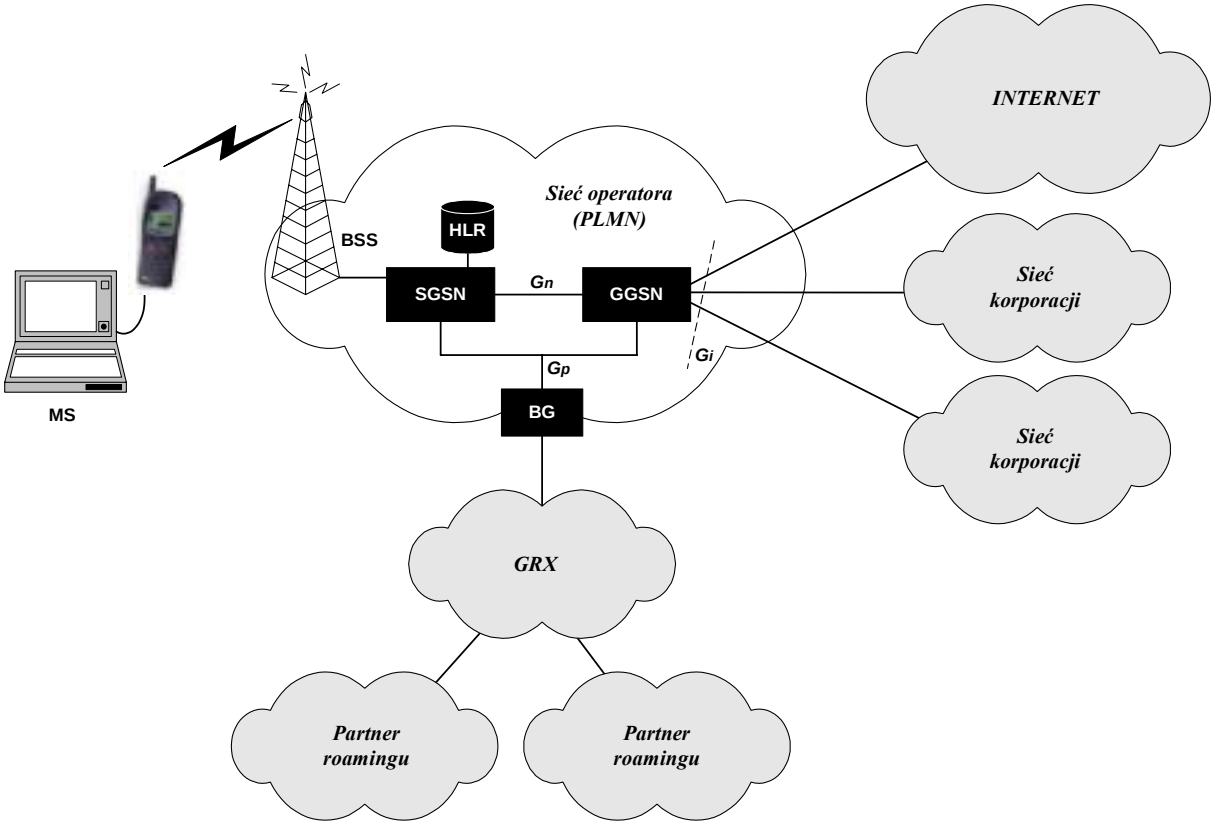
Zagadnienia bezpieczeństwa sieci GPRS

Internet i telefonia komórkowa w krótkim czasie zyskały popularność i powszechne zastosowanie. Internet daje ludziom globalny dostęp do informacji, GSM - swobodę komunikowania się z innymi. Technologia, która łączy ich funkcjonalność to *GPRS*[1]. Rozszerza ona zakres usług operatorów GSM, którzy oprócz mobilnej komunikacji głosowej mogą oferować swoim klientom w pełni mobilny dostęp do Internetu i sieci korporacyjnych. GPRS podobnie jak Internet i inne systemy teleinformatyczne narażony jest na szereg zagrożeń. Jeżeli ma on służyć do prowadzenia biznesu wymagane jest zapewnienie odpowiedniego poziomu bezpieczeństwa (m.in. poufności, integralności, autentyczności).

Technologia GPRS stwarza także szereg nowych zagrożeń dla samych operatorów GSM. Oprócz typowych zagrożeń jak nadużycia i oszustwa klientów, czy klonowanie kart SIM pojawia się wiele nowych niebezpieczeństw. Sieci GPRS są oparte na powszechnie znanych technologiach IP (m.in. stosowanych w Internecie) i posiadają połączenia do wielu sieci zewnętrznych (np. partnerów z umowami roamingu, korporacji, operatów *GRX*[2], Internetu). W większości są to zagrożenia występujące powszechnie w systemach teleinformatycznych, m.in.:

- podsłuch sieciowy i przechwytywanie połączeń,
- podszywanie się po innych użytkowników (*ang. masquerade*),
- nieupoważniony dostęp i manipulacja danych,
- ataki destrukcyjne i destabilizujące.



[1] GPRS - General Packet Radio Service
[2] GRX - GPRS Roaming Exchange

Funkcjonowanie sieci GPRS

Sieć GPRS składa się z części radiowej, odpowiedzialnej za łączność z użytkownikami oraz części teleinformatycznej, zapewniającej m.in. dostęp do Internetu oraz sieci korporacji. Zasady implementacji i funkcjonowania sieci GPRS ustalają protokoły i standardy wydane m.in. przez instytut normalizacji *ETSI*[3]. Rysunek przedstawia podstawowe elementy i architekturę sieci GPRS. Użytkownik do zestawienia połączenia GPRS powinien posiadać telefon umożliwiający obsługę GPRS oraz jako abonent sieci GSM uprawnienia do korzystania z tej usługi. Użytkownik podłącza telefon do komputera i konfiguruje połączenie na podobnych zasadach jak dla zwykłego modemu. Dla sieci GPRS telefon i komputer użytkownika stanowią stację mobilną *MS*[4].

Proces zestawiania połączenia mobilnego użytkownika poprzez GPRS do Internetu lub sieci korporacji przebiega następująco:

1. MS nawiązuje połączenie radiowe z lokalną stacją bazową *BSS*[5], która przekazuje to połączenie do systemu obsługi GPRS w sieci *PLMN*[6].
2. Połączenie ze stacji BSS zostaje przejęte przez węzeł *SGSN*[7], który zajmuje się dalszą obsługą stacji MS (m.in. uwierzytelnieniem i autoryzacją abonenta w oparciu o bazę *HLR*[8]).
3. SGSN zestawia kanał z wybranym węzłem *GGSN*[9] za pomocą protokołu *GTP*[10]. Połączenie w zależności od użytkownika (abonent własny lub innego operatora) realizowane jest z lokalnym GGSN lub z węzłem zlokalizowanym w sieci partnera roamingu. Komunikacja z sieciami PLMN innych operatorów odbywa się zwykle przez sieć GRX i realizowana jest z użyciem urządzeń brzegowych BG[11].
4. GGSN kieruje połączenie to docelowej sieci IP (Internetu, sieci korporacji). Z sieci zewnętrznych GGSN postrzegany jest jak ruter IP.

Węzły SGSN i GGSN fizycznie mogą być zaimplementowane w jednym urządzeniu lub oddzielnie. Ze względu na rodzaj realizowanych połączeń w sieci GPRS można wyróżnić następujące interfejsy (patrz rysunek 1): *Gn* – połączenia w ramach jednej sieci PLMN, *Gp* – połączenia pomiędzy różnymi sieciami PLMN, *Gi* – połączenia do Internetu i sieci korporacji.

Protokół GTP służy do tunelowania innych protokołów (np. TCP/IP) w sieci GPRS. Kanały GTP zestawiane są pomiędzy lokalnymi lub odległymi węzłami SGSN i GGSN (np. z sieci PLMN partnerów, którzy posiadają umowę roamingu). Zestawienie kanału GTP jest inicjowane przez stację MS, która przekazuje do SGSN odpowiednie parametry tego połączenia (m.in. nazwę *APN*[12] identyfikującą sieć IP użytkownika np. *firma.pl.gprs*). SGSN tworzy zapytanie *PDP*[13] *Context* i przekazuje je do odpowiedniego GGSN. Następnie GGSN ustala dla użytkownika adres IP (statyczny/RADIUS/DHCP) i wysyła do SGSN odpowiedz na PDP Context. Cała komunikacja z/do MS jest tunelowana poprzez otwarty kanał GTP. Jeżeli mobilny użytkownik (MS) znajdzie się w zasięgu innego SGSN następuje operacja przekazania kanału GTP (*handover*). Nowy SGSN wysyła wtedy do GGSN zapytanie *Update PDP Context*. Komunikacja GTP pomiędzy SGSN i GGSN nie jest uwierzytelniania. Domyślnie nie jest ona także szyfrowana.

[3] ETSI - European Telecommunication Standards Institute
[4] MS - Mobile Station
[5] BSS - Base Station System
[6] PLMN - Public Land Mobile Network
[7] SGSN - Serving GPRS Support Node
[8] HLR – Home Location Register
[9] GGSN - Gateway GPRS Support Node
[10] GTP - GPRS Tunneling Protocol
[11] BG – Border Gateway
[12] APN - Access Point Name
[13] PDP - Packet Data Protocol

Bezpieczeństwo sieci GPRS

Infrastruktura sieci GPRS składa się z części radiowej i teleinformatycznej. W każdej z nich występują specyficzne zagrożenia oraz wdrożone (lub możliwe do wdrożenia), przeciwdziałające im zabezpieczenia. Dla sieci radiowej standardy GSM określają szereg mechanizmów bezpieczeństwa. Po stronie użytkownika występują unikalne numery identyfikacyjne *Ki*[14], *IMSI*[15] (id abonenta) oraz *IMEI*[16] (id telefonu) za pomocą, których uwierzytelniana jest jego tożsamość. Transmisja danych pomiędzy MS i SGSN chroniona jest z użyciem opartych na kryptografii algorytmach uwierzytelniania i szyfrowania. Zastrzeżenia budzi jakość implementacji tych zabezpieczeń. Analitycy bezpieczeństwa wykazują m.in. potencjalne możliwości klonowania kart SIM i niezauważalnego podsłuchiwania rozmów, łamania algorytmu uwierzytelniania COMP128, „podstawienia" fałszywej stacji BSS, itd.

W części teleinformatycznej GPRS występują zagrożenia specyficzne dla technologii IP oraz elementów GPRS. Infrastruktura sieci GPRS opiera się głównie na systemach i urządzeniach powszechnie wykorzystywanych np. w Internecie. Także urządzenia xGSN zwykle oparte są na sprzęcie i systemach operacyjnych ogólnego przeznaczenia (np. SUN Solaris). Narażona jest więc na niebezpieczeństwa typowe dla systemów i sieci IP (m.in. penetracje, włamania, ataki DoS). Wielkość zagrożenia dodatkowo potęguje fakt, że sieć GPRS posiada połączenia z wieloma sieciami zewnętrznymi (np. partnerów roaming-owych, korporacji, operatów GRX, Internetu). Obowiązujące standardy GPRS nie określają żadnych zabezpieczeń pomiędzy różnymi sieciami GPRS (3GPP TS 09.60). Tylko w gestii operatora jest wdrożenie na urządzeniach brzegowych BG odpowiednich zabezpieczeń, chroniących własne zasoby przed niepożądaną ingerencją z sieci innych operatorów.

Technologia GPRS jest nową technologią i można spodziewać się, że jej podatności na zagrożenia będą w trakcie jej eksploatacji identyfikowane. Obecnie analitycy zwracają uwagę na dwa główne zagrożenia, wynikające ze słabości protokołu GTP:

- przechwytywanie i „zabijanie" sesji GPRS,
- ataki destrukcyjne i destabilizujące GPRS.

SGSN i GGSN komunikują się za pomocą protokołu GTP. Występują pomiędzy tymi komponentami „silne" relacje zaufania (tzn. brak odpowiednich mechanizmów weryfikacji i uwierzytelniania). Stwarza to zagrożenie przechwytywania, bądź „zabijania" sesji GPRS. W trakcie prowadzenia transmisji danych przez użytkownika z jednym SGSN intruz może przechwycić to połączenie korzystając z innego SGSN. Do tego celu potrzebuje znać jedynie numer identyfikacyjny tunelu GTP. Zagrożenie wynika z faktu, że GGSN nie wykonuje weryfikacji, jeżeli SGSN przesyła prośbę o aktualizację PDP-Context. GGSN ufa, że legalny użytkownik wszedł w zasięg innego SGSN i chce kontynuować sesję GPRS. Problem ten potęguje się w środowisku partnerów roaming-owych. Drugie zagrożenie wynika, z tego że protokół GTP nie sprawdza dopuszczalnego rozmiaru nagłówka GTP. Może to zostać wykorzystane do wykonywania różnego rodzaju ataków destrukcyjnych i destabilizujących (*buffer overflow*).

Wielu operatorów wdrożyło w swoich sieciach GPRS dedykowane zabezpieczenia typu Firewall, które umożliwiają im m.in. wykonywanie kontroli dostępu dla określonych MS, SGSN i GGSN, inspekcję i weryfikację integralności protokołu GTP, monitorowanie oraz rejestrowanie ruchu sieciowego, a także alarmowanie w razie wykrycia zdarzeń podejrzanych i nadużyć bezpieczeństwa. Najczęściej stosowanym przez operatorów rozwiązaniem ochrony sieci GPRS jest system zabezpieczeń Check Point FireWall-1 GX.

[14] Ki – Individual Subscriber Authentication Key
[15] IMSI - International Mobile Subscriber Identity
[16] IMEI – International Mobile Equipment Identity