Sieci GSM - działanie i systemy zabezpieczeń

Seminarium z kryptologii i ochrony informacji

Łukasz Kucharzewski
Politechnika Warszawska 2009

Historia

Groupe Spécial Mobile
Global System for Mobile Communications

1988

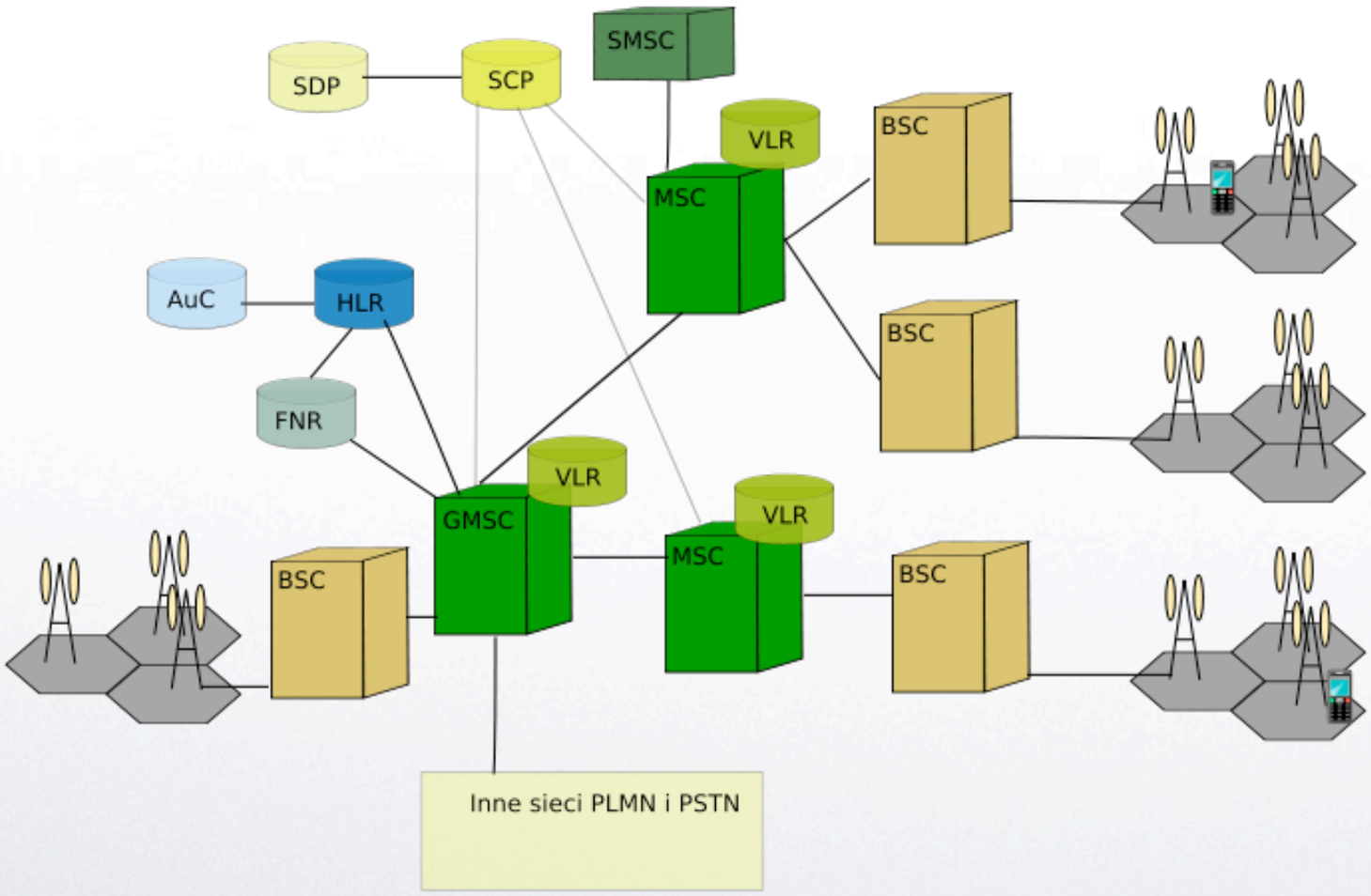
Telefonia analogowa
Wybór pasma
Pierwszy system testowy 1991

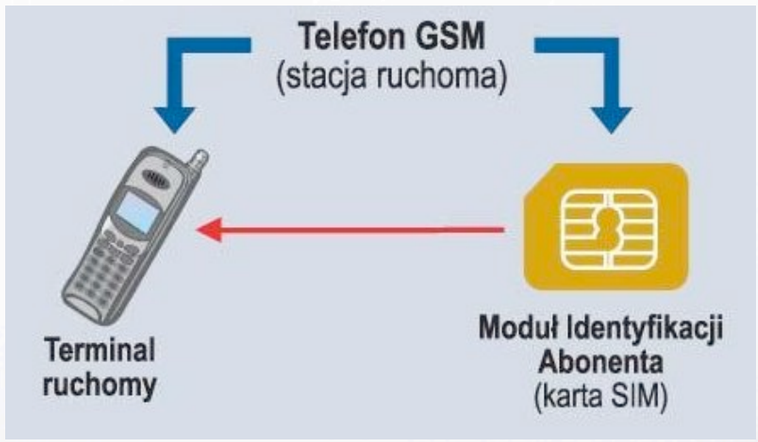
Standardy GSM

System	GSM 400	GSM 850	GSM 900	GSM 1800	GSM 1900
Uplink [MHz]	450.4 - 457.6 or 478.8 - 486	824 - 849	880 - 915	1710 - 1785	1850 - 1910
Downlink [MHz]	460.4 - 467.6 or 488.8 - 496	869 - 894	925 - 960	1805 - 1880	1930 - 1990
Liczba częstotliwości	35	124	174	374	299

GSM coverage

Architektura





Architektura

BSS (sng.Base Station System)

BTS (ang.Base Transceiver Station)- element sieci, który jest intefejsem pomiędzy telefonem komórkowym a siecią GSM. Dzięki antenom, transmituje i odbiera na kilku czętotliwościach zakodowany cyfrowo sygnał.

BSC (ang.Base Station Controler)- zarządza stacjami bazowymi, odpowiada za transmisję pomiędzy stacjami bazowymi a resztą sieci. Kilka BSC jest podłączona do MSC

MSC (ang. Mobile Switching Centre) jest cyfrową centralą telefoniczną pracującą w sieci GSM. Odpowiada za zestawianie połączeń i koordynuje współpracę pomiędzy elementami sieci.

GMS (ang. Gateway Mobile Switching)- specjalna MSC, która kontaktuje się z HLR. Niektóre GMS pracują jako centrale tranzytowe do innych sieci.

Architektura

HLR (ang. Home Location Register)-rejestr stacji własnych. Jest to baza danych, która przechowuje informacje o abonentach, którzy należą do danej sieci.

AuC (ang. Authentication Centre)- element sieciowy odpowiedzialny za bezpieczeństwo użytkowników. Przechowuje dane abonentów danej sieci, na bazie których dokonuje uwierzytelnienia numeru IMSI.

VLR (ang. Visitor Location Register)- rejestr abonentów przyjezdnych. Jest to baza danych, zwierająca informacje o abonentach, którzy w danym momencie znajdują się na obszarze obsługiwanym przez dane MSC.

FNR (ang. Flexible Number Register)-element opcjonlany w strukturze sieci. Związany z usługą przenoszenia MSISDN pomiędzy operatorami. Jest to baza danych zawierająca informacje o wszsytkich abonentach GSM w danym kraju.

Architektura

SMSC (SMS Center)- element odpowiedzialany za przesyłanie krótkich wiadomości tekstowych

SCP (ang. Service Control Point)-element sieci na którym oparte są sieci inteligentne

SDP (ang. Service Data Point)- baza danych zawierająca informacje o abonentach wykorzystywane przez programy działające na platformie SCP

Jak to działa?

Alicja → Bob

Wyszukiwanie: Telefon(A) → BTS(A) → BSC(A) → MSC(A)
→ HLR(B) → MSC-VLR(B) → BSC(B)
→ BTS(B) → Telefon(B)

Rozmowa: Telefon(A) → BTS(A) → BSC(A) → MSC(A)
→ MSC(B) → BSC(B) → BTS(B) → Telefon(B)

Call Data Record

A3/A5/A8

A3- algorytm odpowiedzialny za autentykację użytkownika.
A5-szyfrowanie wiadomości (stały element w postaci szyfru strumieniowego, 3-liniowe rejestry, przesuwane sprzężeniem zwrotnym)
A8- generowanie klucza

AuC dokonuje weryfikacji ważności kart SIM za pomocą algorytmu szyfrującego A3, znajdującego się na karcie SIM i w bazie danych AuC. Proces ten polega na sprawdzaniu klucza uwierzytelniania (KI), liczby pseudolosowej (RND), która przesyłana jest do stacji ruchomej za pomocą styku Um. Po przetworzeniu liczby RND, następuje proces komunikacji z kartą SIM. Klucz uwierzytelniania szyfruje algorytmem A3 liczbę losową, generując dane wyjściowe w postaci 32-bitowej sekwencji SRES (ang. Signed Respond). Sekwencja ta przesyłana jest do AuC i porównywana z matematyką obliczeniową Centrum AuC. Uzyskanie zgodności sekwencyjnej zatwierdza proces autoryzacji.

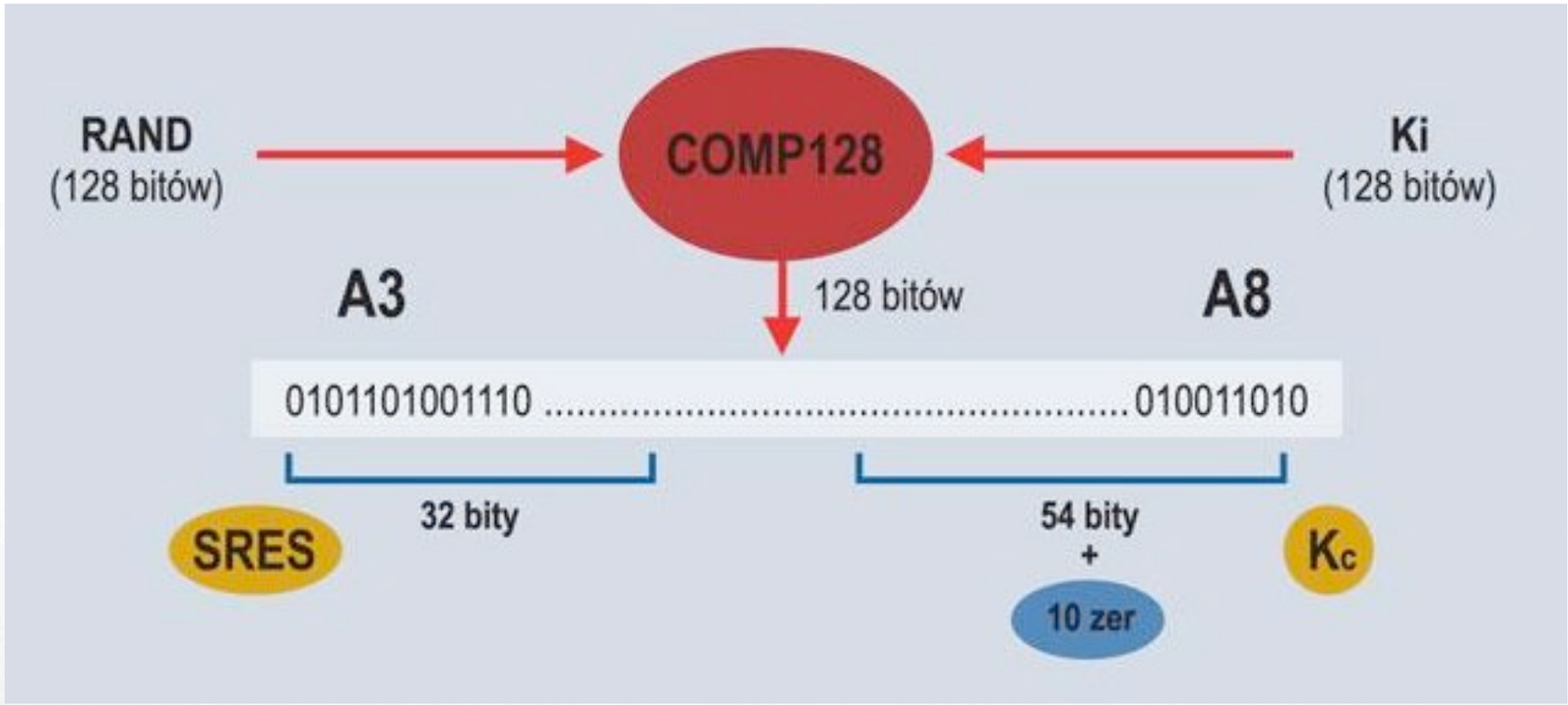
A5

A5/0 - najsłabsza „wersja” algorytmu, polegająca na transmisji wszystkich danych tekstem otwartym (bez szyfrowania)
A5/2 - słabsza wersja algorytmu, zbudowana przy użyciu czterech rejestrów typu LFSR
A5/1 - silniejsza wersja algorytmu, zbudowana przy użyciu trzech rejestrów typu LFSR
A5/3 – najsilniejsza wersja algorytmu; zbudowana jest na bazie algorytmu Kasumi, używana w UMTS

A5 break

Siła algorytmu bezpieczeństwa określona jest przez jego tzw. złożoność czasową (ilość wszystkich możliwych kombinacji, mającą wpływ na czas ich przetestowania). Złożoność czasowa zależy w sposób wykładniczy od długości bitowej właściwych kluczy, stanowiących parametry wejściowe algorytmu. Dla standardowej długości klucza szyfrującego w GSM (64 bity) jest ona rzędu 264. Jednak biorąc pod uwagę fakt, że klucz Kc produkowany przez algorytm COMP128 ma długość realną tylko 54 bity (por. ramka na str. 28), rzeczywista złożoność czasowa obniża się już "na dzień dobry" do wartości 254 (około tysiąc razy mniejszej!)

COMP 128



Odpowiedź autentykacyjna (128 bitów) wytwarzana w tym samym przebiegu; klucz **Kc** 54 bitowy + 8 zerowych bitów dodawanych do **Kc** i podawany dalej do **A5**

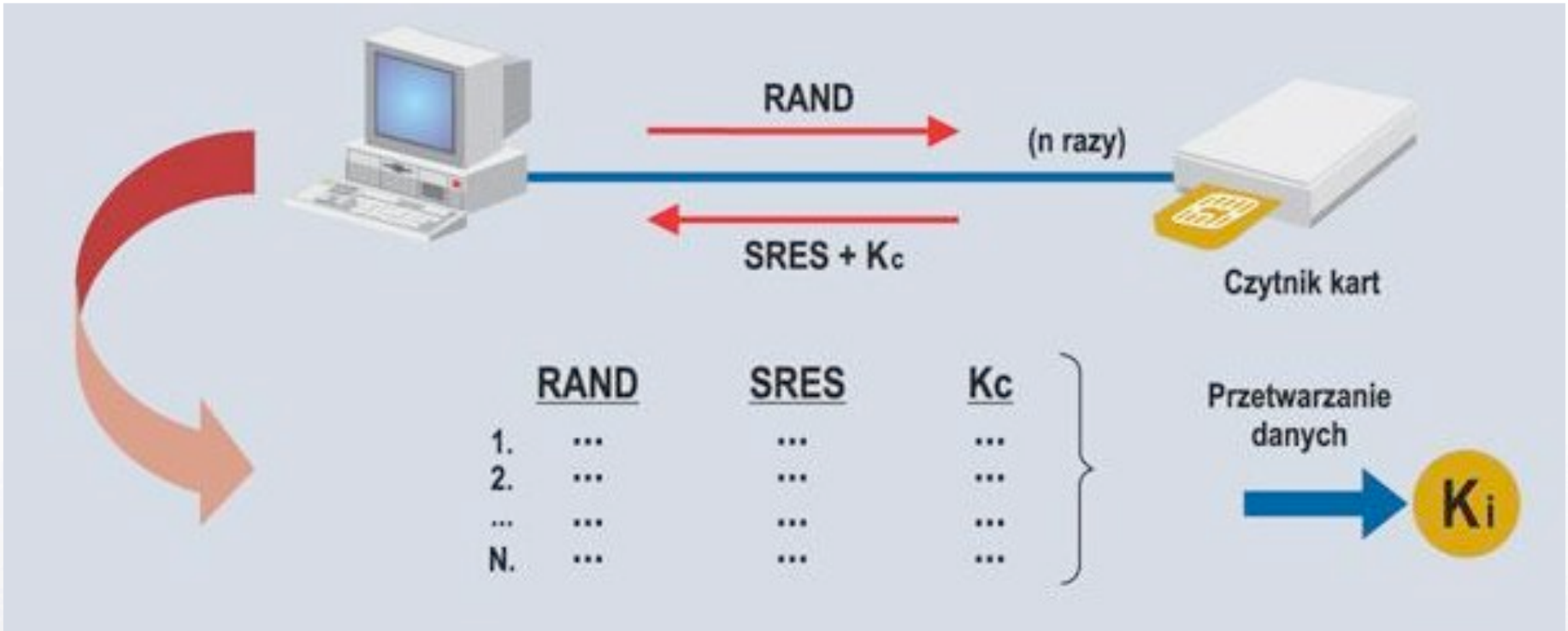
COMP 128 break

Pierwszy atak na algorytm COMP128-1 opracował Marc Briceno, David Wagner i Ian Goldberg w kwietniu 1998 roku w ciągu zaledwie kilku godzin od poznania jego kodu. Świadczy to o wyjątkowo kiepskiej jakości tego algorytmu.

W maju 2002 r. naukowcy z koncernu IBM odkryli nowy sposób uzyskania klucza Ki, przy zastosowaniu ataku poprzez tzw. **kanały boczne** (obserwację emisji ujawniających, zużycia mocy, przebiegów czasowych oraz błędów w trakcie przeprowadzanych w karcie SIM obliczeń).

Metoda ta umożliwia odtworzenie klucza przy użyciu jedynie 1000 przypadkowo wybranych wartości parametru RAND

Klonowanie SIM



Słaby punkt algorytmu **COMP128** wynika z wady polegającej na ujawnieniu klucza **Ki** jako argumentu wejściowego **RAND**. Przy n zapytaniach autentykacyjnych, można metodami analizy kryptograficznej wyliczyć klucz **Ki**.

Podsłuch Real-Time

Ataki „man in the middle”

Posłużyć do tego może tzw. **IMSI catcher** - urządzenie diagnostyczne, służące do symulowania stacji bazowej przy testowaniu telefonów komórkowych. IMSI catcher (użyty przez włamywacza) może udawać przed telefonem stację bazową, a przed inną stacją bazową może udawać telefon (ponownie pojawia się tutaj problem braku autentykacji stacji bazowej przez telefon).

Za pomocą tego urządzenia możliwe jest wyłączenie szyfrowania (poprzez ustanowienie wersji A5/0) i zastosowanie pasywnego podsłuchiwania rozmów

Podsumowanie

Czy sieci komórkowe są bezpieczne?

Odpowiedź na to pytanie zależy od tego, który z wielowymiarowych aspektów bezpieczeństwa mamy na uwadze. Poziom bezpieczeństwa jest często wynikiem kompromisu pomiędzy wygodą użytkownika, kosztem zabezpieczeń, ich zaawansowaniem technologicznym oraz funkcjonującymi regulacjami prawnym

Dziękuję

Literatura

1. "GSM – Kto może mnie podsłuchać", Haking9 nr 1/2004, Reinhard Wobst
2. "GSM and Personal Communications Handbook", Siegmund M. Redl, Matthias K. Weber, 1998
3. "Designing a Wireless Network", Jeffrey Wheat, Randy Hiser, Jackie Tucker, 2001
4. "Porównanie bezpieczeństwa systemów GSM i UMTS", Krzysztof Liszewski, dyplomowa praca inżynierska, Politechnika Warszawska, 2007
5. http://paweljablonski.bblog.pl
6. http://www.idg.pl/artykuly/54685/Bezpieczenstwo.telefonii.komorkowej.2.Ataki.na.system.GSM.html
7. www.wikipedia.pl