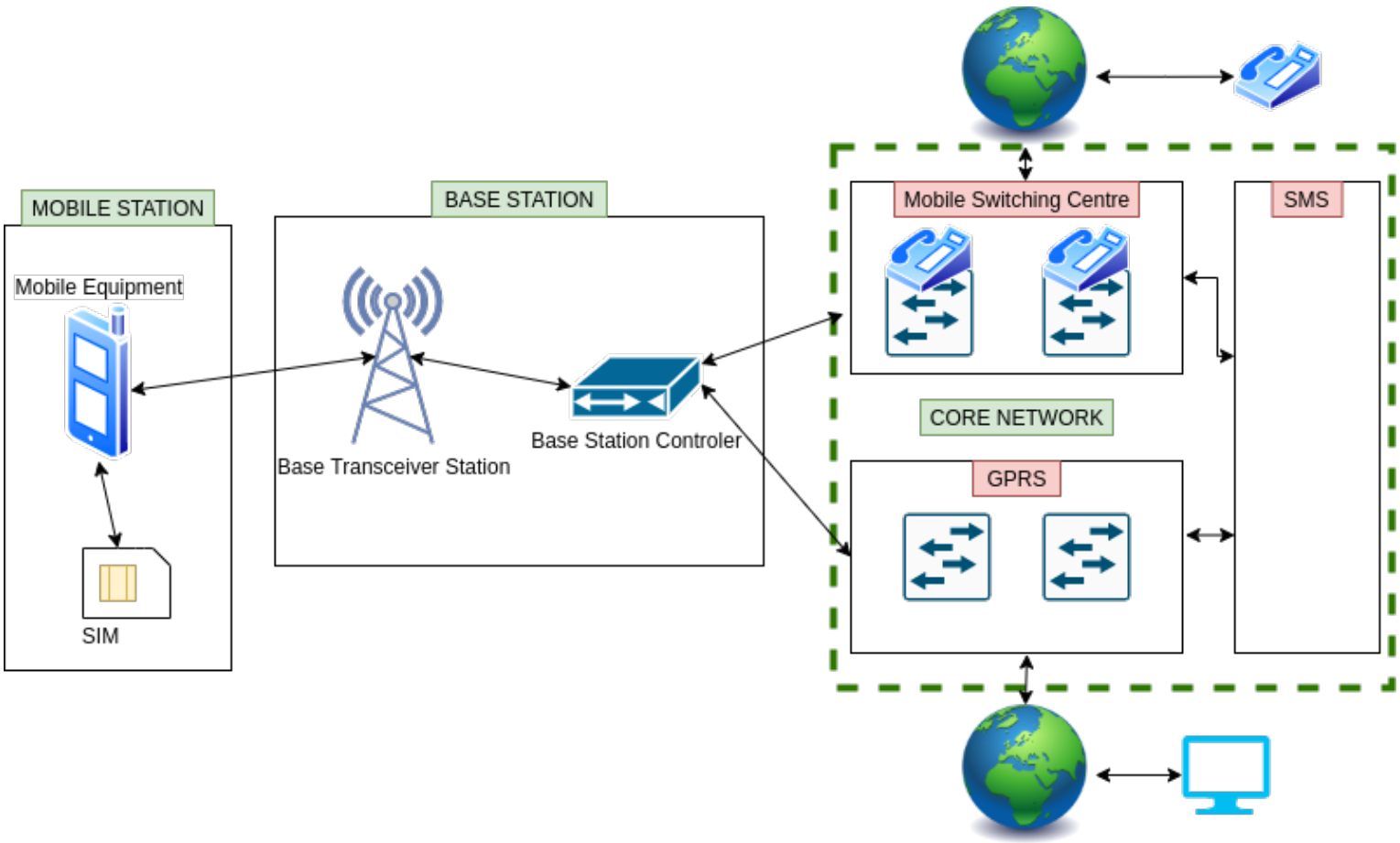
Jest to numer jednoznacznie identyfikujący urządzenie sieci komórkowej. Jest to wartość 64bitowa i używana jest do rejestracji oraz otrzymania danych od stacji. Aby uniknąć łatwego śledzenia użytkownika ten numer jest rzadko przesyłany a generowany jest tymczasowy numer.

Rozwiązanie problemów z GSM

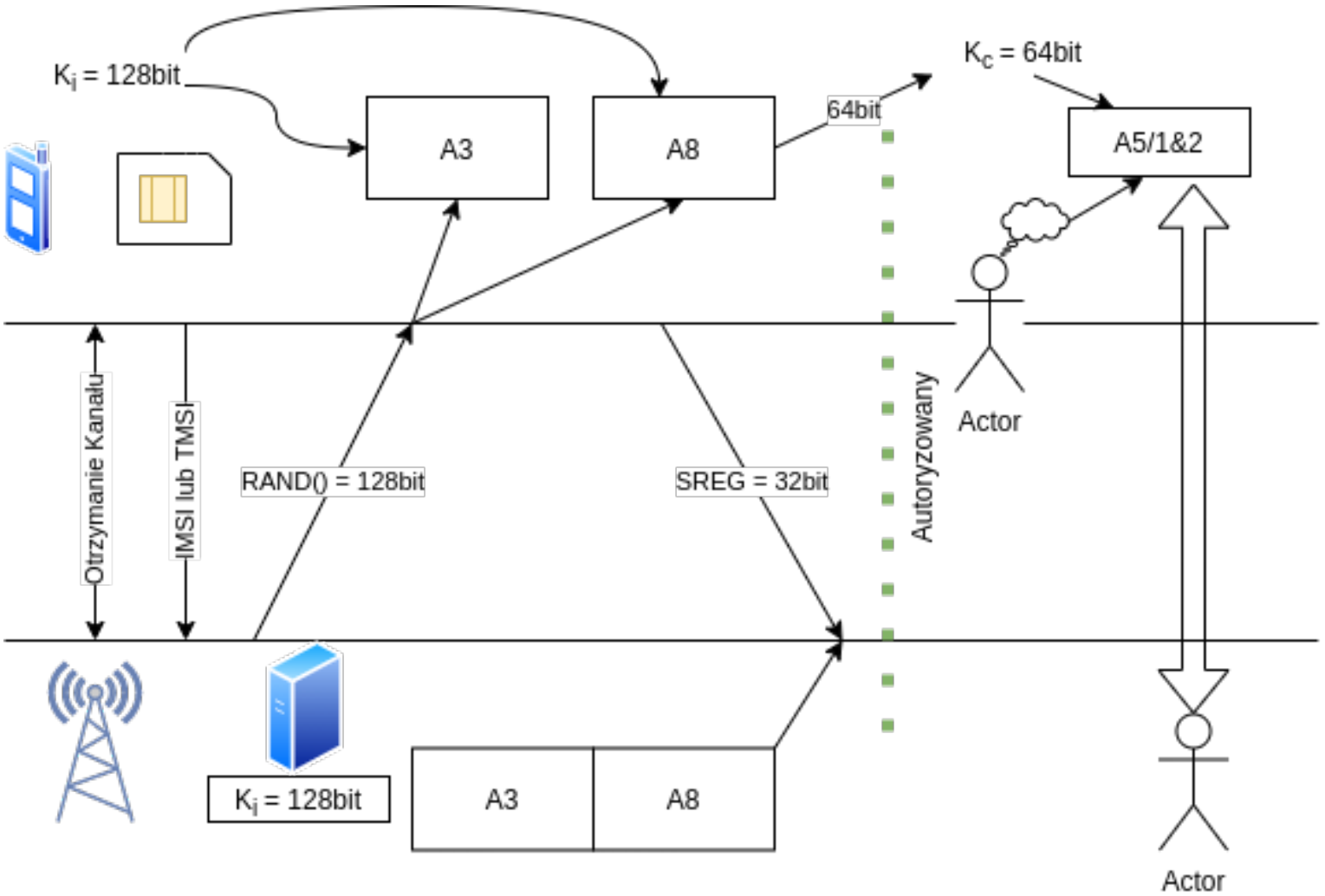
GSM

Global System for Mobile Comunications jest to standard drugiej generacji (2G) cyfrowych sieci komórkowych. Jest to sieć Point-to-Point, Circuit Switched, full duplex. Standard został poźniej rozszerzony poprzez dodanie możliwości wysyłania danych pakietowych (GPRS, EDGE)

Schemat


MOBILE STATION
Mobile Equipment
SIM
BASE STATION
Base Transceiver Station
Base Station Controler
Mobile Switching Centre
SMS
CORE NETWORK
GPRS

Challange-response



Szyfry w GSM

A3/A8

A3/A8 nie jest ścisle określony w standardzie, jednak w praktyce wiekszość operatów zdecydowała sie na użycie tajnego COMP128 zaprojektówanego przez stowarzyszenie GSM.

A5

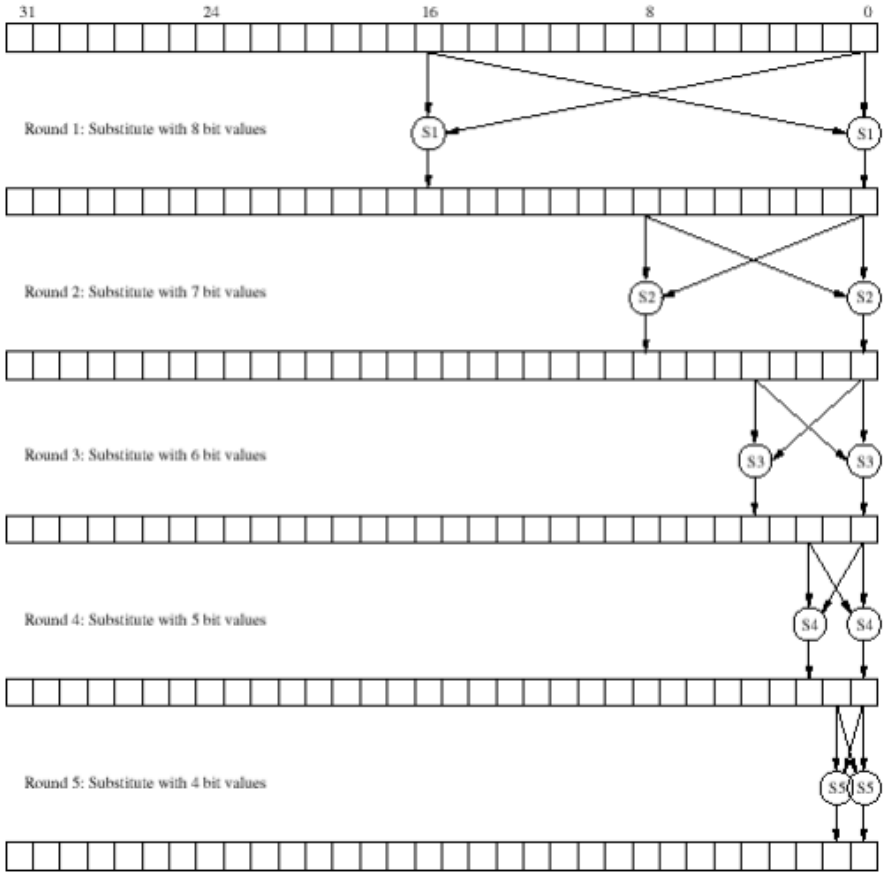
A5/1&2&3 są szyfrem strumieniowym. Używanym by zapewnić prywatność w standardzie GSM

Szyfry w GSM (kont.)

COMP128

```
x[16-31] = RAND;
for(i=1;i<8;i++)
  x[0-15] = Ki;
  Compression();
  FormBitsFromBytes();
  if (i<7)
    Permute();
```

Szyfry w GSM (kont.)



Security by obscurity

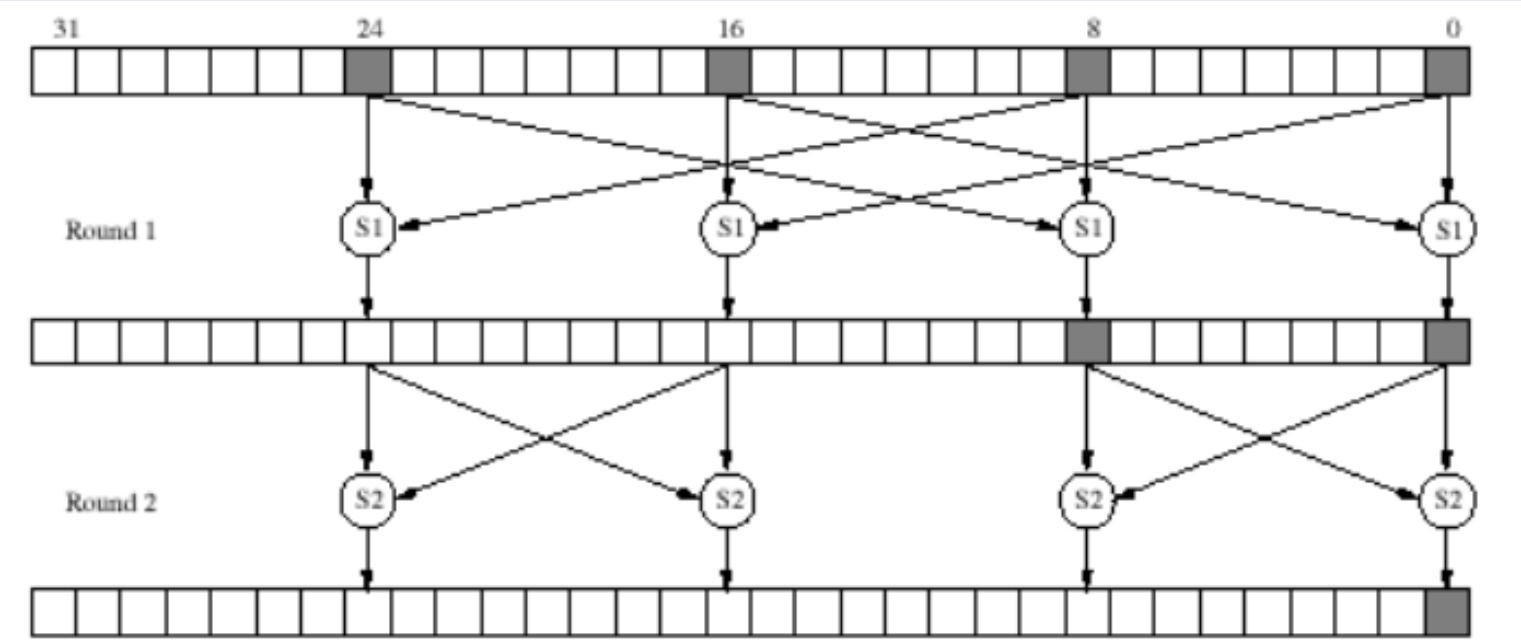
- GSM jest jednym z najlepszych przykładów dlaczego nie należy chronić sekretów poprzez zamknięciem systemów. Mimo braku dokumentacji A5 został odkryty za pomoca inżynieri wstecznej oraz wykradniętych tajnych dokumentów. Szybko zostały zidentyfikowane problemy które prawdopodobnie byłyby zauważone dużo wcześniej.
- Sam GSM został złamany najpierw przez ataki na protokół GSM, zmuszając urządzenie do użycia specjalnie słabszej wersji szyfru A5/2

Problemy GSM

Sieć w żaden sposób nie autoryzuje się urządzeniu

Częste implementacje szyfru są wadliwe (COMP128)

Narrow pipe



Problemy GSM (kont.)

- Dzięki temu problemowi możemy za pomocą wysłania dużej ilości challenge'ów do karty zmieniając tylko bajt i i i+8
- Możemy oczekiwać kolizji po $2^{(4*7/2)} = 2^{14}$ wezwaniach
- Po znalezieniu kolizji mozemy poprostu to samo powtórzyć dla kolejnych par bajtów

Brute force K_i

```
for(i=0; i<256; i++)
  for(j=0; j<256; j++)
    key[0]=i; key[8]=j;
    A3A8(chal1,key,hash1);
    A3A8(chal2,key,hash2);
    if(hash1=hash2) //znaleziony hash
```

Problemy GSM (kont.)

- jeżeli sieć nie ma TMSI użytkownika to musi wysłać zapytanie o IMSI poprzez otwarte połączenie
- atakujący może oczywiście użyc tej samej mechaniki do uzyskania IMSI od użytkownika
- Szyfrowanie następuje po korekcji błędów więc znając algorytm korekcji błedów można zmiejszyć entropie szyfrowanego strumienia

Rozwiązanie problemów z GSM

GSM

Został dodany nowy standard szyfrowania bazujący na szyfrze używanym do 3G (UTMS)

A5/3

KASUMI jest to szyfr blokowy zaprojektowany przez Mitsubishi wykorzystywany do generowania kluczy pośrednich do szyfra strumieniowego A5/3

GPRS

- FEC jest wykonywany na wyższym poziomie w modelu warstwowym (LLC)
- Podobnie do A5/3 został dodany nowy algorytm szyfrujący bazujący na Kasumi

GEA3

KASUMI jest to szyfr blokowy zaprojektowany przez Mitsubishi wykorzystywany do generowania kluczy pośrednich do szyfra strumieniowego GEA3

UTMS

- Nowa możliwość
- Zmodyfikowana procedura autoryzacji
  - Stacja bazowa wysyła oprócz RAND() także AUTN który jest generowany z K_{root} oraz RAND
  - telefon może w takim wypadku sprawdzić czy stacja bazowa jest prawdziwa !!!

Rozwiązanie problemów z GSM

Podsumowanie

- Autoryzacja
- Integralność
- Poufność
- Bezpieczeństwo urządzenia

Podsumowanie

- Sieć GSM była projektowana z bezpieczeństwem. Widać jednak że problemy natury politcznej (A5/2) oraz nacisku na sekretność w specifikacji standardu (COMP128) a nawet specjalnemu obniżaniu bezpieczeństwa (K_c 64->54bity) bezpieczeństwo zostało zdecydowanie obniżone
- Opinia społeczności zarówno akademickiej jak i hobbystycznej mogła by wykryć wiele wad w publicznych specyfikacjach i naprawić większość błedów zanim standard trafi do krzemu lub oprogramowania konsumenckiego
- W czasach ograniczonej mocy obliczeniowej (<2005), można by było nawet postawić hipoteze, że zostało to zrobione specjalnie aby umożliwić aktorom światowym (Rządy & Wojsko) złamać to bezpieczeństwo w celu "wyższych środków".

Bibliografia

- Study and Implementation of 3G Mobile Security, Sutirtha Prakash, Sachikanta Behera
  - https://core.ac.uk/download/pdf/53187397.pdf
- Security In Wireless Cellular Networks, National Institute of Technology Rourkel, Ali I. Gardezi
  - https://www.cse.wustl.edu/~jain/cse574-06/ftp/cellular_security/
- A3/A8 & COMP128, Helsinki University of Technology, Billy Brumley
  - http://www.tcs.hut.fi/Studies/T-79.514/slides/S5.Brumley-comp128.pdf

Bibliografia (kont.)

- Security in the GSM system, Jeremy Quirke
  - https://web.archive.org/web/20040712061808/http://www.ausmobile.com/downloads/technical/Security%20in%20the%20GSM%20system%2001052004.pdf
- Rooting SIM cards, Black Hat 2013, Karsten Nohl
  - https://www.youtube.com/watch?v=scArc93XXWw
- OsmocomBB: Open Source GSM Implementation, Fabian Faessler
  - https://www.youtube.com/watch?v=0i7wOfyJsW8
- How do SIM Cards work? - SIMtrace, Fabian Faessler
  - https://www.youtube.com/watch?v=iJFnYBJJiuQ