Tomasz SERAFIN

Zabezpieczanie biznesowych rozmów telefonicznych

Tajemnicą przedsiębiorstwa są nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.[1] Jest to obszerny zbiór danych, które przedsiębiorca może uznać za istotne z punktu widzenia bezpieczeństwa firmy i objąć je specjalnym nadzorem. Taka decyzja wiąże się również z koniecznością zastosowania konkretnych rozwiązań technicznych, a jednym z nich jest zabezpieczenie środków łączności telefonii komórkowej.

Zapis art. 55[1] Kodeksu cywilnego stanowi, że tajemnica przedsiębiorstwa jest jednym ze składników majątkowych przeznaczonych do prowadzenia działalności gospodarczej i wymieniana jest obok innych licznych uprawnień, takich jak: prawo własności nieruchomości lub ruchomości, wierzytelności, koncesje, licencje lub majątkowe prawa autorskie i prawa pokrewne. Przedsiębiorca posiada więc prawo do określenia zakresu informacji, które stanowią dla niego szczególną wartość i równocześnie nie są informacją publiczną.[2] Ten niematerialny składnik przedsiębiorstwa zdefiniowany został w ustawie o zakazie nieuczciwej konkurencji i rozszerzony o „inne informacje posiadające wartość gospodarczą" nowelizacją, która weszła w życie 10 listopada 2002 r. Aby określone przez przedsiębiorcę informacje otrzymały ochronę prawną, musi on podjąć pewne „niezbędne" działania w celu ich zabezpieczenia. Interpretacja słowa „niezbędne" nastręcza trudności i wielu szefów firm porusza się po omacku, próbując wdrażać niektóre z dostępnych rozwiązań. Niestety bardzo często konkretne decyzje podejmowane są według kryterium ich ceny. Jednak trzeba mieć świadomość, że zabezpieczenie informacji powinno tworzyć spójny system i należałoby budować go całościowo, integrując nowe jego składniki z funkcjonującymi dotychczas w firmie, pamiętając, że o sile zastosowanych zabezpieczeń decyduje najsłabszy element systemu. Zazwyczaj mamy więc zbiór różnego rodzaju zabezpieczeń, w tym technicznych, ale nie możemy mówić o bezpieczeństwie. Bez szczegółowego audytu procesów zachodzących w danym przedsiębiorstwie i wyodrębnienia danych wrażliwych, trudno mówić o bezpieczeństwie informacyjnym.

Niniejszy artykuł może zainicjuje dyskusję na temat bezpieczeństwa w biznesie. Będzie to zależało od Państwa zainteresowania i opinii, które proszę przesyłać na adres mailowy redakcji. Natomiast w tym numerze chcę omówić kilka metod zabezpieczania treści przekazywanych za pośrednictwem telefonów komórkowych GSM, które mogą ochronić informacje wrażliwe przedsiębiorcy, chociażby w trakcie prowadzenia negocjacji handlowych. Zacznę od przybliżenia problematyki podsłuchu.

---

[1] Art. 11 ust. 4 *Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji* (Dz. U. z 1993 r. Nr 47 poz. 211 z późn. zm.).

[2] Art. 5 *Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej* (Dz. U. z 2001 r. Nr 112 poz. 1198 z późn. zm.).

Jak działa podsłuch treści sygnału GSM?

Do przechwytywania sygnału GSM i podsłuchiwania treści rozmowy telefonicznej może zostać wykorzystany sprzęt, który nie wymaga instalowania w telefonie dodatkowych urządzeń lub aplikacji. Łączność GSM oparta jest na dwóch rodzajach transmisji danych: za pośrednictwem fal radiowych i standardowej kablowej łączności telekomunikacyjnej, która opiera się na sieci szkieletowej i centralach telefonicznych. Użytkownik korzystający z mobilnego telefonu pracującego w systemie GSM łączy się za pośrednictwem stacji bazowych BTS (*Base Transceiver Station*) i kontrolerów stacji bazowych BSC (*Base Station Controller*). Przy nawiązywaniu połączenia z siecią telefon jest odpowiednio autoryzowany (autentykacja) w najbliższej stacji, co zapewnia podstawowe zabezpieczenie przekazywanych informacji. Niestety taka organizacja transmisji umożliwia przeprowadzenie kilku rodzajów ataków. Podsłuch bezpośredni ze względu na małą siłę używanego algorytmu ustalania klucza oraz algorytmu szyfrowego jest możliwy w czasie rzeczywistym. Urządzenie do przechwytywania sygnału GSM (IMSI-Catcher) może na przykład zostać umieszczone w pobliżu osoby inicjującej połączenie. Dochodzi wtedy do jego przekierowania na to urządzenie, które symuluje BTS. IMSI-Catcher umożliwia więc połączenie z dowolnym telefonem komórkowym, który wykorzystywany będzie jako urządzenie podsłuchowe. Następnie sygnał zostanie przekazany do odpowiedniej stacji BTS. Tym sposobem, jednocześnie możliwe jest podsłuchiwanie kilkudziesięciu rozmów, nawet w dużej odległości od urządzenia podsłuchowego. Obecnie wyposażenie umożliwiające prowadzenie takiego podsłuchu jest stosunkowo drogie, trwają jednak prace nad takim urządzeniem opartym na powszechnej licencji publicznej GNU (*GNU General Public License*), którego koszt wykonania nie przekroczy 1 tys. USD. Większej wiedzy i inwestycji rzędu kilkunastu tysięcy złotych wymaga podsłuch na międzycentralowych łączach telekomunikacyjnych, który może zostać założony pomiędzy stacją BTS a kontrolerem BSC. Na tym trudności się kończą, ponieważ łączność ta nie jest szyfrowana. Ostatnią formą przechwycenia informacji jest włączenie się do centrali, lecz ten sposób ma inną specyfikę, ponieważ wiąże się z fizycznym dostępem do urządzeń telekomunikacyjnych, a tym samym najistotniejszy jest czynnik ludzki. W skrócie tak wyglądają ogólne zasady przechwytywania rozmów prowadzonych za pośrednictwem telefonów komórkowych.

Metody szyfrowania i transmisji szyfrowanych rozmów telefonicznych

Generalnie, gdy wiemy już jak działają podsłuchy, należy przyjąć, że najpewniejszym zabezpieczeniem informacji przekazywanych za pośrednictwem telefonów komórkowych jest zaszyfrowanie całego toru telekomunikacyjnego pomiędzy użytkownikami końcowymi. Obecnie dostępne są na rynku dwa typy rozwiązań, które przeznaczone są docelowo dla:

1) Biznesu lub użytkowników prywatnych, czyli telefony GSM, smartfony lub urządzenia PDA działające z wykorzystaniem standardowych systemów operacyjnych (Symbian, Windows Mobile lub Linux), na których instalowane są specjalne aplikacje realizujące połączenia szyfrowane. Rozwiązanie to stanowi w nich typowo jeden z wielu możliwych dodatków.
2) Służb specjalnych, Policji i wojska, czyli specjalnie zaprojektowane urządzenia (telefony) przeznaczone do realizacji połączeń szyfrowanych. Posiadają one rozbudowane zabezpieczenia, zazwyczaj kosztem funkcjonalności oraz ergonomii użytkowania.

Biorąc pod uwagę zakres mojego artykuły opiszę tylko pierwszą grupę tych rozwiązań na przykładzie kilku produktów firm z Wielkiej Brytanii, Niemiec i Polski.

Magazyn biznesowy „Fortune” zamieścił niedawno zestawienie najszybciej rozwijających się przedsiębiorstw na świecie, w którym na pierwszym miejscu znalazła się kanadyjska firma Research In Motion (RIM) produkująca smartfony BlackBerry. W poprzednich latach przedsiębiorstwo to w ogóle nie znalazło się na liście 100 najprężniejszych firm, którą opracowują dziennikarze tego magazynu. W 2009 roku na corocznym forum Wireless Enterprise Symposium[3] w Orlando na Florydzie, które organizowała RIM, angielska firma Cellcrypt zademonstrowała oprogramowanie do szyfrowania rozmów telefonicznych w czasie rzeczywistym, prowadzonych za pomocą urządzenia BlackBerry Bold.

Szyfrowanie rozmów odbywa się przy wykorzystaniu procesora zainstalowanego w smartfonie, tak więc aplikacja Cellcrypt Mobile for BlackBerry nie potrzebuje dodatkowego urządzenia (np. Smartcard). W tym oprogramowaniu zastosowano wiele różnych technik kryptograficznych. Producent wymienia: szyfrowanie asymetryczne RSA[4] i bazujące na krzywych eliptycznych ECDH (*Elliptic Curve Diffie-Hellman*)[5] z 2048-bitowym kluczem służącym do uwierzytelniania. Dla każdej rozmowy tworzone są nowe klucze sesji, które po wykorzystaniu są niszczone. Właściwe pakiety z danymi rozmowy są kodowane najpierw za pomocą 256-bitowego szyfru AES (*Advanced Encryption Standard*)[6], a potem raz jeszcze za pomocą 256-bitowego RC4 (*Rivest Cipher 4*)[7]. Integralność przesyłanych danych gwarantuje zastosowanie kryptograficznych funkcji skrótu[8] SHA-512 (*Secure Hash Algorithm*)[9] i MD5 (*Message-Digest algorithm 5*)[10]. Według firmy Cellcrypt oprogramowanie jest obecnie poddawane procesowi certyfikacji według standardu FIPS 140-2[11].

Program Cellcrypt przesyła rozmowy telefoniczne nie przez tradycyjną sieć głosową, ale przez tzw. telefonię internetową – VoIP (*Voice over Internet Protocol*), używając usługi transmisji danych operatora. Program nie może więc działać bez odpowiednich usług dostarczanych przez dostawcę telefonii. Zastosowanie VoIP jest o tyle interesujące, że firma RIM ani teraz, ani wcześniej nie udostępniała interfejsu programowania aplikacji API (*Application Programming Interface*) do VoIP, w związku z czym Cellcrypt sama musiała stworzyć odpowiednie funkcje. Portal „Heise Online” zacytował wypowiedź szefa Cellcrypt Simona Bransfield-Gartha, który stwierdził, że do prowadzenia rozmowy w typowej jakości sieci komórkowej wystarczy szerokość pasma w granicach 13 kbps. Urządzenie może więc działać również w konwencjonalnych sieciach GPRS.

---

[3] http://www.attendwes.com.

[4] *RSA* – asymetryczny system kryptograficzny opracowany w 1978 r. przez Ronalda Rivesta, Adiego Shamira i Lena Adlemana, w którym wykorzystano fakt, że można bardzo szybko mnożyć przez siebie dwie duże liczby pierwsze, natomiast nie ma algorytmu rozkładania w krótkim czasie otrzymanych iloczynów na czynniki

[5] *ECDH* – metoda szyfrowania oparta na kluczach publiczno-prywatnych, która została ogłoszona publicznie przez Whitfielda Diffiego i Martina Hellmana w 1976 r.

[6] *AES* – symetryczny szyfr blokowy przyjęty w wyniku konkursu ogłoszonego w 1997 r. przez National Institute of Standards and Technology (amerykańską agencję federalną pełniącą funkcję zbliżoną do Głównego Urzędu Miar w Polsce), jako standard opublikowany w Federal Information Processing Standards (FIPS-197)

[7] *RC4* – jest popularnym szyfrem strumieniowym opracowanym przez Rona Rivesta z RSA Security w 1987 r., który używany jest np. w protokołach SSL oraz WEP

[8] funkcja skrótu kryptograficznego jest to funkcja, która na podstawie pewnego tekstu głównego generuje relatywnie krótki tekst lub liczbę – zwaną sumą kontrolną, a związane w pewien sposób z tym tekstem głównym

[9] *SHA* – rodzina powiązanych ze sobą kryptograficznych funkcji skrótu zaprojektowanych przez amerykańską agencję National Security Agency i publikowanych przez National Institute of Standards and Technology

[10] *MD5* – algorytm kryptograficzny (kryptograficzna funkcja skrótu) opracowany przez Ronalda Rivesta w 1991 r., który z dowolnego ciągu danych generuje 128-bitowy skrót

[11] *FIPS 140-2* – amerykańska norma bezpieczeństwa wobec systemów kryptograficznych (zobacz przyp. 6)

Program Cellcrypt for Mobile szyfruje na zasadzie end-to-end, w związku z czym aparat odbierający rozmowę musi być również wyposażony w to oprogramowanie. Specjalna magistrala Cellcrypt umożliwia także prowadzenie rozmów z abonentami sieci stacjonarnych. Połączenia między dwoma urządzeniami BlackBerry – podobnie jak w rozmowie VoIP prowadzonej przez SIP (*Session Initiation Protocol*) – są przekazywane przez serwer firmy Cellcrypt. Oprogramowanie to jest licencjonowane, a za uzyskanie SMS-em linku umożliwiającego pobranie programu licencjobiorca musi zapłacić 1 tys. USD za jedno urządzenie, na okres jednego roku. Dla porównania oprogramowanie Mobile 3.2 tej samej firmy, dedykowane dla systemu operacyjnego Symbian S60 stosowanego w telefonach Nokii serii E i N, w 2008 roku kosztowało 500 GBP za jeden telefon, przy czym konfiguracja minimalna to dwa takie urządzenia.[12]

Globalizacja wpływa na rozwój przedsiębiorstw, a tym samym wzrasta konkurencja, która zaostrza metody działania ich kierownictwa. Umożliwienie bezpiecznego porozumiewania się w biznesie ma ogromne znaczenie nie tylko w trakcie prowadzenia negocjacji handlowych. Zabezpieczenie informacji, które przekazywane są pomiędzy pracownikami jednej firmy może mieć również wpływ na ograniczenie ich wypływu do środków masowego przekazu. Często przecież zbyt wczesne upublicznienie niektórych danych może wpłynąć na sytuację na giełdzie, a tym samym na sytuację firmy.

Innym przykładem szyfrowania tego rodzaju rozmów jest urządzenie Secuvoice Card w wersji 1.0, opracowane przez niemiecką firmę Secusmart. Jest to mała karta, która po włożeniu do aparatu telefonicznego i przy pierwszym uruchomieniu Secuvoice, automatycznie instaluje oprogramowanie Secuvoice Application. Urządzenie to jest kompatybilne z telefonami Nokii posiadającymi gniazdo microSD. Producent informuje, że dotyczy to przede wszystkim aparatów serii E i N. Natomiast w czasie rocznej lub dwuletniej licencji można bez problemu zmieniać telefony. No i co jest ważne, z telefonu można korzystać w trybie normalnym lub utajnionym. Ponadto wszystkie inne aplikacje pozostają dostępne.

Transmisja danych odbywa się w oparciu o bezpieczną (nietransparentną) usługę GSM-CSD (*Circuit Switched Data*)[13], która w przeciwieństwie do zwykłej usługi GSM-CSD lub 3G dostępna jest wszędzie, gdzie dociera zasięg sieci świadczącej usługi GSM. Połączeniom za pośrednictwem CSD zarzuca się jednak, że ulegają przerwaniu, jeśli użytkownik telefonu porusza się z prędkością powyżej 80 km/h oraz występują pewne ograniczenia w połączeniach roamingowych, które dodatkowo wiążą się z wysokimi opłatami. Niektórzy operatorzy ograniczają możliwość odbierania połączeń z danymi CSD, a w wyniku zakazu wydanego przez Departament Bezpieczeństwa Wewnętrznego USA, system CSD nie jest dostępny w tym kraju. W przypadku wszystkich rozwiązań CSD, czas nawiązywania połączenia trwa co najmniej 30 s. Oprogramowanie tej firmy również działa na zasadzie end-to-end.

Bazowa platforma bezpieczeństwa wykorzystuje algorytm opracowany przez niemiecki Federalny Urząd ds. Bezpieczeństwa w Technikach Informacyjnych (*BSI – Bundesamt für Sicherheit in der*

[12] http://www.idg.pl/news/151378/Komorki.bez.podsluchu.html.

[13] *CSD* – transmisja danych z wykorzystaniem komutacji łączy. Technologia, dzięki której możliwe jest przesyłanie w sieci GSM danych z prędkością 9.6 kb/s (od i do użytkownika). Podczas przesyłania danych, używane są te same kanały radiowe, które mogą być użyte podczas transmisji głosu. Kanały te zajęte są cały czas podczas nawiązanego połączenia, nawet w momencie, gdy transmisja się nie odbywa (np. użytkownik zapoznaje się z treścią strony WAP). Opłata pobierana jest więc za czas, w którym połączenie jest aktywne, a nie za faktycznie przesłaną ilość danych.

Informationstechnik). Rozmowy mogą być chronione z wykorzystaniem 128-bitowego algorytmu szyfrowania danych AES i ECDH z 2048-bitowym kluczem. Koszt urządzenia to ok. 2,2 tys. USD.

W 2009 roku na targach nowych technologii CeBIT (*Centrum der Büro- und Informationstechnik*) w Hanowerze, w których udział wzięło 4,3 tys. wystawców z 69 krajów, niemiecka firmę Rohde & Schwarz zademonstrowała innego rodzaju urządzenie służące do zabezpieczania rozmów prowadzonych przez telefony komórkowe. Koncern ten zaprezentował TopSec Mobile, który z wyglądu przypomina mały (99 x 34 x 22 mm; waga – 55 g) telefon komórkowy lub pamięć USB (*PenDrive*). Charakterystyczna cecha odróżniająca to urządzenie od wcześniej omawianego polega na zastosowaniu modułu Bluetooth, który przesyła zaszyfrowaną rozmowę do telefonu użytkownika. Warunkiem jest jednak, aby telefon komórkowy wykorzystywany do tego rodzaju rozmów posiadał uruchomioną nietransparentną usługę GSM-CSD i funkcję Bluetooth (wersji 1.2 lub starszą) z profilem usług modemowych DUN (*Dial-up Networking Profile*) do szyfrowania transmisji. Najnowocześniejsze telefony posiadają już te funkcje. Jak widać rozwiązanie to posiada pewne elementy wymienione w powyższych przykładach, ale wprowadzone zostało dodatkowe połączenie w torze telekomunikacyjnym, a jak już wspomniałem wcześniej nie jest to korzystne z punktu widzenia bezpieczeństwa przesyłanych informacji. Także samo szyfrowanie przeprowadzane jest przy wykorzystaniu słabszych algorytmów. Producent podaje, że utajniana informacja szyfrowana jest przy użyciu 128-bitowego algorytmu, natomiast klucz połączenia generowany jest według asymetrycznego algorytmu 1024-bitowego. Cena takiego rozwiązania sięga 1,8 tys. USD.

Polska firma TechLab 2000 Sp. z o.o. zajmująca się m.in. produkcją urządzeń pomiarowych i szyfrujących, opracowała telefon Xaos Gamma, który jest szyfrującym aparatem komórkowym przeznaczonym do pracy w standardowej sieci GSM, w tym również w roamingu. Aparat realizuje typowe dla telefonów komórkowych funkcje, a ponadto umożliwia szyfrowanie połączeń głosowych, wiadomości tekstowych i transferu danych. Wszystkie funkcje kryptograficzne wkomponowane zostały w standardową funkcjonalność telefonu GSM. Cechuje go szybkość nawiązywania połączenia szyfrowanego rzędu ok. 1,5 s, opóźnienie głosu przy połączeniu szyfrowanym – 450 ms i kryptografia symetrycznym algorytmem szyfrującym AES-256 oraz uzgadnianie kluczy sesyjnych według schematu Diffie-Hellmana. Zastosowano także uwierzytelnianie kluczy sesyjnych według funkcji skrótu SHA-256. Przy realizacji połączenia szyfrowanego w pierwszej kolejności ustalane są klucze szyfrujące, osobno dla każdego połączenia, które niszczone są niezwłocznie po jego przerwaniu. Klucze są nieprzewidywalne, niezależne i nie wynikają z wewnętrznej struktury i oprogramowania. Jednocześnie zastosowano mechanizmy kontrolne uniemożliwiające niezauważony atak metodą „man in the Middle", która jest jedyną realną możliwością ataku na ten algorytm. Takich metod szyfrowania nie wolno wykorzystywać m.in. w Rosji, na Białorusi, w Turcji, Arabii Saudyjskiej czy Chinach.

TechLab 2000 Sp. z o.o. oparła swój produkt na transmisji w transparentnym trybie GSM-CSD. Mimo wszystkich braków usługa ta zapewnia najwierniejszy przekaz danych, ponieważ dane w drodze nie są traktowane jako głos i nie są kompresowane, ale zdarza się również, że występują w nich przekłamania. Cały montaż, uruchamianie i kontrola jakości działania odbywają się w Polsce, natomiast obudowy importowane są z Finlandii. Xaos Gamma ma wygląd typowego telefonu, pozbawiony został jednak dodatków, takich jak radio, odtwarzacz mp3, aparat fotograficzny, kamera filmowa, dostęp do Internetu oraz możliwości przesyłania wiadomości MMS. Konstruktorzy telefonu uważają, że powinien on zainteresować przede wszystkim drugą grupę odbiorców wymienionych na

wstępie, ale również w niektórych branżach działalności gospodarczej może znaleźć wykorzystanie, dlatego też pozwoliłem sobie o nim napisać.

Podsumowanie

Każdy z tych wariantów różni się przede wszystkim sposobem transmisji danych. Jedne wykorzystują telefonię internetową, inne nietransparentną lub transparentną transmisję danych z wykorzystaniem komutacji łączy. Natomiast sposób szyfrowania jest zbliżony i wykorzystuje hybrydowe systemy kodowania, w których klucz do szyfrowania symetrycznego jest przekazywany jako wiadomość zakodowana kluczem publicznym. Pomimo, iż telefonom komórkowym wyposażonym w funkcję szyfrowania danych, które wykorzystują rozbudowane, powszechne i otwarte systemy operacyjne można zarzucić, że wystawiają aplikację szyfrującą rozmowy na wszelkiego rodzaju ataki przy użyciu oprogramowania złośliwego i szkodliwego, to jednak równocześnie dysponują szerokim spectrum funkcji biurowych, których nie posiadają profesjonalne telefony do rozmów niejawnych. Prawdą jest również, że klucze kryptograficzne generowane są na bazie, często prymitywnych, ciągów pseudolosowych, które zmniejszają rzeczywistą siłę zastosowanych algorytmów szyfrujących poprzez znaczne ograniczenie przestrzeni kluczy. Ponadto w standardowym telefonie może bez naszej wiedzy zostać zainstalowana aplikacja szpiegująca, która umożliwi podsłuchiwanie rozmów prowadzonych w zasięgu wbudowanego w telefonie mikrofonu, nawet kiedy uważamy, że telefon jest wyłączony. Jednak to użytkownik powinien sam rozważyć, jakie rozwiązanie jest dla niego optymalne – jeśli jest konieczne – ponieważ obecnie znany jest już wielomianowy algorytm faktoryzacji liczb (algorytm Shora[14]), który zastosowany do odszyfrowania danych zakodowanych przy pomocy algorytmów opartych na faktoryzacji, odszyfruje każdą informację. Oczywiście jakiś czas będziemy jeszcze używać obecnie produkowanych urządzeń szyfrujących, ponieważ praktycznie nie ma odpowiedniego komputera kwantowego, który jest niezbędny do zastosowania algorytmu Shora. W przypadku wynalezienia komputerów kwantowych większość algorytmów używanych obecnie w kryptografii będzie bezużyteczna.

[14] *Algorytm Shora* – algorytm ten stanowi potencjalne zagrożenie dla systemu kryptograficznego RSA, ponieważ klucz publiczny w RSA jest iloczynem dwóch dużych liczb pierwszych, a możliwość efektywnego odtworzenia tych liczb na podstawie klucza publicznego pozwalałaby poznać klucz prywatny i tym samym złamać cały szyfr. Jest to algorytm probabilistyczny: zwraca poprawną odpowiedź jedynie z pewnym prawdopodobieństwem, ale w przypadku możliwości szybkiego sprawdzenia odpowiedzi, powtarzanie algorytmu umożliwia uzyskanie poprawnej odpowiedzi w sposób efektywny z dowolnie dużym prawdopodobieństwem. Został opublikowany przez Petera Shora w 1994 r., natomiast w 2001 r. grupa informatyków z firmy IBM i Uniwersytetu Stanforda zademonstrowała jego działanie na 7-kubitowym komputerze kwantowym opartym o jądrowy rezonans magnetyczny.

Spółka: http://so.pwn.pl/zasady.php?id=629569