MARIUSZ GIBKI

Podsłuch GSM

Stopień trudności

Nowe technologie, mobilność i bezpieczeństwo, czy prywatność nadal jest tylko nasza ? Czy zabezpieczenia komunikacji mobilnej stosowanej w technologii GSM są na wystarczającym poziomie? Zapraszam do zapoznania się z kilkoma informacjami na ten temat.

Właśnie stałeś się posiadaczem nowego, pięknego urządzenia, które od teraz, w dowolnej chwili połączy Cię ze światem i z kim tylko zechcesz. Otworzy przed Tobą nieograniczone możliwości i da poczucie mobilności. Twoi znajomi mogą zawsze z Tobą porozmawiać, zostawić Ci wiadomość sms lub pokazać zdjęcie z podróży.

Czasy, gdy mobilna komunikacja była wyznacznikiem statusu i zamożności, dawno już minęły, a ceny tej technologii sprawiają, iż jest ona dostępna dla wszystkich i wykorzystywana zarówno w celach biznesowych, jak i towarzyskich.

Nigdy nie rozstajesz się ze swoim telefonem, masz w nim ulubione utwory muzyczne, nieco zdjęć i filmów oraz kilka innych plików. Być może zapisałeś sobie w notatniku kilka prywatnych informacji, które są dostępne tylko dla Ciebie i masz do nich wgląd zawsze, kiedy tego potrzebujesz. Zastanawiałeś się jednak kiedyś, czy Twoje dane są bezpieczne? Czy wysłana wiadomość trafia tylko do adresata? Czy gdy rozmawiasz, Twoją rozmowę słyszy tylko odbiorca? Co z połączeniami internetowymi, obecne telefony obsługujące GPRS czy HSDPA, bezproblemowo radzą sobie z siecią internetową. Czy tą drogą również można wykraść Twoje prywatne dane? Czy podczas rozmowy słyszysz tajemnicze szmery i trzaski w Twojej słuchawce? Być może, ktoś słyszy to co mówisz, być może ktoś odczytuje Twoje smsy i teraz przegląda Twoją książkę numerów. Właśnie przypomniałeś sobie, że zapisałeś w pamięci telefonu ważne informacje dotyczące Ciebie lub Twojego konta bankowego. Być może zapisałeś tam PIN do karty... a teraz zastanawiasz się, czy to faktycznie bezpieczne i czy Twoja prywatność nadal jest tylko Twoja?

Technologia GSM informacje teoretyczne

GSM (ang. *Global System for Mobile Communications)* to najpopularniejszy na chwilę obecną standard telefonii komórkowej. Sieć oparta o tę technologię umożliwia przesyłanie głosu, danych oraz wiadomości tekstowych i multimedialnych. Powstanie technologii GSM zainicjowane zostało potrzebą stworzenia jednego, otwartego standardu telefonii komórkowej na terenie Europy. Początkowo standard ten miał objąć 12 członków EWG (Europejskiej Wspólnoty Gospodarczej) i jednego spoza tej organizacji. W 1982 roku wewnątrz Europejskiej Konferencji Administracji Poczty i Telekomunikacji powołano instytut *Grupe Spécial Mobile* (GSM), którego zadaniem było opracowanie standardu telefonii komórkowej, funkcjonującej w paśmie 900MHz. Pasmo to zarezerwowano we

Z ARTYKUŁU DOWIESZ SIĘ

o historii, technologii GSM, stosowanych algorytmach bezpieczeństwa, i istniejących sposobach ich łamania.

CO POWINIENEŚ WIEDZIEĆ

znać podstawy technologii GSM i stosowanych w niej algorytów.

wszystkich krajach członkowskich, w celu zapewnienia międzynarodowego roamingu. Powstały prototypy urządzeń radiowych oraz przeprowadzono testy dotyczące optymalnego sposobu dostępu do sieci, których wyniki stały się podwaliną tworzonej specyfikacji. Projekt wspólnego standardu zatwierdzony został przez Komisję Europejską w 1984, a 3 lata później 7 września 1987 r. w *Memorandum of Understanding* grupa 15 operatorów zobowiązała się do wdrożenia i uruchomienia technologii GSM. Oficjalna specyfikacja została opublikowana w 1988 r. i nosiła nazwę GSM 900 Phase 1. Akronim GSM zmienił znaczenie na *Global System for Mobile Communications*. Później, w 1989 roku, powstał Europejski Instytut Norm Telekomunikacyjnych (ETSI) i przejął wszystkie prace dotyczące rozwoju standardu GSM. W 1990 rozpoczęto pracę definiującą standard nadający w paśmie 1800 MHz (*Digital Communication System).*

Pierwsza komercyjna sieć, pracująca w architekturze GSM 900 Mhz, powstała w Finlandii w 1992. Rok później uruchomiona została druga sieć w Wielkiej Brytanii. Poza Europą wprowadzanie technologii GSM rozpoczęła również Telstra w Australii. Pierwsze sieci w swojej ofercie umożliwiały tylko transmitowanie głosu, dopiero w 1994 r. dodano transmisję danych. Druga specyfikacja ukazała się w roku 1995, pod nazwą GSM Phase 2+, uwzględniała ona model transmisji, w którym można odbierać dane z maksymalną prędkością 57,6 kb/s, a nadawać z prędkością 14,4 kb/s. Mowa tu oczywiście o technologii HSCSD (ang. *High Speed Circuit Switched Data*). W specyfikacji tej uwzględniono również technologię CAMEL, dzięki której abonenci będący w roamingu mogą korzystać z usług udostępnianych w ich macierzystej sieci przy wykorzystaniu sieci inteligentnych. Dalej w roku 1997 do specyfikacji dołączona zostaje technologia GPRS, a w tym samym czasie GSM rozpowszechnia się poza granicami Europy. W Stanach Zjednoczonych, z powodu zajętego pasma 1800MHz, powstaje GSM 1900MHz, gdzie zastosowano również model kodowania mowy zwany *Adaptive Multi Rate*. W związku z tym, iż standard stawał się coraz bardziej popularny powołano *3rd Generation Partnership Project* (3GPP),

Listing 1. *Kod przedstawiający prace algorytmu COMP128*

```
VOID A3A8 (wejście RAND[16], Ki[16],
           wyjście SIMoutput[12])-operują na bajtach
 {
          x[32]-[[bufor (programowanie)|bufor]] wewnętrzny-operuje na bajtach,
                    bit[128]-bufor roboczy;
          T[5][]-bloki podstawieniowe zapisane w tablicy (512, 256, 128, 64, 32
                    bajtów);
          pozostałe zmienne i, j, k, l, m, n, y, z, następny_bit;

          zapisanie RAND na ostatnich 16 bajtach bufora (x[16...31])
          for i=16 to 31{
              x[i]=RAND[i]
          }
          wykonanie pętli 8 razy
          for i=1 to 8{
              zapisanie Ki na pierwszych 16 bajtach bufora (x[0...15])
              for j=0 to 15{
              x[j]=Ki[j]
              }
              kompresja (tzw. [[kompresja motyla]], czyli jedna z głównych słabości
                        algorytmu COMP128)
              for j=0 to 4{
                  for k=0 to (2^j)-1{
                      for l=0 to 2(^4-j)-1{
                          m=1+k2^(5-j)
                          n=m+2^(4-j)
                          y=(x[m]+2x[n])mod 2^(9-j);
                          z=(2x[m]+x[n])mod 2^(9-j);
                          x[m]=T[j][y];
                          x[n]=T[j][z];
                      }
                  }
              }
              "Form bits From bytes" czyli przestawienie bitów w buforze
               for j=0 to 31{
                   for k=0 to 3{
                       bit[4j+k]=(x[j]>>(3-k))&1
                   }
               }
               [[permutacja]] z pominięciem ostatniej pętli
               if i<8{
                  for j=0 to 15{
                      for k=0 to 7{
                          następny_bit=17(8j+k)mod 128
                          k-ty bit x[j+16]=bit[następny_bit]
                      }
                  }
              }
          }
          [[Kompresja (informatyka)|kompresja]] 16 bajtów wynikowych do 12
                    bajtów oraz zapisanie
          ich w SIMoutput[] (x[0...3]-SRES; x[4...11]-Kc);
          wyzerowanie ostatnich 10 bitów klucza Kc
          for i=0 to 3
              SIMoutput[i]=(x[2i]<<4)|x[2i+1]
          for i=0 to 5
              SIMoutput[4+i]=(x[2i+18]<<6|(x[2i+18+1]<<2)|(x[2i+18+2]>>2)
          SIMoutput[4+6]=(x[26+18]<<6)|(x[26+18+1]<<2)
          SIMoutput[4+7]=0
 }
```

w którego skład weszło wiele instytutów standaryzacyjnych spoza Europy. Dalszy rozwój standardu zaowocował technologią EDGE (ang. *Enhanced Data for GSM Evolution*) służącą do przesyłania danych, w której uzyskano trzykrotne polepszenie przepływności danych (teoretycznie do 236,8 kbit/s).

Od maja 2009 odnotowano 3 mld unikatowych numerów abonenckich telefonii GSM.

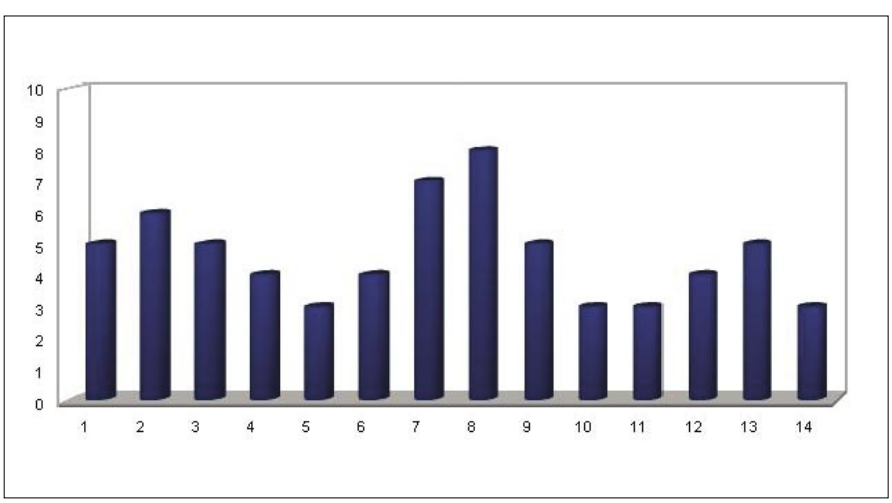
Transmisja głosowa i metody kodowania

W celu transmitowania głosu, przy użyciu technologii GSM, kontroler stacji bazowych BSC (ang. *Base Station Controller*), pełniący kontrole nad wieloma stacjami bazowymi BTS (ang. *Base Transceiver Station*), przydziela odpowiedni cyfrowy kanał radiowy dla danego telefonu na dany czas połączenia. Rozmowy mogą być transmitowane przez 8 szczelin czasowych (ang. *time slot*) dla każdej dostępnej częstotliwości. Zależnie od obciążenia danej sieci oraz użytej metody kodowania dla połączenia może zostać przydzielona cała lub częściowa szczelina czasowa (co oczywiście ma wpływ na jakość prowadzonej rozmowy). Decyzje o użytej metodzie kodowania ustalane są przez kontrolera stacji bazowej, na podstawie przesyłanych przez nadajnik (aparat telefoniczny) raportów pomiarowych (ang. *measurement reports*), zawierających informacje o jakości i sile sygnału, jaki jest odbierany ze znajdujących się w pobliżu stacji bazowych. Po nawiązaniu połączenia i ustaleniu jego parametrów, dźwięk z postaci analogowej zostaje poddany konwersji na postać cyfrową. Pierwszym etapem konwersji jest próbkowanie, inaczej dyskretyzacja lub kwantowanie w czasie, polegające na stworzeniu sygnału impulsowego z pierwotnego sygnału ciągłego. Próbkowanie idealne reprezentowane jest przez iloczyn funkcji grzebieniowej (niekończony ciąg impulsów Diraca, położonych w równych odstępach czasu) i sygnału ciągłego.

Technicznie nie realizuje się generowania impulsów Diraca, a funkcję impulsową przybliża się sygnałem prostokątnym o bardzo małym wypełnieniu. W praktyce realizowane jest to w taki sposób, iż w danych odstępach czasu zmierzona zostaje wartość jaką w danej chwili przyjmuje sygnał i na tej podstawie utworzone zostają tak zwane próbki. Sygnał zapisany w postaci próbek nosi nazwę sygnału dyskretnego (ciąg zbudowany z serii próbek – ang. *sampli*).

Następnym krokiem jest proces kwantowania, w którym każdej próbce przypisywana jest odpowiednia wartość liczbowa. Amplituda sygnału mierzonego w czasie próbkowania jest dzielona na 8192 odcinki i każda próbka znajdująca się w danym odcinku ma przyporządkowaną liczbę z zakresu (0 – 8192). Kolejnym krokiem jest kodowanie liczb uzyskanych w procesie kwantyzacji i ich zero-jedynkowy zapis, w postaci 13-bitowej (2^13 = 8192). Przesłanie danych w tak uzyskanym formacie wymagałoby szybkości 104 kb/s, jednak wartość taka jest nie do zaakceptowania, dlatego zastosowano uproszczenie, polegające na podzieleniu uzyskanego sygnału na 20 ms odcinki, kompresowane na sygnał 260-bitowy, nadający się do uzyskania wystarczającej jakości opisu dźwięków ludzkiej mowy, co przekłada się na wymaganą szybkość przesyłu 13 kb/s. Sposób kodowania 20 ms odcinków jest realizowany przy pomocy algorytmu:

- 260 bitów (odpowiednik 20 ms) dzielony jest na trzy części :
  - 50 najważniejszych bitów,
  - 132 ważnych bitów,
  - 78 bitów o mniejszym znaczeniu.



Rysunek 1. *Funkcja grzebieniowa*

Tabela 1. *Rozmieszczenie punktów sygnału zwrotnego w rejestrach*

Rejestr	Rozmieszczenie punktów sygnału zwrotnego	Okres sekwencji pseudolosowej
R1	13;16;17;18	(2^19)-1
R2	20;21	(2^22)-1
R3	7;20;21;22	(2^23)-1

Tabela 2. *Taktowanie w rejestrach*

Rejestr	Punkt startowy	Pozycja Startowa
R1	C1	8
R2	C2	10
R3	C3	10

- W bloku najważniejszych 50 bitów dodane zostają 3 bity parzystości, mające zastosowanie przy korekcji błędów, dając w sumie 53 bity.
- Część pierwsza i druga sumuje się co daje 53 bity + 132 bity oraz dodawane są 4 bity jako uzupełnienie, dając w sumie 189 bitów.
- Blok 189 bitów zostaje zdublowany dając wartość 378 bitów.
- Ostatnim krokiem jest uzupełnienie całości o bity mniejszego znaczenia, otrzymując w ten sposób segment danych o wartości 456 bitów.

Stosując nadmiarowość i bity parzystości możliwe będzie korekcja błędów po otrzymaniu takiego sygnału. Może zdarzyć się również i tak, że podczas przesyłania sygnału rozmowy, fragment sygnału w wyniku zakłóceń zostanie zgubiony i nie przesłany do adresata. By zachować spójność rozmowy stosuje się tzw. przeplot, w którym bity z zakodowanej rozmowy zostają przeplatane pomiędzy sobą w taki sposób, by ewentualne utracone fragmenty powodowały co najwyżej spadek jakości rozmowy bez utraty sensu przekazu. Przeplot w pierwszym etapie zwanym *przeplotem bitowym* tworzony jest procedurą *channel coding*, polegającą na podziale 456 bitów (odpowiednik 20 ms rozmowy) na 8 części po 57 bitów.

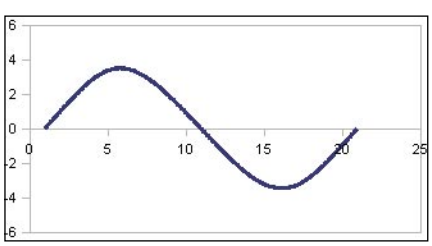
Jedna ramka wysyłana w jednej szczelinie czasowej zawiera 2 przedstawione na Rysunku bloki, w momencie utraty całej przesyłanej ranki BRE (ang. *Bit error ratio* – współczynnik błędnych bitów) wynosi 25%. Kolejnym krokiem jest przeplot blokowy, pozwalający uzyskać jeszcze mniejszy współczynnik błędu BRE. Etap polega na wysyłaniu w jednej ramce 2 bloków, ale z różnych segmentów, zawierających inne odpowiedniki 20 ms fragmentów rozmowy. W takim układzie, w momencie utracenia transmitowanej ramki, zaginie tylko jeden blok z 20 ms fragmentu rozmowy, co daje BRE 25%/2 12,5%. W związku z zastosowaniem przeplotu blokowego powstaje nieznaczne opóźnienie w systemie, jednak korzyść wynikająca z 50% zmniejszeniem możliwości występowania błędów, przemawia za wykorzystywaniem tego rozwiązania.

Następnym krokiem jest zakodowanie ramki, tak by była ona możliwa do odkodowania tylko przez uprawnionego adresata. W tym celu wykorzystuje się algorytmy szyfrujące, przedstawione w dalszej części tego artykułu. W wyniku przeprowadzenia opisanych wyżej operacji, ramka składa się z dwóch bloków zawierających zawartych w 57 bitach, podczas formatowania dodawane są dodatkowo sekwencje treningowe, zawierające się w 26 bitach, następnie 2 bity flagi oraz 6 bitów dopełnienia, co daje łącznie 148 bitów na ramkę. W takiej formie możliwe jest przesłanie ramki w jednej szczelinie czasu na przyznanej przez kontrolera stacji bazowej częstotliwości. Przerwa pomiędzy częstotliwościami wynosi 200kHz i jest to odstęp, w jakim musi zmieścić się jedna transmisja. Wynika z tego, że ramka to 148 bitów, natomiast jedna szczelina czasowa ma długość odpowiadającą czasowi przesłania 156,26 bita, w rezerwie pozostaje jeszcze 8,25 bita zwane *guard period*. Powstała nadwyżka zabezpiecza przez nadpisaniem rozmowy w sąsiadujących szczelinach czasowych. Szczelina czasowa to 0,577 ms. W ośmiu kolejnych szczelinach czasowych transmitowane jest 8 kolejnych rozmów, więc w tym czasie (8*0.577 ms) telefon prześle 33.8 Kb/s (156.25 [bit]/ (0.577[ms]*8)). Na jednej częstotliwości kodowanych jest 8 rozmów, daje to transfer 270,9 Kb/s (8*33.8 Kb/s). Aby zmieścić tę ilość bitów w 200 KHz paśmie stosowana jest modulacja GMSK (ze współczynnikiem BT = 0.3). Jest to kompromis pomiędzy błędami, a występującą interferencją istniejącą między kanałami.

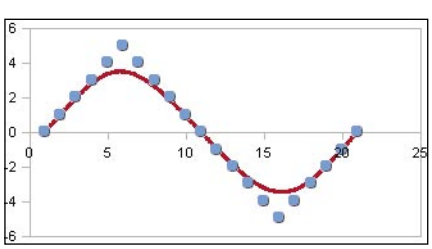
Bezpieczeństwo kart elektronicznych SIM

Karta SIM (ang. *Aubscriber Identity Module*) czyli moduł identyfikacji abonenta, to plastikowa karta elektroniczna z mikroprocesorem i wbudowaną pamięcią. Karta SIM pozwala zidentyfikować abonenta przez stacje bazową oraz umożliwia przechowywanie informacji we własnej pamięci. Spełnia funkcję klucza dostępowego do sieci GSM. Każda karta posiada 19 lub 20 cyfrowy numer identyfikacyjny SSN (*Sim Serial Number*). Zgodnie z ustaloną specyfikacją 3GPP z aparatu bez karty SIM możliwe są połączenia z numerami 000, 08, 112, 110, 118, 119, 911 i 999. Numery te są numerami alarmowymi mają najwyższy priorytet i są darmowe. Więcej na ten temat pod adresem : *http://www.3gpp.org/ftp/Specs/archive/22_series/22.101/22101-3h0.zip.*

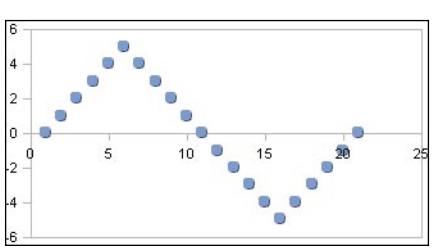
Jak to z tym bezpieczeństwem kart SIM jest naprawdę? W rzeczywistości karta SIM odgrywa bardzo dużą rolę, jeżeli chodzi o kwestię bezpieczeństwa informacji w sieciach GSM, procedurze szyfrowania sygnału i uwierzytelniania. Na karcie zawarte są algorytmy szyfrujące A3 oraz A8 dalej numer IMSI oraz (Ki), czyli indywidualny klucz uwierzytelniania abonenta.



Rysunek 2. *Sygnał analogowy*



Rysunek 3. *Próbkowanie*



Rysunek 4. *Sygnał próbkowany*

W momencie połączenia następuje weryfikacja autentyczności użytkownika GSM, przez centrum autoryzacji. Odbywa się to poprzez sprawdzenie ważności karty SIM, używając algorytm szyfrujący A3, znajdujący się zarówno na karcie, jak i w bazie centrum autoryzacji (AuC). Operacja ta polega na sprawdzeniu klucza (Ki), dalej liczby pseudolosowej (RAND) mającej długość 128 bitów, przesyłanej do stacji przy pomocy styku (Um). Autoryzacja następuje po uzyskaniu zgodności pomiędzy aparatem, a stacją bazową.

Skoro karta SIM odgrywa tak ważną rolę jednym ze sposobów ataku i zdobycia ważnych informacji jest wejść w posiadania karty lub lepiej w posiadanie jej kopii. Żeby wykonać kopię karty SIM trzeba znać dwie wartości – klucz (Ki) i numer IMSI. O ile numer IMSI daje się odczytać z karty SIM, to największe kłopoty pojawiają się, gdy musimy zdobyć wartość indywidualnego klucza uwierzytelniania abonenta. Podsumowując więc w kartach SIM, stosowanych w sieciach GSM zastosowano następujące algorytmy:

- algorytm A3 – uwierzytelnianie abonenta w trybie wyzwanie – odpowiedź,
- algorytm A8 – generowanie i przesłanie klucza sesyjnego,
- algorytm A5 – strumieniowe szyfrowanie przesyłanych informacji.

Algorytmy A3 i A8 stanowią jeden symetryczny, blokowy algorytm szyfrujący, połączony z jednokierunkową funkcją zwany COMP128.

W sieci można nabyć wiele urządzeń służących do wykonywania kopii kart SIM i jeżeli myślisz, że po skasowaniu wiadomości sms ze swojego telefonu nie da się ich odczytać, jesteś niewątpliwie w błędzie. Już rok temu można było zakupić gadżet, pozwalający na odczytanie wiadomości z karty SIM, również tych usuniętych przez użytkownika. Producent urządzenia to firma Brickhous Security. Sam produkt reklamowany jest hasłem: Miałeś kiedyś ochotę szpiegować swoją żonę, męża, nastoletnie dziecko czy kolegę z pracy? Czy interesuje Cię co kryją ich telefony? To sprytne urządzenie pozwoli Ci czytać i kasować wiadomości z karty SIM.

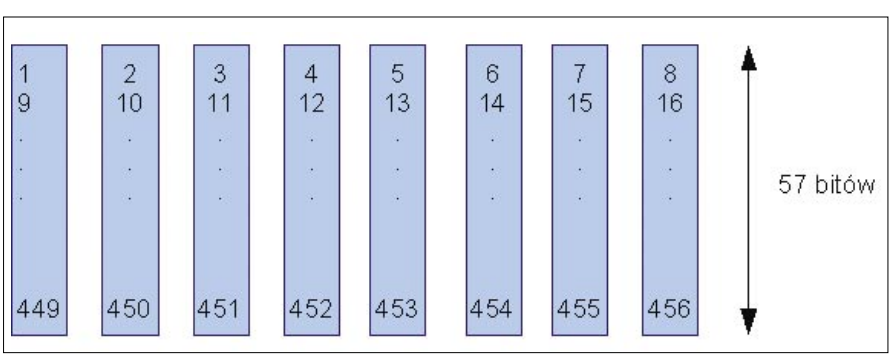
Dzięki urządzeniu możemy skopiować książkę adresową na komputer, podglądać usunięte wiadomości, zobaczyć 10 ostatnio wybieranych numerów, przeprowadzić transfer danych pomiędzy kartami SIM. Dostępna jest edycja informacji zawartych na karcie i to wszystko za cenę około 100 dolarów. Na chwilę obecną bez problemu można nabyć taki czytnik na aukcjach internetowych w cenie od 8 do 25 zł, potem tylko potrzebujemy odpowiedniego oprogramowania.

Można również sprawić sobie jedną kartę SIM z kopią nawet 12 innych kart SIM zestaw tego typu warto jest 163, 11 gr + VAT a wszystko pod adresem: *http://sklep.gsmphone.pl/index.php/pl_PL,details,id_pr,2769,menu_mode,categories.html*

Kryptografia i bezpieczeństwo w sieciach GSM

Podstawą zapewnienia bezpieczeństwa w sieciach GSM jest AuC, czyli centrum potwierdzania identyfikacji. Jest to kluczowe miejsce, jedyne dla całej sieci, gdzie generowane są klucze potrzebne do szyfrowania danych i dokonywanie uwierzytelnienia klienta oraz kart SIM. W obydwu miejscach przechowywany jest klucz (Ki). Klucz ten, jak już wiemy, przypisany jest każdej karcie SIM, dalej poprzez AuC klucz ten powiązany jest z identyfikatorem IMSI i dokładnie oznacza identyfikator konkretnego abonenta. W kolejnej fazie pojawia się wykorzystanie algorytmów A3 i A8 sprawujących piecze nad uwierzytelnieniem i wygenerowaniem klucza sesyjnego, który następnie wykorzystywany jest przez szyfrowanie strumieniowe algorytmu A5. Implementacje algorytmów A3 i A8 znajdują się zarówno w karcie SIM, jak i w AuC, a szyfrowanie algorytmem A5, producenci implementują w telefonie komórkowym, dlatego też szyfrowanie odbywa się poza kartą SIM, natomiast generowanie klucza w samej karcie. Patrząc od strony sieci, szyfrowanie algorytmem A5 odbywa się w Bazowej Stacji Nadawczej, emitującej i odbierającej sygnał od użytkowników, otrzymując odpowiedni klucz od VLR-a, czyli bazy danych rejestrującej łączących się abonentów.

Struktura sieci komórkowej realizuje trzy podstawowe usługi zapewniające bezpieczeństwo, w skład których wchodzą: uwierzytelnienie, anonimowość i poufność. Tworząc standaryzację systemu pozostawiono jednak wolną rękę operatorom w zakresie zastosowania algorytmów szyfrujących. Mówi się o istnieniu odmian algorytmu A5 podzielonego na A5/1 (najsilniejsza wersja algorytmu), A5/2 (słabsza wersja algorytmu) i A5/0 (brak szyfrowania). Standaryzacja miała na celu ujednolicenie systemu zabezpieczeń implementowanych w telefonach tak, by mogły funkcjonować w różnych sieciach, nie ograniczając się tylko do sieci macierzystej. Ciekawą informacją jest fakt, iż zabezpieczenie kryptograficzne obejmuje jedynie radiową część systemu, informacje krążące wewnątrz samej sieci nie posiadają zabezpieczeń. Prowadząc atak na sieć GSM można wykorzystać każdy rodzaj nasłuchu oraz wszelkie sposoby modyfikowania danych wewnątrz stacji bazowej. Twórcy



Rysunek 5. *Procedura Channel Coding*

systemu zakładali, iż ataki polegające na podstawianiu fałszywej stacji bazowej i prowadzeniu nasłuchu są bardzo mało prawdopodobne z powodów finansowych przy zakupie lub budowie takiego urządzenia.

Zapewnieniem anonimowości zajmuje się protokół, zgodnie z którym pod numer IMSI przy każdym połączeniu podstawiany jest tymczasowy nr TMSI, stosowany podczas komunikacji radiowej. Każdorazowa zmiana numeru TMSI sprawia wrażenie, iż daje to dość duże bezpieczeństwo i brak możliwość identyfikacji konkretnego abonenta. W praktyce jednak nie do końca tak jest. Na stacji mobilnej nie zastosowano żadnej procedury uwierzytelniającej, co pozwala przeprowadzać ataki typu *man-in-the-middle*, podstawiając nieprawdziwą stację bazową, której koszt mieści się w granicach nieprzekraczających 10 000 dolarów, więc przy odpowiedniej motywacji i potrzebach zdobycia informacji jest to nie wielka przeszkoda, szczególnie w przypadku, gdy wartość informacji może przekraczać wartość fałszywej stacji. W wyniku tego, iż dopuszczono przesyłanie numeru IMSI kanałem bez zabezpieczeń, wystarczy więc podesłać sygnał *Identiti Request* (typ IMSI) z podstawionej stacji, by aparat telefoniczny abonenta w odpowiedzi podesłał prawdziwy nr IMSI (należy przeprowadzić odszyfrowanie prawdziwego IMSI z odebranego TMSI, nie jest to jednak specjalnie duży problem).

Algorytmy szyfrujące w sieciach GSM

Algorytm A3 wykorzystywany jest w chwili nawiązywania połączenia, zawarty na karcie tajny klucz (Ki) zostaje zweryfikowany przez centrum autoryzacji w momencie wezwania sieci – RAND (przesłanie użytkownikowi liczby pseudolosowej zawartej w 128 bitach). W odpowiedzi sieć otrzymuje od użytkownika SRES (32 bity informacji). Kolejnym etapem jest dokonanie porównania odpowiedzi z wartością wyliczona przez sieć, i jeżeli są zgodne następuje autoryzacja i uwierzytelnienie. Cała operacja trwa krócej niż 500 ms.

W chwili obecnej stosowane i znane kodowania to COMP128-1, COMP128-2 i COMP128-3. Udało się złamać i upublicznić wersję COMP128-1, dwa pozostałe pozostają, jak do tej pory niejawne.

Algorytm A8

A8 jest algorytmem odpowiadającym za wybór klucza sesyjnego (Kc), umożliwiającego szyfrowanie danych.

Algorytm COMP128

Algorytm COMP128 realizuje w jednym kroku zadania, jakie wykonują algorytmy A3 i A8, czyli mówiąc w skrócie uwierzytelnianie i wybór klucza sesyjnego. W związku z tym, iż algorytmy te posiadają identyczne parametry wejścia, w praktyce dały się zastąpić jednym algorytmem posiadającym dwa wyjścia, stąd więc algorytm COMP128 jest składową algorytmów A3 i A8.

By zachować wysokie bezpieczeństwo algorytm COMP128 miał być utajniony. W 1997 opublikowany został tekst dokumentu zawierającego notatki jednego z inżynierów pracujących nad tym algorytmem, dzięki czemu w kwietniu 1998 Ian Goldberg i David Wagner z Uniwersytetu Kalifornijskiego w Berkeley zrekonstruowali kod algorytmu wraz z zagubionymi liniami tekstu i dokonali implementacji algorytmu w języku C, przez co udało się przeprowadzić pierwszy udany atak na algorytm COMP128.

Po przeprowadzonych testach, polegających na złamaniu algorytmu COMP128 odkryto, że klucz sesji (Kc) zawiera jedynie 54 bity, które są użyteczne. Natomiast ostatnie 10 bitów zawsze jest zerowane, co zmniejsza zabezpieczenie o 1 000 razy w stosunku do tego co zostało określone w specyfikacji GSM. Twórcy przeprowadzili atak na COMP128, zawierający 2^19 zapytań do karty SIM. Trwał on około 8 godzin. Działania te doprowadziły do poznania długoterminowego klucza (Ki), zapisanego na karcie SIM. Następnie w roku 2002 Josyula R. Rao, Pankaj Rohatgi, Helmut Scherzner z firmy IBM wraz z Stephanie Tinguely ze Szwajcarskiego Instytutu Technologii przeprowadzili atak partycyjny, polegający na uzyskaniu dostępu bocznymi kanałami, umożliwiając przez to złamanie algorytmu COMP128 w czasie krótszym niż minuta. Informacje na ten temat opublikowane zostały w artykule *Partitionig Attack: Or How to Rapidly Clone Some GSM Cards*.

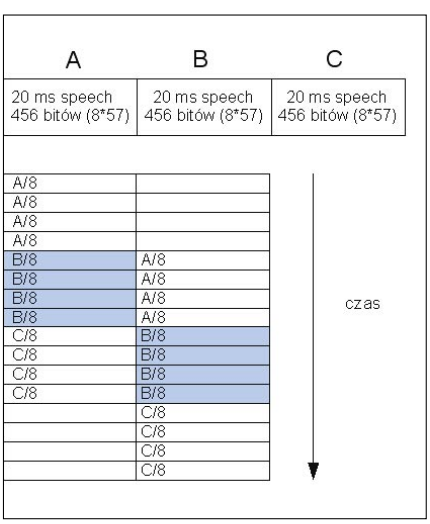
Algorytm A5

Transmitowany sygnał w sieciach GSM zakodowany został przy użyciu algorytmu zwanego A5. A5 jest szyfrem strumieniowym, służącym do uwierzytelniania i szyfrowania konwersacji między telefonem abonenta a stacją bazową. Istnieją dwa warianty algorytmu A5 tj. Silniejsza, dająca większe bezpieczeństwo wersja A5/1 i wersja słabsza A5/2. Obydwie wersje mają zastosowanie w Europie. Jak wiemy transmisja głosu w sieciach GSM realizowana jest przy pomocy przesyłu ramek. Numer każdej ramki -Fn zliczany jest za pomocą licznika w cyklu o długości 222. Transmisja szyfrowana jest 64-bitowym kluczem sesji – k, utworzonego przy pomocy funkcji haszującej z klucza głównego użytkownika i wartości losowej.

Wygenerowanie klucza odbywa się przy zastosowaniu algorytmu A8.

Przebieg procesu szyfrującego algorytmem A5 przedstawia się następująco :

- 64-bitowy klucz k dla każdej ramki jest nieliniowo łączony z 22-bitową wartością licznika ramek Fn.



Rysunek 6. *Przeplot blokowy*

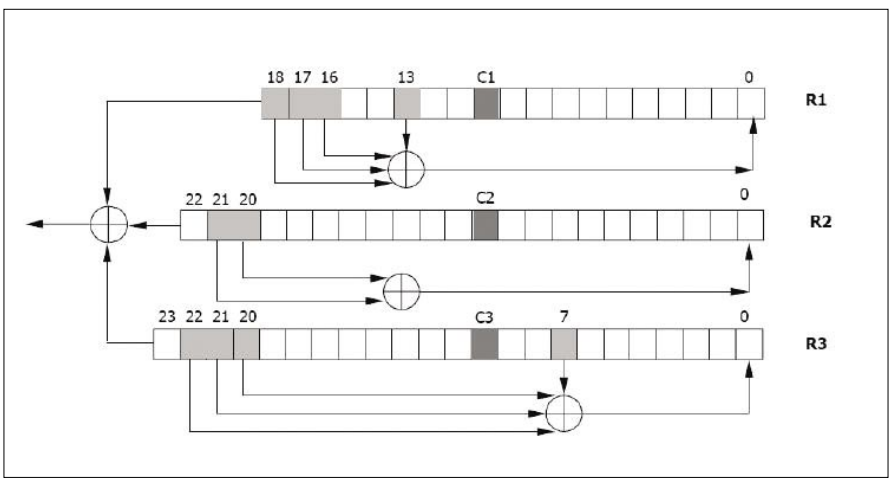
- Z powyższego połączenia powstaje wektor inicjujący pseudolosowego generatora, generującego ciąg 228 bitów, który następnie sumowany jest modulo 2 z 228 bitami tekstu jawnego w celu wytworzenia szyfrogramu.

Układ ma budowę trzech liniowych rejestrów cyklicznych (R1, R2, R3) ze sprzężeniem zwrotnym.

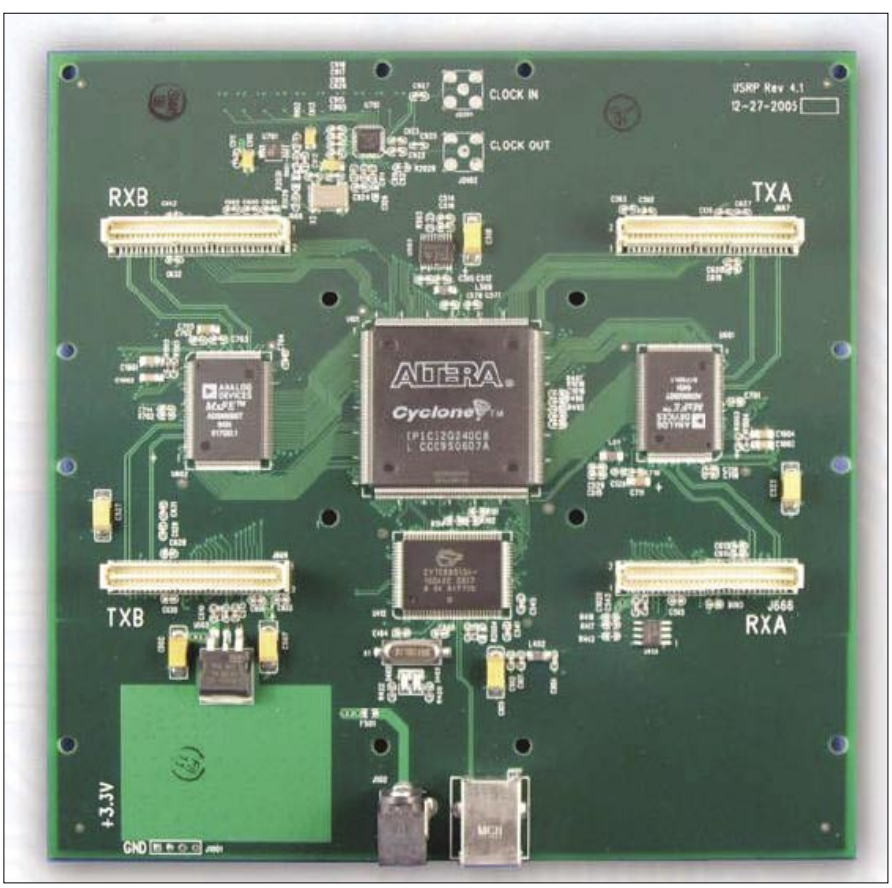
- R1 – długość 19 bitów,
- R2 – długość 22 bitów,
- R3 – długość 23 bitów.

Najmłodszy bit każdego rejestru wynosi zero.

Rejestry tworzone są generatorem sekwencji pseudolosowej, są różnej wielkości i posiadają różne punkty wyprowadzenia sygnału zwrotnego. Rozmieszczenie punktów sygnału zwrotnego rozkłada się jak w Tabeli 1.



Rysunek 7. *Schemat szyfrowania algorytmem A5 (źródło Wikipedia)*



Rysunek 8. *Universal Software Radio Peripheral (źródło: internet)*

Punkty dobrane zostały w taki sposób, by maksymalnie wydłużyć okresy sekwencji pseudolosowych, generowanych przez poszczególne rejestry. Rejestry poddawane są taktowaniu wedle reguły strat/stop.

Każdy z rejestrów ma punkt, w jakim sygnał zostaje wprowadzony, gdzie następuje wystartowanie taktowania, co przedstawia się w sposób, jak na Tabeli 2.

W każdym cyklu, analizie poddawana jest zawartość bitów C1, C2, C3. Jeżeli w wyniku analizy dwa z trzech rejestrów mają wartość równą 1, taktowaniu podlegają tylko rejestry równe 1. Jeżeli w analizie dwa z trzech rejestrów mają wartość równą 0, taktowaniu poddane zostaną tylko rejestry z wartością 0. Taktowanie realizowane jest przy użyciu funkcji większościowej (*majority function*). Wynika z tego, iż każdorazowo taktowane są co najmniej 2 rejestry.

W sieci istnieje zaimplementowanie algorytmu A5 w języku Java – aplet dostępny pod adresem : *http://citata.ovh.org/a5/aplet.php*.

Urządzenia i technologie dekodujące zabezpieczenia GSM

Jak napisane zostało wyżej, do szyfrowania sygnałów GSM stosowany jest szyfr strumieniowy A5, jednak zabezpieczenie to może uchronić co najwyżej przed radio amatorami, nieco zdolniejsi są w stanie ominąć je bez trudu.

W początkowych okresach działalności technologii GSM moc obliczeniowa, jaka byłaby potrzebna do załamania użytych do zabezpieczenia algorytmów (A5, A8, COMP128), dostępna była jedynie w instytucjach wojskowych i naukowych. Z czasem jednak postęp technologiczny, szczególnie w zakresie pamięci i mocy obliczeniowej, sprawił, iż sprzęt, jaki jest potrzebny do pokonania zabezpieczenia GSM, stoi już w naszych domach. Utajnione przed ogółem specyfikacje dotyczące algorytmów A5 i A8 w wyniku przecieków informacji, stały się obiektem badań naukowych i hakerskich. Pomimo dużego wysiłku, jaki włożono w utajnienie algorytmów, już w 1994 pojawiły się pierwsze przecieki

na ich temat. Natomiast w roku 1999 używając metody inżynierii odwrotnej, wykorzystując przy tym terminal GSM udało się odtworzyć cały algorytm.

Moc zabezpieczenia w kryptografii w dużej mierze odnosi się do pojęcia długości użytych parametrów kryptograficznych, które w przypadku GSM wynoszą :

- klucz identyfikacyjny abonenta Ki: 128 bitow,
- zapytanie autentykacyjne RA ND: 128 bitow,
- odpowiedź autentykacyjna SRES: 32 bity,
- klucz szyfrujący Kc : 64 bity.

Najważniejszym elementem, na jakim bazuje cały model bezpieczeństwa GSM, jest klucz identyfikacyjny abonenta (Ki), który w momencie ujawnienia, daje możliwość szybkiego złamania podstawowych zabezpieczeń systemu. Jeżeli klucz ten dostanie się w ręce *sprawnego użytkownika*, umożliwia mu pełen dostęp do połączeń wraz z szyfrowaniem i deszyfrowaniem informacji oraz możliwość podszycia się pod danego abonenta w celu wykonywania połączeń na jego koszt, co więcej, gdy oszust wykona dla siebie sklonowaną kartę SIM, sieć w żaden sposób nie rozróżni, która z kart jest prawdziwa. Jeżeli uda się przeprowadzić udany atak na uwierzytelnianie, inne zabezpieczenia nie mają już najmniejszego zastosowania.

David Hultom i Steve Muller udowodnili, iż da się pokonać szyfrowanie A5 w czasie około 30 minut, wykorzystując do tego powszechnie dostępny sprzęt i oprogramowanie. Zestaw jakiego użyli kosztował około 1 000 dolarów. Po uruchomieniu urządzenia można było podsłuchiwać rozmowy w promieniu 20km.

W skład zestawu wchodziło urządzenie noszące nazwę *Universal Software Radio Peripheral.*

Specjaliści odpowiednio dostosowali urządzenie, by mogło przechwytywać sygnały nadawane w sieciach GSM, następnie metodą porównywania sygnałów nadawanych przez stację oraz telefon testowy rozpracowali szyfrowanie A5, stosując w tym celu układ *Field Programmable Gate Array.* Układ FPGA jest to bezpośrednio programowalna macierz bramek o funkcjonalności zbliżonej do układów typu ASIC. Różnica polega na tym, iż może być wielokrotnie przeprogramowany już po tym, jak został wytworzony i zamontowany w urządzeniu docelowym. Największymi dostawcami tego układu są firmy Altera Corp., XilinX oraz Alcatel i QuicLogic.

Więcej informacji o samym układzie FPGA można znaleźć na stronach : *http://www.fpgacentral.com/, http://www.fpga-faq.com/.*

Kalendarium ataków na algorytm COMP128-1

- 1 kwietnia 1998 roku – autorami ataku są D.Wagner, I.Goldberg, M.Briceno. Atakujący wykorzystali słabość polegającą na istnieniu wąskiego gardła w kompresji motyla. Zasada jest taka, iż po drugim kroku kompresji 4 bajty wyjściowe zależą od 4 bajtów wejściowych i dwa z nich należą do (Ki) kolejne dwa do (RAND). Algorytm kompresji motyla powoduje również, iż kolizję w kolejnych rundach są propagowane dalej i zmieniając zatem dwa pierwsze bajty wejściowe można bez trudu znaleźć kolejną kolizję. Kolejne 2 bajty wyszukujemy losowo, aż do skutku, a powtarzając ten schemat 8 razy można uzyskać pełny 16 bajtowy klucz Ki. Czas potrzebny na złamanie algorytmu to około 6 godzin. *Briceno M., Goldberg I., GSM Cloning – http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html.*
- D.Kalijewic poprawił poprzedni sposób, stosując wywoływanie kolizji w kompresji motyla w kilku

krokach, nie tylko w drugim, w wyniku przyspieszyło to cały proces ataku. Autor umieścił swój program pozwalający na łamania klucza Ki i nr IMSI w sieci. Czas potrzebny na złamanie algorytmu to około 60 minut. *Quirke J., Security in the GSM system - http://www.ausmobile.com/downloads/technical/Security%20in%20the%20GSM%20system%2001052004.pdf*

- 1 maja 2002 roku – autorzy ataku: J.R Rao, P.Rohatgi, H.Scherzer (pracownicy IBM). Wykorzystano fakt bardzo małej wydajności kart SIM w momencie działania algorytmu COMP128, procesory kart adresują jedynie na 8 bitach, a do pierwszej kompresji w algorytmie motyla potrzeba adresowania 9 bitów. Prowadzenie mierzenia czasów działania pozwoliło na przeprowadzenie ataku 1 000 dowolnych wyzwań RAND lub 8 konkretnych. Złamanie algorytmu przy wywołaniu 8 zapytań trwa około 2 sekund

Technologia Bluetooth a bezpieczeństwo

Bluetooth to doskonała technologia umożliwiająca wymianę informacji pomiędzy urządzeniami mobilnymi w tym oczywiście pomiędzy telefonami GSM. Zapewne niejednokrotnie odbierałeś czy wysyłałeś tym kanałem pliki multimedialne, fotografie, dźwięki MP3 i inne informacje, by wymienić je ze znajomymi. Czy zastanowiło Cię jednak, co można jeszcze zrobić, jeżeli ma się dostęp do telefonu z włączonym bluetooth? W tym miejscu zapoznam Cię czytelniku z takimi pojęciami jak *bluehacking*, w skład którego wchodzą:

- *Bluesnarfing* – uzyskanie dostępu do prywatnych informacji na urządzeniu, na które przeprowadza się atak przy wykorzystaniu technologii bluetooth. Odczytywanie wiadomości tekstowych, kopiowanie książki adresowej itd.
- *BlueBug* – wygenerowanie dużej ilości połączeń do telefonu, akceptującego połączenia bluetooth, doprowadza to do zawieszenia się systemu telefonu.
- *BlueBump* – atak przeprowadzony przy wykorzystaniu metod socjotechnicznych i *bluesnarfingu*. Wymaga wymuszenia na użytkowniku włączenia akceptacji połączeń bluetooth np.: w celu przesłania wizytówki i uzyskania dostępu do poufnych danych.

Bibliografia

- ISO/IEC 7816-8, *Security related interindustry commands*,
- Kubas Monika, Molski Marian, *Karta elektroniczna. Bezpieczny nośnik informacji*. MIKOM 2002,
- Chocianowicz Włodzimierz, Urbanowicz Jerzy, *Kryptografia w kartach elektronicznych: możliwości i ograniczenia*,
- 3GPP TS 55.216 v6.2.0 *A5/3 and GEA3 Specifications – www.gsmworld.com/using/algorithms/docs/a5_3_and_gea3_specifications.pdf*
- Aranibar N., *GSM Security - www.mcs.csuhayward.edu/~pwong/cs6520_win03/gsm_security.doc*
- Barkan E., Biham E., Keller N., *Instant Ciphertext-only Cryptanalysis of GSM Encrypted Communication (polski tytuł: Błyskawiczna kryptoanaliza z samym szyfrogramem komunikacji szyfrowanej w systemie GSM) - http://cryptome.org/gsm-crack-bbk.pdf (polskie tłumaczenie: www.phreak.pl/gsm/szyfrowanie.pdf)*,
- *www.wikipedia.pl* (artykuły dotyczące GSM)
- Briceno M., Goldberg I., Wagner D., *A pedagogical implementation of the GSM A5/1 and A5/2 "voice privacy" encryption algorithms* (przedstawienie algorytmów A5/1 I A5/2 w języku C) - *http://www.mirrors.wiretapped.net/security/cryptography/algorithms/gsm/a5-1-2.c*
- Briceno M., Goldberg I., Wagner D., An implementation of the GSM A3A8 algorithm. (Specifically, COMP128.) (implementacja wersji COMP128-1 w języku C) – *http://www.gsm-security.net/papers/a3a8.shtml.*

Podsumowanie

W chwili obecnej, gdy telefony wyposażone są w komunikujące się poprzez bluetooth aplety javy lub inne oprogramowanie, istnieje zagrożenie, iż atakujący może wykonać połączenie na koszt swojej ofiary. oczywiście zachowując odpowiednią odległość.

Jest to tylko wzmianka, by uczulić użytkowników urządzeń mobilnych na możliwości jakie oferują urządzenia mobilne, które mogą być wykorzystane w nieodpowiedni sposób.

Jak krucha jest *prywatność* w erze mobilnych bezprzewodowych technologi służących do przesyłania informacji. Czy w ogóle można jeszcze mówić, że prywatność istnieje? Czy korzystając z telefonu komórkowego mamy pewność, że nikt oprócz właściwego adresata nie pozna tego, co mamy mu do przekazania. Wobec powyższego minimalistycznie przedstawionego skrótu można sądzić, że wydobycie informacji dla zmotywowanego na takie działanie człowieka jest w zasięgu ręki.

Co na to firmy i korporacje, których droga mobilnego transmitowania ważnych danych narażone są na ich utratę? Należy się zastanowić, jakie informacje przekazujemy tą właśnie drogą i czy faktycznie zachowujemy przy tym odpowiedni poziom zabezpieczeń. Projektanci technologii GSM nie do końca przyłożyli odpowiednią uwagę do bezpieczeństwa informacji. Widoczne słabe punkty to brak uwierzytelniania stacji bazowej wobec stacji mobilnej, wykorzystywanie słabych algorytmów szyfrujących i brak wdrożenie nowych wersji algorytmów już opracowanych (np.: COMP128 – 4), niekontrolowanie integralności danych, zastosowanie tych samych kluczy we wszystkich algorytmach szyfrujących.

Mariusz Gibki

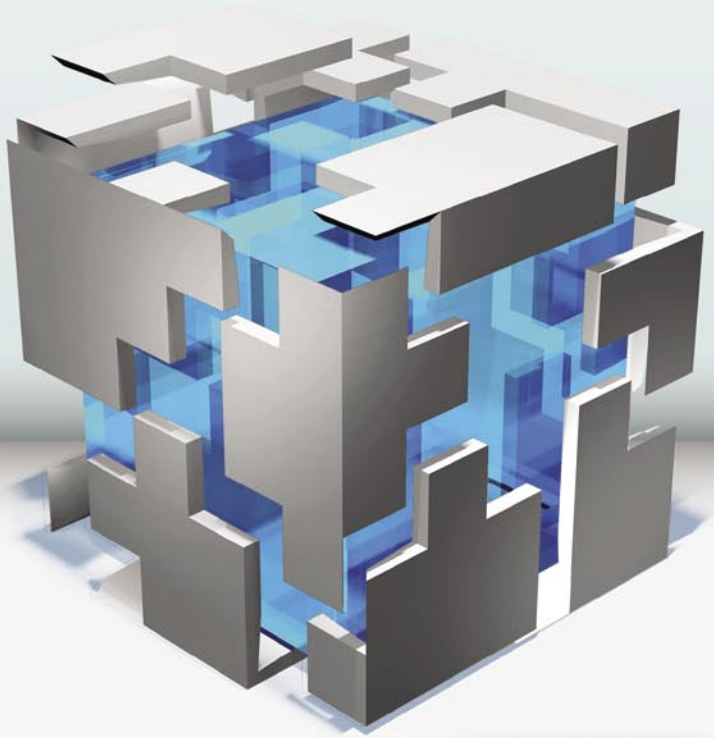
Inżynier informatyki specjalizacja informatyka w zarządzaniu absolwent Wyższej Szkoły Informatyki w Łodzi, członek ms-group.pl, pasjonat programowania, baz danych i fotografii

Kontakt z autorem: *mariusz.gibki@gmail.com*

Każdego dnia

użytkownicy tracą

terabajty danych



STREAMDATA

Odzyskiwanie danych

www.streamdata.pl biuro@streamdata.pl +48 605-06-16-06