Prywatność w sieciach bezprzewodowych Wi-Fi, Bluetooth, ZigBee oraz RFID

Igor Margasiński, Krzysztof Szczypiorski
Politechnika Warszawska, Instytut Telekomunikacji
e-mail: igor@margasinski.com, krzysztof@szczypiorski.com

Streszczenie

Celem referatu jest przedstawienie zagadnień bezpieczeństwa w najpopularniejszych sieciach bezprzewodowych LAN (Wi-Fi - IEEE 802.11a/b/g) oraz PAN (Bluetooth – IEEE 802.15.1, ZigBee - IEEE 802.15.4) pod kątem zagadnień związanych z prywatnością. Dla każdego z systemów zostanie przedstawiony zarys architektury bezpieczeństwa oraz znane podatności. Nieskuteczność zabezpieczeń kryptograficznych doprowadziła do tego, że jedynym prawie pewnym zabezpieczeniem są torby na urządzenia bezprzewodowe (PDA, GPS, karty chipowe, telefony komórkowe) wykonane z materiałów skutecznie tłumiących fale radiowe (np. 80 dB w paśmie 10 MHz-20 GHz). Dodatkowo w referacie zostanie poruszona kwestia RFID (Radio Frequency IDentification) jako metody oznaczania towarów za pomocą bezprzewodowych metek. Pasywne RFID nie zawierają źródeł zasilania, natomiast aktywne mogą bazować na rozwiązaniach klasy LAN i PAN – tak jedne, jak i drugie stanowią potencjalne źródło pogwałcenia prywatności.

And through the wire you are secure
- Peter Gabriel

1 Tło

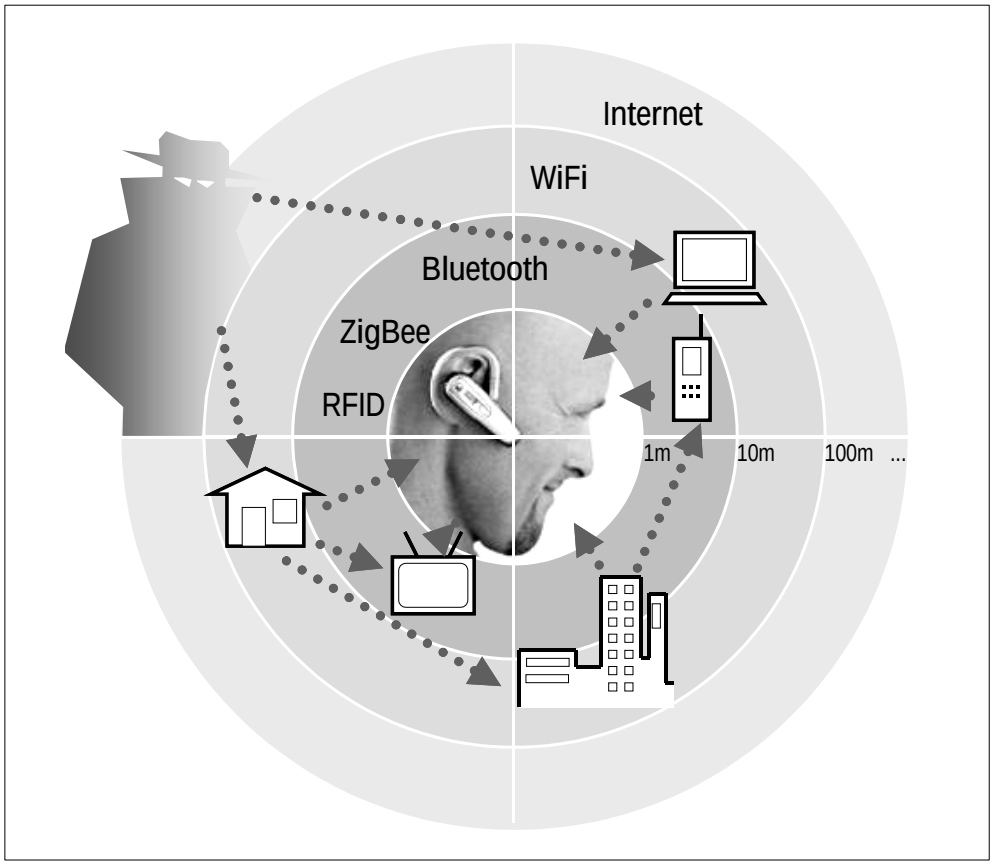
Możliwość wszechstronnego zapewnienia prywatności w sieciach telekomunikacyjnych staje się w ostatnich latach coraz realniejsza. Techniczna ewolucja, która nastąpiła przez ostatnie ćwierć wieku, z apogeum przypadającym na początek obecnego stulecia, spowodowała odejście klasycznej telekomunikacji na rzecz technologii IP. Klasyczna telekomunikacja, mimo że zbudowana według modelu odniesienia **dla systemów otwartych** (OSI RM) paradoksalnie oparta jest na zamkniętych, jeśli chodzi o rozszerzenia, standardach. Bezpieczeństwo w klasycznej telekomunikacji jest złośliwym dodatkiem, na który przeważnie nie ma już miejsca, wypada je jednak traktować jako wyrafinowaną usługę dla specyficznego klienta, nawet jeśli operator nie zamierza go szukać. Technologia IP, wyśmiewana przez wiele lat przez „ekspertów od prawdziwej telekomunikacji" ze względu na swoją niedoskonałość i brak standaryzacji, stała się twórczym katalizatorem zmiany w podejściu do realizacji wielkich idei, takich jak przesyłanie głosu w sieciach pakietowych (IP Telephony), uwierzytelnienie czy poufność (IPsec).

Można zaryzykować stwierdzenie, że sieci IP są samodzielnymi bytami w zasadzie niezależnymi od konstrukcji niższych warstw sieci. Warto jednak zwrócić uwagę na obłędny wyścig przepływności w budowie tzw. szerokopasmowego dostępu do sieci IP, który doprowadził do klonowania techniki Ethernet i tworzenia coraz to nowszych jego instancji (szybszych 10-krotnie), jako lekarstwa na całe zło. „Ethernet wszędzie" to proste uniknięcie problemów związanych z łączeniem sieci lokalnych, a także nieświadomy inkubator współczesnych sieci bezprzewodowych, w szczególności IEEE 802.11 (Wireless LANs).

Sieci bezprzewodowe uwolniły terminale klientów od biurek. Dzięki nim użytkownicy otrzymali dostęp do sieci IP z każdego miejsca, które jest w zasięgu, nawet z miejsca, do którego król sam chodzi piechotą. Ludzka potrzeba ulepszania rzeczy dobrych doprowadziła do eksplozji tej gałęzi telekomunikacji i wykreowania bytów niezależnych zarówno od technologii Ethernet, jak i technologii IP. Nie ulega wątpliwości, że nowe sieci bezprzewodowe stanowią nowe wyzwania dla metod ochrony informacji. Dobrze, że wśród twórców nowych standardów dominuje pogląd, że współczesną telekomunikację należy od samego początku projektować tak, aby było zapewnione elementarne bezpieczeństwo (tj. integralność danych, poufność i uwierzytelnienie). Uniknie się w ten sposób tworzenia kuriozalnych potworków, dla których ochrona informacji jest niewygodna, ale jednocześnie stanowi tzw. killer application.

Wycieczka w stronę fal radiowych niesie za sobą zerwanie z paradygmatem bezpiecznych kabli, wtyczek i niewinnie komutujących urządzeń sieciowych. Ta wycieczka to zaproszenie do zmagania się z nowoczesną (ale często niepoprawnie zastosowaną) kryptografią, która pojawia się w powietrzu albo, co jest nagminne, nie pojawia się wcale. Powszechne traktowanie przez producentów sprzętu użytkowników nowoczesnych rozwiązań jak kompletnych idiotów doprowadziło do sytuacji, w której wszystko, co wyjmuje się z pudełka musi działać.

Nie zamierzamy w tym artykule nikogo zmuszać do tego, aby używał rozwiązań bezpiecznych, nie będziemy zbyt ostro piętnować użytkowników urządzeń wyjętych z pudełka. Pragniemy zwrócić uwagę na problemy bezpieczeństwa w najpopularniejszych sieciach bezprzewodowych LAN (Wi-Fi - IEEE 802.11a/b/g) oraz PAN (Bluetooth, ZigBee - IEEE 802.15.4) pod kątem zagadnień związanych z prywatnością. Dodatkowo w artykule przedstawimy technikę RFID (Radio Frequency IDentification) jako metodę oznaczania towarów za pomocą bezprzewodowych metek.



Rys. *1*. Technologie bezprzewodowe ułatwiają codzienne czynności; pozostawione bez kontroli – ułatwiają śledzenie codziennych czynności

1.1 Człowiek

Zmierzamy do świata, gdzie komunikacja cyfrowa nie wymaga rozpinania kabli i gdzie nie trzeba zastanawiać się nad doborem odpowiednich wtyczek (*don't plug - just play*). Fale radiowe stanowią wszechobecne medium, szeroko zagospodarowane przez współczesne protokoły telekomunikacyjne. Zwalniani jesteśmy nie tylko z wysiłku fizycznego łączenia węzłów sieci, ale również marginalizujemy zadania konfiguracyjne samych urządzeń. Producenci małych, przenośnych terminali często ograniczają możliwości konfiguracji do włączenia lub wyłączenia łączności w ramach określonej technologii bezprzewodowej (takiej jak **Bluetooth**). Dyżurnym usprawiedliwieniem jest zazwyczaj mały rozmiar wyświetlacza i ograniczona liczba przycisków. W powszechnym zastosowaniu znalazły się podręczne terminale pełniące rolę osobistych asystentów. Chcemy, by telefon nie służył jedynie do prowadzenia rozmów głosowych, ale by był osobistym, zawsze obecnym pomocnikiem. Powinien mieć obszerne zasoby pamięci, mocy obliczeniowej i posiadać wszystkie popularne interfejsy bezprzewodowe. Poręczny, elektroniczny terminal powinien zapamiętać pomysły, przyjmować notatki i informacje kontaktowe. Ma pozwalać na komunikację w zakresie współczesnych usług, takich jak poczta elektroniczna, nawigacja WWW, telefax i inne. Ma pomagać w odnajdywaniu czasu (funkcja terminarza) i ułatwiać odnajdywanie się w przestrzeni (**GPS** – Global Positioning System). W skrócie ma być oknem na świat – chowanym w kieszeni. Urządzenia typu **PDA** (Personal Digital Assistant), stanowią już dziś środek uzależniający – to uniwersalny i scentralizowany interfejs cyfrowy ze światem. Osoby dłużej stosujące terminale PDA często, po ich utracie, doświadczają poważnego zgubienia i nie są w stanie efektywnie pracować. Powszechnie wyposażamy się w cyfrowe **alter-ego**, któremu powierzamy pieczę nad codziennymi czynnościami i które **skupia informacje o nas**.

1.2 Aglomeracje

W interfejsy bezprzewodowe wyposażamy nie tylko urządzenia nam towarzyszące, ale również otaczające nas środowisko – instalacje budynków, oraz szerzej – tereny skupisk ludzkich. Atrakcyjne wydają się możliwości sterowania np. instalacją elektryczną, grzewczą, klimatyzacją pomieszczeń, czy systemem alarmowym, bez udziału kabli (m.in. standard ZigBee). Pożądane jest także, by budynki i miejsca, w których przebywamy, istniały również w sensie wirtualnym – istniały w sieci. W każdym miejscu chcemy mieć kontakt z siecią Internet. Mówi się żartobliwie, że jeśli czegoś nie ma w sieci, to nie istnieje naprawdę. Okazuje się jednak, że już całkiem poważnie brany jest pod uwagę czynnik bezprzewodowego dostępu do sieci (Wi-Fi) przy wyborze miejsca odpoczynku, a nawet przy zakupie nieruchomości. Połączenie tych dążeń oznacza możliwości sterowania np. oświetleniem domu, systemami antywłamaniowymi lub nowo zakupionym zestawem kina domowego, z dowolnego skrawka cywilizacji na świecie.

1.3 Przedmioty

Na tym nie koniec. Poza nami samymi i miejscami, w których przebywamy, pozostaje jeszcze niezliczona liczba przedmiotów, dóbr, którymi otacza się człowiek. W tym wymiarze również obserwujemy indeksacje rzeczywistości, digitalizację obrazującą tęsknotę za owymi przedmiotami w wymiarze wirtualnym. Liczne produkty zaopatrywane są w elektroniczne znaczniki umożliwiające bezprzewodową lokalizację, zapis i odczyt informacji (**RFID** – Radio Frequency IDentification). Możliwość śledzenia bagażu podróżnego wydaje się bardzo korzystna. Stosowanie identyfikatorów RFID w samochodach może oznaczać skuteczną ochronę przed kradzieżą pojazdu, a także może być praktycznym sposobem realizacji kontroli dostępu i opłat na płatnych odcinkach dróg. Jaka jest cena? Globalna identyfikacja i techniczne środki **automatycznego śledzenia** rysują się w zasięgu ręki. Wszczepianie ludziom podobnych znaczników też nie jest już fikcją, a nawet jest związane z modą, określającą styl bycia w określonych środowiskach.

2 Nowe możliwości i zagrożenia

Sukces technologii bezprzewodowych oznacza nowe, zdumiewające możliwości. Szerokie spektrum dziedzin życia, w które ingerują technologie bezprzewodowe, kreuje globalne środowisko cyfrowego opisu codziennych czynności społeczeństwa. Powszechne dążenie do integracji technologii to włączenie bezprzewodowych sieci o małym zasięgu do globalnej komunikacji IP. Posiadanie dostępu do informacji skupionych w powszechnie stosowanych sieciach bezprzewodowych staje się bardzo cennym orężem – od skutecznej promocji produktów do wpływania na konsumentów i upowszechniania poglądów.

2.1 Bluetooth

Standard *Bluetooth* należy do technologii łączności na małe odległości i jest zaliczany do bezprzewodowych sieci osobistych WPAN (Wireless Personal Area Network). Został stworzony z myślą o budowaniu bezprzewodowych, tanich pomostów ad-hoc, integrujących sprzęt cyfrowy w najbliższym otoczeniu. Dużą popularnością cieszą się obecnie telefony, przenośne komputery typu notebook i PDA wyposażone w takie interfejsy. Technologia została objęta standaryzacją IEEE. Norma 802.15.1 specyfikuje warstwę fizyczną i łącza danych. **W warstwie łącza danych umiejscowiono usługi bezpieczeństwa** – uwierzytelnienie i poufność. Oznacza to, że ochrona komunikacji zapewniana jest w relacji pomiędzy sąsiadującymi węzłami. Węzły tworzą grupy ad-hoc zwane *piconet*-ami. Owa sieć (do 8 węzłów) zawiera jedną stację synchronizująca, zwaną *master* i pozostałe *slave*. Niezależne sieci „skali piko" - *piconets* mogą być dalej łączone w „rozrzucone sieci" – *scatternet*s. **Każdy węzeł posiada niepowtarzalny adres**. Opcjonalne **uwierzytelnienie** stron (zwane procesem parowania – *pairing*) opiera się na wykazaniu się wiedzą o kodzie PIN (do szesnastu znaków ASCII). Na tej podstawie generowane są 128 bitowe klucze (*link key*). Przebieg uwierzytelnienia ma schemat wyzwanie-odpowiedź, w którym strony posługują się niepowtarzalnymi adresami stacji i kluczami *link key*s. **Poufność** zapewniana jest poprzez szyfrowanie łącza za pomocą szyfru strumieniowego typu liniowego rejestru przesuwnego ze sprzężeniem zwrotnym (Linear Feedback Shift Registers – LFSR). Kontrola dostępu związana jest z podziałem węzłów na dwie grupy: zaufane – uprawnione do pełnego dostępu do zasobów, oraz na nie zaufane – o ograniczonych prawach. Przyporządkowanie do jednej z grup odbywa się w procesie uwierzytelnienia. Urządzenia mogą pracować w jednym z trzech poziomów bezpieczeństwa (*security mode*). W zależności od wybranego poziomu stosowane są odpowiednie usługi bezpieczeństwa.

Przy powszechnym zastosowaniu standardu Bluetooth, jako łączności w „relacjach osobistych" (Personal Area Network), jest szczególnie istotna ochrona prywatności użytkowników. Świadomość, że dane urządzenie przedstawia się zawsze tym samym, niepowtarzalnym adresem, jest dużym powodem do niepokoju. W przypadku posługiwania się zawsze tym samym urządzeniem (np. telefonem lub terminalem PDA) jesteśmy łatwym celem śledzenia. Zwyczaje osób wyposażonych w elektroniczne alter-ego z interfejsem Bluetooth są

łatwe do poznania. Przewidywane było wprowadzenie do standardu trybu anonimowego, gdzie ukrywany byłby adres stacji. W obecnej wersji 2.0 nie zostało to jednak zrealizowane. Problem pogłębia konieczność wprowadzania kodów PIN przy generacji kluczy *link key*. Zarządzanie PIN-ami w obrębie większej sieci jest utrudnione. Ponadto w grupie urządzeń wspólnie komunikujących się, musi występować ten sam kod PIN. Ponownie, rozwiązanie wyraźnie wykazuje trudną skalowalność i obniżenie poziomu bezpieczeństwa dla większych sieci. Przechwycenie sekwencji PIN oznacza między innymi uzyskanie dostępu do wszelkich danych przechowywanych w urządzeniu. W efekcie sporządzany profil użytkownika może być powiązany ze szczegółowymi danymi osobowymi, danymi kontaktowymi itd. Globalne zastosowanie technologii Bluetooth stwarza dogodne środowisko do ingerencji w prywatność. Innym sposobem na uzyskanie pełnego dostępu do urządzenia jest kradzież dowolnego urządzenia, które zostało zaliczone do zaufanych w stosunku do obiektu ataku. Pamiętamy, że uwierzytelnienie dokonywane jest pomiędzy urządzeniami, a nie pomiędzy użytkownikami stacji.

Praktyka pokazała, że możliwości ingerencji w prywatność użytkowników Bluetooth są znacznie większe. Powodem jest zazwyczaj błędna i nieświadoma implementacja przez producentów sprzętu, w zakresie warstw wyższych. Większość sprzętu wyposażonego w interfejs *Bluetooth* jest podatna na szereg ataków. Najpopularniejsze to:

- ***bluesnarf*** – kopiowanie danych ze wskazanego urządzenia; w zależności od powodzenia fazy uwierzytelnienia, będą to wszystkie dane lub ich podzbiór zawierający książkę telefoniczną i terminarz; atak nie jest widoczny dla użytkownika atakowanej stacji,
- ***bluestumbler*** – monitorowanie urządzeń w zasięgu – odczyt parametrów: nazwa, adres urządzenia, moc sygnału, możliwości, producent sprzętu (na podstawie adresu),
- ***bluejacking*** – wysyłanie niepożądanych wiadomości do innych urządzeń *Bluetooth* (również w trybie rozgłoszeniowym – *broadcast*).

2.2 ZigBee

Młodszym standardem z zakresu bezprzewodowych sieci PAN jest ZigBee. Cechą wspólną ZigBee i Bluetooth jest zastosowanie ogólnodostępnej częstotliwości transmisji radiowej 2.4 GHz. Warstwa fizyczna oraz podwarstwa MAC objęte zostały standaryzacją IEEE pod nazwą 802.15.4. Kluczowym założeniem ZigBee jest maksymalna prostota i tani koszt implementacji. Aby zmniejszyć zużycie energii i uprościć implementacje, celowo ograniczono pasmo i wielkość stosowanych nagłówków. W efekcie ZigBee ma stać się powszechnie stosowaną technologią bezprzewodową rewolucjonizującą podejście do elektronicznych instalacji domowych. Ma zaspokajać potrzeby związane z automatyką w pomieszczeniach.

W podwarstwie MAC umiejscowiono usługi poufności, integralności i uwierzytelnienia ramek, w oparciu o znany z Wi-Fi protokół Counter Mode with CBC-MAC Protocol (CCMP). Bezpieczeństwo w relacji od końca do końca (analogiczne rozwiązania jak w podwarstwie MAC) nie jest objęte standaryzacją. Wydaje się, że podobnie jak w przypadku Bluetooth, wraz z upowszechnieniem się technologii stanie się to podstawowym problemem w bezpieczeństwie ZigBee.

Niski koszt urządzeń ma pozwolić na powszechne stosownie nawet bezprzewodowych włączników światła ZigBee i jako wyposażenie zabawek. Integracja z Wi-Fi i dalej z Internetem to możliwości zdalnego sterowania domostwami. Pokusa ataków jest ogromna. Brak kontroli nad mechanizmami bezpieczeństwa realnie rysuje wizję *Wielkiego Brata*.

2.3 Wi-Fi

W połowie lat 90. XX wieku twórcy technologii Wi-Fi postawili sobie zadanie stworzenia mechanizmu bezpieczeństwa dla sieci bezprzewodowych odpowiadającemu bezpieczeństwu przewodowego Ethernetu. Założenie to zamknięte w koncepcji Wired Equivalent Privacy (Odpowiednik Przewodowej Prywatności) stało się wzorcowym przykładem fatalnego wdrożenia prywatności. Recepta na klęskę była nad wyraz prosta:
Składnik 1) weź algorytm symetryczny, o którym panuje opinia, że jest kiepski (RC4),
Składnik 2) użyj kodu cyklicznego zamiast funkcji skrótu (CRC-32),
Składnik 3) nie zmieniaj kluczy kryptograficznych (brak zarządzania kluczami).

W przypadku użycia RC4 (Składnik 1) popełniono poważny błąd, który w połączeniu z brakiem zarządzania kluczami (Składnik 3) spowodował spektakularną kompromitacje WEP. Klucz WEP można „zgadnąć" przez obserwację początkowych bajtów szyfrogramu (nałożenie działania modulo 2 na stały element ramki MAC). W zależności od szczęścia i poziomu ruchu odgadnięcie nie zmienianego klucza może zająć od kilku minut do kilkudziesięciu godzin.

Brak dynamizmu w zmianie klucza postanowiono nadrobić tworząc tzw. łatkę na WEP, czyli TKIP (Temporary Key Integrity Protocol), protokół tworzący unikalny klucz dla każdej ramki 802.11. W ten sposób odgadnięcie klucza nie jest już możliwe. Rozwiązanie to można zastosować do urządzeń wspierających WEP poprzez zmianę sterownika, bądź firmware'u. W ten sposób także pozbyto się kiepskiej integralności – powstał nowy algorytm MICHAEL.

Poważniejsze i współczesne podejście do prywatności opiera się na protokole CCMP. Protokół ten wykorzystuje algorytm AES i nie ma nic wspólnego z WEP ani TKIP. Protokół implementuje także integralność. Wymaga jednak większych zasobów obliczeniowych, stąd wciąż jest niedostępny dla wielu kart bezprzewodowych i punktów dostępowych

Warto tutaj zwrócić uwagę, że część (czołowych!) wytwórców urządzeń IEEE 802.11 do końca nie dowierza mocy CCMP - pojawiają się urządzenia, które oferują pracę w trybie łączonym WEP+TKIP+CCMP. Bezradność wytwórców sprzętu w tworzeniu takich krzyżówek bierze się przede wszystkim z przekonania o historycznie krótkotrwałym żywocie mechanizmów zapewnienia prywatności w Wi-Fi.

Realizację prywatności w Wi-Fi oczywiście wspiera protokół IEEE 802.1X. Koncepcja wyniesienie inteligencji związanej z uwierzytelnianiem do specjalizowanych serwerów AAA spowodowała wreszcie możliwość stworzenia zaawansowanych mechanizmów zarządzania kluczami. IEEE 802.1X wraz z CCMP to główny trzon zalecanego przez Wi-Fi Alliance profilu WPA2 (Wi-Fi Protected Access 2), a także standardu IEEE 802.11i.

2.4 RFID

RFID to małe i proste układy elektroniczne, wyposażone w antenę. RFID może odbierać sygnały radiowe i wysyłać odpowiedź. Dodatkowo każdy RFID posiada niepowtarzalny identyfikator. RFID nie muszą być wyposażone w źródło zasilania, układ może wykorzystywać energię dostarczoną wraz z sygnałem nadawczym. Konstruowane są również układy RFID ze stałym zasilaniem.

RFID nazywane niekiedy mikroprocesorami szpiegującymi – *spychips* – pozwalają śledzić oznakowane przedmioty, zwierzęta i ludzi w zakresie zasięgu anten układów. W zastosowaniach komercyjnych znalazły się produkty z umieszczonymi w metce identyfikatorami RFID. Są już również stosowane urządzenia RFID wyposażone w miniaturowe kamery, określające profile klientów kupujących dane produkty.

Przy szerokim zastosowaniu identyfikatorów RFID, integracja z innymi technologiami bezprzewodowymi oznacza wytworzenie się środowiska umożliwiającego globalną i zautomatyzowaną inwigilację.

3 Perspektywy

Upowszechnienie się technologii bezprzewodowych wydaje się drugim, po Internecie, przełomem w dziedzinie prywatności elektronicznej. Nakazuje radykalną zmianę spojrzenia na ochronę prywatności. Nieskrępowane możliwości komunikacji za pomocą globalnej sieci IP zaowocowały eksplozją praktyk zautomatyzowanego śledzenia użytkowników sieci na szeroką skalę. Technologie bezprzewodowe rozwiązują problemy braku elastyczności w dostępie do Internetu. Pozwalają na dostęp do sieci niemalże z każdego miejsca. Wyposażanie siebie, a także domów i różnego rodzaju innych dóbr w interfejsy komunikacji bezprzewodowej wprowadza liczne obszary naszego życia w wymiar cyfrowy – ze wszystkimi skutkami ubocznymi. Dowolność i brak dbałości przez producentów o odpowiednią implementację mechanizmów bezpieczeństwa, otwiera pole do nadużyć na szeroką skalę i powszechne profilowanie.

Literatura

[1] Fluhrer S., Mantin I., Shamir A.: Weaknesses in the Key Scheduling Algorithm of RC4. Cisco and The Weizmann Institute, August 2001
[2] Gehrmann, Ch., Persson, J. Smeets, B., Bluetooth Security, Artech House, London 2004
[3] IEEE 802.11 Standard for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999
[4] IEEE 802.11b-1999 Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band
[5] IEEE 802.11i Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN

Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004
[6] IEEE 802.15.1 Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), 14 June 2002
[7] IEEE 802.15.4 Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), 1 October 2003
[8] Specification of the Bluetooth System Version 1.2, 5 November 2003
[9] Specification of the Bluetooth System Version 2.0 + EDR [vol 0], 4 November 2004
[10] Whiting, D., Housley, R. Ferguson, N. Counter with CBC-MAC (CCM), RFC 3610, September 2003

Artykuł recenzowany