STUDIA INFORMATICA 2014
Volume 35 Number 3 (117)

Tomasz BILSKI
Politechnika Poznańska, Instytut Automatyki i Inżynierii Informatycznej

SYSTEMY UWIERZYTELNIANIA POZAPASMOWEGO[1]

Streszczenie. Standardowe kanały komunikacyjne oparte na falach elektromagnetycznych nie mogą być uznawane za zaufane i autentyczne. Docierające do odbiorcy fale elektromagnetyczne mogą pochodzić ze źródeł, których istnienie może być ukryte przed odbiorcą. W ogólnym przypadku użytkownik odbierający takie sygnały nie jest w stanie określić ich pochodzenia i nie ma pewności co do tego, czy sygnały te pochodzą od określonego (zaufanego) nadawcy. Brak tej pewności może prowadzić do naruszeń bezpieczeństwa, takich jak podszywanie się czy podsłuch. Tak więc pojawia się potrzeba uwierzytelnienia urządzenia bezprzewodowego bez użycia zwykłego kanału komunikacyjnego opartego na falach radiowych. Artykuł stanowi przegląd metod uwierzytelniania pozapasmowego. Uwzględniono zarówno prace teoretyczne, standardy, jak i rozwiązania komercyjne.

Słowa kluczowe: sieci bezprzewodowe, uwierzytelnianie, uwierzytelnianie pozapasmowe, ustanawianie kluczy, kojarzenie urządzeń, efemeryczne kojarzenie urządzeń, ataki typu *man in the middle*

OUT-OF-BAND AUTHENTICATION SYSTEMS

Summary. Standard communication channels based on radio waves may not be considered safe. Signals that user receives may come from different places, which may be hidden. User is not able to determine the source of the signals. This may be used by illegitimate users to spoof or to sniff wireless channel. In order to authenticate the sender's wireless device one has to use additional out-of-band channel. The paper is a survey of out-of-band authentication methods and systems. Standards, theoretical works as well as commercial solutions have been presented.

Keywords: wireless networks, authentication, out-of-band authentication, key exchange, man in the middle attacks, ephemeral pairing problem

[1] Praca sfinansowana ze środków na projekt badawczy 04/45/DSPB/0105.

1. Wprowadzenie

1.1. Problemy uwierzytelniania w systemach bezprzewodowych

W tradycyjnym systemie komunikacji bezprzewodowej docierające do odbiorcy fale elektromagnetyczne mogą pochodzić z odległych źródeł, z różnych miejsc, których istnienie może być ukryte przed odbiorcą. Człowiek nie jest w stanie zidentyfikować miejsca pochodzenia sygnałów radiowych. Stosunkowo łatwe staje się przeprowadzenie takich ataków, jak MitM (ang. *Man in the Middle*). Oczywiste jest, że podobny problem istnieje w sieciach przewodowych – np. w przypadku komputera podłączonego do sieci Ethernet. Problem nie występuje tylko wtedy, gdy urządzenie jest podłączone przewodowo tylko do jednego innego węzła
i drugi koniec kabla jest widoczny. W wielu sytuacjach konieczne jest zagwarantowanie tego, że użytkownik kontaktuje się ze ściśle określonym innym urządzeniem.

Problem uwierzytelniania (kojarzenia urządzeń bezprzewodowych, a także problem ustanowienia wspólnego klucza kryptograficznego dla symetrycznego systemu kryptograficznego) jest często rozwiązywany z użyciem kryptografii asymetrycznej (Infrastruktury Kluczy Publicznych i Certyfikatów) lub zaufanej strony trzeciej (np. Kerberos). Dodatkowe możliwości daje wykorzystanie dynamicznych właściwości kanału radiowego. Na przykład, propozycję generowania wspólnego klucza z użyciem pomiaru RSS (ang. *Received Signal Level*) przedstawiono w [16]. Zwykle (np. w standardzie IEEE 802.11) uwierzytelnianie odbywa się z użyciem tego samego kanału komunikacyjnego (radiowego), który jest stosowany jednocześnie do innych celów (w tym do transmisji danych zarówno przed procesem uwierzytelnienia, jak i po uwierzytelnieniu).

Zastosowanie kryptografii w procesach uwierzytelniania wiąże się z wieloma problemami. Należą do nich: złożoność procesów zarządzania kluczami kryptograficznymi, niezbędna dodatkowa moc obliczeniowa (a także pamięć i energia) na procesy kryptograficzne. Problemy te są szczególnie istotne w przypadku środowiska bezprzewodowego, heterogenicznego i w przypadku użycia mobilnych urządzeń komunikacyjnych, wyposażonych we własne źródła zasilania. Wśród proponowanych rozwiązań jest zastąpienie procesu uwierzytelniania kryptograficznego przez specjalny system zagłuszania sygnałów, pochodzących z węzła podszywającego się [12], oraz wykorzystanie chaotycznego charakteru i nieprzewidywalności związanej z propagacją fal elektromagnetycznych w pomieszczeniu [11].

Dodatkowo, użycie infrastruktury kluczy publicznych lub zaufanej strony trzeciej do uwierzytelnienia jest możliwe pod warunkiem wstępnego istnienia urzędów certyfikacji oraz określonych relacji zaufania między podmiotami – w praktyce (zwłaszcza w systemach typu

ad hoc) relacje takie nie zawsze istnieją. Konieczne staje się zastąpienie kryptografii metodami ochrony w niższych warstwach stosu protokołów komunikacyjnych.

Warto w tym miejscu zaznaczyć, że także klasyczne zastosowania kryptografii do ochrony poufności danych w systemach bezprzewodowych są niekiedy zastępowane metodami z niższych warstw stosu TCP/IP. Zamiast szyfrowania danych można zastosować formowanie wiązki (ang. *Beamforming*) i kooperacyjne formowanie wiązki (ang. *cooperative beamforming*) lub odpowiedni przydział podnośnych (ang. *subcarrier allocation*) w systemach korzystających z techniki OFDMA (ang. *Orthogonal Frequency Division Multiple Access*) [6].

Ponadto, pasma fal radiowych, w szczególności pasma nielicencjonowane ISM (and. *Industry, Science, Medicine*), są obecnie wykorzystywane przez wiele różnych systemów komunikacji. Przykładowo, pasmo 2,4-2,5 GHz jest używane w takich systemach, jak: IEEE 802.11, Blutooth (IEEE 802.15.1), HomeRF, RFID, ZigBee (IEEE 802.15.4). Transmisja w tych pasmach jest narażona na interferencje, zakłócenia, a w skrajnych przypadkach występują przerwy w transmisji lub całkowite blokady kanałów komunikacyjnych.

Kolejnym aspektem transmisji w paśmie radiowym jest stosunkowo wysokie zużycie energii podczas transmisji, zarówno nadawania, jak i odbioru danych.

Zatem, niezbędne niekiedy staje się zastosowanie innych, prostszych i pozapasmowych metod kojarzenia urządzeń i uwierzytelniania lub wstępnego uwierzytelniania (ang. *pre-authentication*), metod których działanie i bezpieczeństwo może być zweryfikowane przez użytkownika (ang. *human-assisted device authentication*).

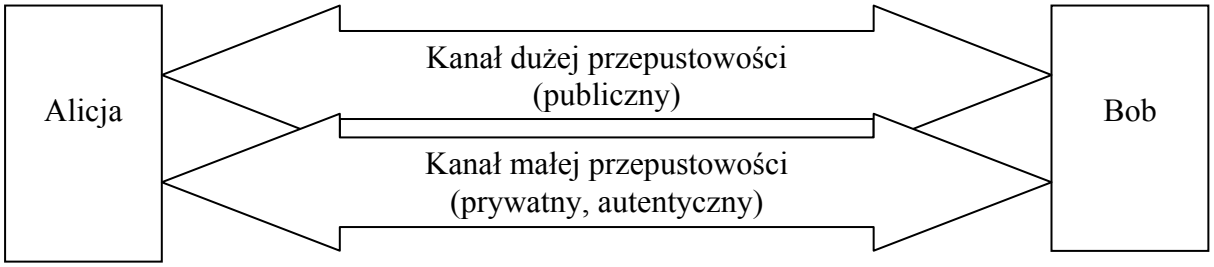
1.2. Model komunikacji uwierzytelniania pozapasmowego

Uwierzytelnianie pozapasmowe jest trybem uwierzytelniania, który wykorzystuje dodatkowy kanał komunikacyjny (poza głównym pasmem używanym do transmisji danych). Zakłada się, że cały proces komunikacji oparty jest na dwóch kanałach komunikacyjnych o różnych parametrach. Kanał komunikacyjny do normalnej transmisji danych charakteryzuje się wysoką przepustowością – jest to najczęściej kanał oparty na transmisji w paśmie mikrofalowym i jednocześnie niegwarantujący pełnego bezpieczeństwa dla procesów uwierzytelniania – dane związane z procesem uwierzytelniania i transmitowane tym kanałem muszą być weryfikowane, np. przez porównanie ich z danymi odebranymi za pomocą drugiego kanału.

Drugi, pozapasmowy kanał komunikacyjny nie musi mieć dużej przepustowości. Ma także niewielki zasięg (ang. *location limited channel*). W niektórych przypadkach wymaga się, aby urządzenia stykały się ze sobą. Kanał ten jest wykorzystywany wyłącznie do przesyłania informacji związanych z procesem uwierzytelnienia lub wstępnego uwierzytelniania.

W przypadku wstępnego uwierzytelniania dane przesłane tym kanałem w sposób bezpieczny są następnie wykorzystywane w procesie właściwego uwierzytelniania, który odbywa się z użyciem podstawowego kanału komunikacyjnego.

Niewielki zasięg transmisji oraz konieczność istnienia linii widzialności optycznej LoS (Line of Sight) między nadajnikiem a odbiornikiem są w tym przypadku zaletą. Potencjalny intruz ma mniejsze możliwości przeprowadzenia ataku w sposób niezauważalny. Zakłada się, że kanał uwierzytelniania jest kanałem autentycznym lub zaufanym (rys. 1).



Rys. 1. Model komunikacji w systemie uwierzytelniania pozapasmowego
Fig. 1. Communication model for out-of-band authentication

Kanał komunikacyjny jest uważany za autentyczny, jeżeli Bob ma gwarancję tego, że komunikat, który otrzymał, został faktycznie wysłany przez Alicję. Innymi słowy, zakłada się, że potencjalny intruz nie ma możliwości wysłania danych za pomocą tego kanału w sposób niewykrywalny. Niemniej dopuszcza się, że komunikat może być podsłuchany przez nieupoważnionego użytkownika – podsłuchane dane nie dają możliwości naruszenia bezpieczeństwa. Zakłada się, że autentyczność nadawcy komunikatu może być potwierdzona bezpośrednio przez użytkownika, a niekoniecznie przez elektroniczne urządzenie komunikacyjne. Kanał komunikacyjny uważa się za prywatny, jeżeli Alicja ma gwarancję tego, że komunikat, który wysyła, zostanie odebrany tylko przez Boba. Niemniej dopuszcza się sytuację, w której Bob nie wie, że komunikat został wysłany przez Alicję.

W niektórych rozwiązaniach problemu zakłada się dodatkowy udział człowieka w procesie uwierzytelniania, np. na etapie porównywania skrótów. Przykładem są protokoły oparte na systemie MANA (Manually Authenticated Strings) [9]. Oczywistą wadą rozwiązań opartych na porównywaniu manualnym jest stosunkowo wysokie ryzyko błędu człowieka.

Nieco innym rozwiązaniem są systemy oparte na konieczności zagwarantowania bliskości urządzeń, które są kojarzone. Formalne uwierzytelnienie nie jest w tym przypadku niezbędne. Zakłada się, że komunikacja jest możliwa tylko wtedy, gdy urządzenia znajdują się blisko siebie (w odległości nieprzekraczającej kilku centymetrów). Ponadto, niewielka odległość między urządzeniami eliminuje część zagrożeń.

Użycie kanału pozapasmowego lub zagwarantowanie bliskości urządzeń pozwala niekiedy skrócić czas potrzebny na uwierzytelnienie (np. [10]).

1.3. Rodzaje kanałów dla uwierzytelniania pozapasmowego

Dla celów uwierzytelniania pozapasmowego oraz tzw. efemerycznego kojarzenia urządzeń bezprzewodowych (ang. *ephemeral pairing*) wykorzystać można wiele różnych kanałów komunikacyjnych i metod transmisji. Należą do nich [5]:

- systemy oparte na sąsiedztwie
  - transmisja z użyciem kontaktu elektrycznego,
  - transmisja w technologii NFC (ang. *Near Field Communication*),
  - system Dhwani,
  - uwierzytelnianie na podstawie analizy danych z akcelerometrów,
- transmisja w pasmach „pozaradiowych"
  - w paśmie podczerwieni (np. [2]),
  - w paśmie wizualnym (np. metoda Seeing is Believing [14]),
  - w paśmie akustycznym (np. metoda Loud&Clear [7]) i w paśmie ultradźwięków,
- inne
  - uwierzytelnienie na podstawie analizy położenia (pomiar za pomocą ultradźwięków).

Wymienione metody kojarzenia urządzeń pozwalają na transmisję danych między urządzeniami, które albo stykają się ze sobą, albo znajdują się w niewielkiej (rzędu metrów) odległości od siebie.

Prace dotyczące poszczególnych rozwiązań są aktualnie na różnym poziomie zaawansowania. Przeprowadza się eksperymenty naukowe, istnieją protokoły komunikacyjne (np. [12]), wdraża się rozwiązania komercyjne.

2. Kanały komunikacyjne uwierzytelniania pozapasmowego

2.1. Standard IEEE 802.15.7

Opracowany niedawno standard IEEE 802.15.7 jest standardem transmisji danych w paśmie widzialnym (fale o długościach 380-780 nm, częstotliwości 428-750 THz). Dane są transmitowane z użyciem kodowania RLL (Run Length Limited) i jednej z kilku metod modulacji:

- modulacji typu włącz-wyłącz (ang. *on-off keying*),
- modulacji ze zmiennym położeniem impulsu (ang. *variable pulse-position modulation*),
- modulacji przesunięcia koloru (ang. *color shift keying*).

Różne metody modulacji umożliwiają uzyskiwanie różnych prędkości transmisji. Metoda umożliwia przesyłanie danych na niewielkie odległości z maksymalną prędkością nominalną dochodzącą do 96 Mbit/s. Transmisja może się odbywać wewnątrz i na zewnątrz budynków.

Wzrost zainteresowań transmisją w paśmie widzialnym jest spowodowany między innymi rozwojem technologii diod świecących LED (Light Emitting Diode) i spadkiem kosztów. W ostatnich latach opracowano diody o dużej efektywności energetycznej, a także diody z krótkimi, nanosekundowymi czasami przełączania. Transmisja może się odbywać z użyciem pojedynczej diody nadawczej i pojedynczej fotodiody odbiorczej PD (ang. *photodetector*) lub z użyciem zbioru diod tworzących macierze – metoda MIMO (ang. *Multiple Input Mutiple Output*).

Komunikacja w paśmie widzialnym wymaga rozwiązania problemów związanych z migotaniem (ang. *flickering*) i przyciemnianiem (ang. *dimming*) źródeł światła.

Migotanie źródła światła jest skutkiem ubocznym przyjętej metody modulacji. Migotanie musi być zminimalizowane ze względu na wpływ, jaki może wywierać na znajdujących się w otoczeniu ludzi. W opracowanym standardzie przyjęto, że zmiany jasności źródła światła muszą się zawierać w ściśle określonym przedziale czasu MFTP (ang. *Maximum Flickering Time Period*). MFTP jest to maksymalny czas, w którym intensywność źródła światła może się zmienić i ludzkie oko nie jest w stanie tego dostrzec. Uznaje się, że wartość MFTP poniżej 5 ms jest bezpieczna [3]. W systemie komunikacji w paśmie widzialnym konieczne jest zagwarantowanie, by procesy modulacji nie powodowały niepożądanego migotania zarówno podczas transmisji ramki danych, jak i między kolejnymi ramkami.

Kolejnym problemem jest przyciemnianie źródła światła. Transmisja danych nie może być zakłócona w wyniku np. przypadkowego przyciemnienia nadajnika. Problem przyciemniania jest rozwiązywany z użyciem odpowiednio zmodyfikowanych metod modulacji (np. poprzez okresową resynchronizację i adaptacyjną zmianę parametrów czasowych modulacji) [17].

2.2. NFC

NFC (ang. *Near Field Communication*) to metoda transmisji wykorzystująca fale elektromagnetyczne i zjawiska bliskopolowe. Transmisja odbywa się na niewielkie odległości, rzędu centymetrów, przy czym średnica obszaru bliskopolowego jest zależna od długości fal. Prędkości transmisji dochodzą do 1 Mbit/s. Standardowo transmisja opiera się na częstotliwości 13,56 MHz, z modulacją amplitudy i pasmem o szerokości 1,8 MHz.

Fale elektromagnetyczne w obszarze bliskopolowym charakteryzują się innymi właściwościami niż w obszarze dalekopolowym używanym w standardowych systemach komunikacji radiowej. W szczególności absorpcja promieniowania przez odbiornik wpływa na ob-

ciążenie nadajnika. Pola elektryczne i magnetyczne są niezależne od siebie. Pole wypadkowe może być (zależnie od źródła) zdominowane przez składową magnetyczną lub elektryczną. Jedną
z zalet jest możliwość zapewnienia komunikacji między urządzeniami, z których jedno nie ma własnego zasilania (ang. *passive mode*) – energię czerpie z pola elektromagnetycznego emitowanego przez drugie z urządzeń [1].

Niewielka odległość między urządzeniami eliminuje część zagrożeń. Niemniej doświadczalnie wykazano [8], że istnieje możliwość podsłuchania transmisji z odległości większej (nawet kilku metrów) niż odległość między komunikującymi się urządzeniami.

Opracowano wiele standardów interfejsów, protokołów NFC i metod ochrony danych, w tym: ISO/IEC 14443, ISO/IEC 18000-3, ISO/IEC 18092/ECMA-340l-1 (NFCIP-1), ISO/IEC 21481/ECMA-352 (NFCIP-2), ECMA-385 (NFC-SEC). Funkcje komunikacji NFC są dostępne w smartfonach, między innymi takich producentów, jak: LG, Samsung, Sony.

2.3. Seeing-is-believing

Metoda uwierzytelniania SiB (ang. *Seeing-is-believing*) korzysta z kanału komunikacyjnego w paśmie widzialnym [14]. Do uwierzytelniania stosuje się dwuwymiarowe kody kreskowe (ang. *data matrix bar code*) i kamery zintegrowane z urządzeniami przenośnymi. W procesie uwierzytelniania biorą udział dwa urządzenia. Pierwsze z urządzeń (ang. *showing device*) ma na swojej powierzchni widoczny kod kreskowy – jest on wydrukowany na etykiecie przyklejonej do urządzenia (klucz długoterminowy) lub generowany dynamicznie i wyświetlany na wyświetlaczu danego urządzenia (klucz krótkoterminowy, efemeryczny). Kod kreskowy może zawierać takie informacje, jak klucz publiczny lub skrót klucza publicznego. Drugie z urządzeń (ang. *finding device*), wyposażone w cyfrowy aparat fotograficzny, robi zdjęcie kodu z pierwszego urządzenia. Wykonanie zdjęcia wymaga nakierowania obiektywu na właściwe urządzenie – użytkownik kontroluje to, jakie urządzenie jest fotografowane. Następnie klucz publiczny pierwszego urządzenia jest transmitowany radiowym kanałem komunikacyjnym do drugiego urządzenia. Następuje wyznaczenie skrótu odebranego klucza i porównanie tego skrótu ze skrótem klucza odebranego za pomocą kanału w paśmie widzialnym. Brak zgodności między skrótami oznacza próbę podszycia się w kanale radiowym.

Uwierzytelnianie metodą SiB może być jednokierunkowe lub dwukierunkowe. Uwierzytelnianie dwukierunkowe polega na wykonaniu dwóch procesów uwierzytelniania z zamienionymi rolami urządzeń.

2.4. Loud&Clear

Alternatywnym rozwiązaniem w stosunku do SiB jest Loud&Clear z użyciem kanału akustycznego [7]. Metoda może być zastosowana w przypadku urządzeń pozbawionych kamer,
a także wtedy, gdy użycie takich urządzeń jest niemożliwe, np. zakazane prawnie w obiektach wojskowych, elektrowniach atomowych.

Skrót klucza publicznego jednego z urządzeń jest przekształcany do postaci bezsensownego ale poprawnego gramatycznie zdania w języku angielskim (przykładowe zdanie wygenerowane z wartości skrótu może mieć postać: *Durward the fragile Egyptian-vulture flawlessly end-ed over the drunk egret*). Następnie za pomocą oprogramowania przekształcającego zdanie do postaci sygnału mowy i za pomocą głośnika w urządzeniu zakodowany skrót klucza jest przesyłany w postaci głosu do drugiego urządzenia, a właściwie do użytkownika tego urządzenia. Zadaniem użytkownika jest wysłuchanie tekstu i porównanie go z ciągiem znaków wyświetlonym na ekranie lub umieszczonym na etykiecie znajdującej się na urządzeniu. Brak zgodności oznacza próbę podszycia się. Uwierzytelnianie metodą Loud&Clear może być jednokierunkowe lub dwukierunkowe [7].

Istotną wadą rozwiązania jest stosunkowo długi całkowity czas uwierzytelniania. Może on sięgać kilkudziesięciu sekund.

2.5. Dhwani

Dhwani jest systemem komunikacji akustycznej, krótkiego zasięgu (rzędu centymetrów) i niewielkiej przepustowości (do 2,4 kbit/s). System został opracowany przez Microsoft. System jest przeznaczony dla telefonów komórkowych. Problem uwierzytelniania jest w tym przypadku rozwiązywany przez konieczność zagwarantowania bliskości urządzeń (ang. *association by physical proximity*). Dhwani ma zastosowania podobne do NFC, jednak nie wymaga sprzętowego modułu NFC w smartfonie, a jedynie zmodyfikowanego oprogramowania.

Transmisja odbywa się w paśmie 0-22 kHz. Problemy związane z zakłóceniami charakterystycznymi w paśmie akustycznym są rozwiązywane z użyciem ortogonalnego podziału częstotliwości OFDM (ang. *Orthogonal Frequency Division Multiplexing*). Te podzakresy OFDM, w których występują zakłócenia, nie są używane do transmisji.

Wyjątkową cechą Dhwani jest sposób zagwarantowania poufności. Zastosowano ochronę na poziomie warstwy fizycznej poprzez autozagłuszanie (ang. *selfjamming*). Autozagłuszanie polega na tym, że legalny odbiorca celowo zagłusza sygnał odbierany w paśmie akustycznym. Wysyłanie pseudolosowego sygnału zagłuszającego o wartościach znanych legalnemu odbiorcy (ang. *jamming sequence predetermined by the receiver*) w momencie transmisji

danych w dużym stopniu utrudnia podsłuch. Jednocześnie legalny odbiorca używa techniki autokasowania interferencji (ang. *self-interference cancellation*) do poprawnego zdekodowania odbieranych sygnałów akustycznych [15].

2.6. Generowanie kluczy współdzielonych z użyciem akcelerometrów

W przypadku kojarzenia ze sobą dwóch urządzeń przenośnych, takich jak smartfony możliwe staje się wygenerowanie współdzielonych kluczy kryptograficznych poprzez określone oddziaływanie na oba urządzenia w identyczny sposób. Idea metody polega na tym, że dwa urządzenia zostają poddane identycznemu oddziaływaniu. Jednocześnie inne (nielegalne) urządzenie nie jest poddane takiemu oddziaływaniu. Poprzez jednoczesny pomiar pewnych wartości oddziaływania w obu urządzeniach można doprowadzić do sytuacji, w której oba urządzenia będą dysponowały tymi samymi danymi (np. wspólnym kluczem kryptograficznym dla systemu symetrycznego). Jednocześnie urządzenie trzecie nie będzie tymi danymi dysponowało. Wygenerowany klucz będzie poufny.

Implementacją powyższej metody jest system generowania klucza za pomocą danych z akcelerometrów [4]. Zakłada się, że urządzenia wyposażone są w akcelerometry. Dwa urządzenia stykają się ze sobą i są potrząsane (w trzech wymiarach) przez użytkownika. Czas synchronicznego potrząsania sięga kilku sekund. Zakłada się, że potrząsanie ma charakter pseudolosowy. Dane odczytywane z akcelerometrów w obu urządzeniach służą do wygenerowania klucza. Potrząsanie stykającymi się urządzeniami ma gwarantować identyczność danych z akcelerometrów, a tym samym zgodność wygenerowanych kluczy (w praktyce dane nie zawsze są identyczne, niemniej zastosowane w metodzie algorytmy przetwarzania danych o określonym stopniu zgodności generują identyczne klucze). Klucz wygenerowany w ten sposób jest jednocześnie poufny, ponieważ inne urządzenia nie są poddane takiemu samemu potrząsaniu i nie dysponują tymi samymi danymi z akcelerometrów. Należy dodać, że entropia kluczy jest zależna od entropii procesu potrząsania i można ją zwiększyć wydłużając czas potrząsania.

Sposób generowania klucza z danych akcelerometru musi gwarantować to, że prawdopodobieństwo wygenerowania identycznych kluczy w urządzeniach potrząsanych, ale niestykających się ze sobą będzie minimalne [4].

3. Podsumowanie

W artykule przedstawiono systemy uwierzytelniania pozapasmowego, dostępne dla bezprzewodowych systemów komunikacji. Wyjaśniono przyczyny stosowania tej formy uwierzy-

telniania. Zdefiniowano model komunikacji z uwierzytelnianiem pozapasmowym. Przedstawiono różne kanały komunikacyjne i metody uwierzytelniania. Uwzględniono metody, które znajdują się obecnie na różnych etapach ewaluacji, w tym prac eksperymentalnych, protokołów i wdrożeń (tab. 1).

Tabela 1

Charakterystyka metod uwierzytelniania pozapasmowego

Metoda	Charakterystyka
IEEE 802.15.7	• standard komunikacji w paśmie widzialnym • względnie duże prędkości transmisji • zasięg do ~1 km • nadajnik, proces transmisji widoczne dla użytkownika • wymagana linia widzialności optycznej LoS
NFC	• dostępne liczne protokoły komunikacyjne • dostępne implementacje, np. w smartfonach • bardzo ograniczony zasięg transmisji
Seeing is Believing	• transmisja w paśmie widzialnym • prace na etapie eksperymentów • wymagany aktywny udział człowieka • wymagana linia widzialności optycznej
Loud & Clear	• transmisja w paśmie akustycznym • prace na etapie eksperymentów • stosunkowo długi czas uwierzytelniania • wymagany aktywny udział człowieka • problem błędów użytkownika
Dhwani	• transmisja w paśmie akustycznym • rozwiązanie firmowane przez Microsoft • dodatkowe elementy bezpieczeństwa
Metoda akcelerometrów	• metoda generowania kluczy współdzielonych za pomocą synchronicznego potrząsania • prace na etapie eksperymentów • wymagany aktywny udział człowieka

W ostatnich latach opracowano wiele metod uwierzytelniania pozapasmowego. Każda z nich ma swoje wady i zalety (np. długi czas uwierzytelniania, zaangażowanie człowieka w proces uwierzytelniania). Stosowanie nowych kanałów komunikacyjnych i nowych metod transmisji powoduje, że pojawiają się zupełnie nowe problemy. W szczególności dotyczą one tych systemów, w których nie tylko urządzenie, ale także człowiek jest w stanie odbierać nadawane sygnały (w paśmie widzialnym lub w paśmie akustycznym) lub w których zachowanie człowieka wpływa na wartości danych uwierzytelniania – ryzyko popełnienia błędu przez człowieka jest stosunkowo wysokie.

Przedstawione metody nie gwarantują pełnego bezpieczeństwa. Problemem może być na przykład użycie w procesie uwierzytelniania urządzenia przenośnego, zainfekowanego. W takim

przypadku żaden wynik przetwarzania realizowanego w urządzeniu nie może być uznany za wiarygodny. Ponadto doświadczalnie wykazano, że zakładane bezpieczeństwo wynikające z bliskości urządzeń nie zawsze jest pełne. Pozapasmowe kanały uwierzytelniania pozwalają wyeliminować niektóre zagrożenia oraz skrócić całkowity czas potrzebny na skojarzenie urządzeń bezprzewodowych przed właściwą transmisją.

BIBLIOGRAFIA

1. Ahson M., Ilyas S. A.: Near Field Communications Handbook. Auerbach Publications 2011.
2. Balfanz D., Smetters D., Stewart P., Wong H.C.: Talking to strangers: authentication in ad-hoc wireless networks. Proceedings of the Symposium on Network and Distributed Systems Security (NDSS), 2002, s. 23–35.
3. Berman S. et al.: Human Electroretinogram Responses to Video Displays. Fluorescent Lighting and Other High Frequency Sources, Optometry and Vision Science, vol. 68, 1991, s. 645–62.
4. Bichler D., Stromberg G., Huemer M., Löw M.: Key Generation Based on Acceleration Data of Shaking Processes, J. Krumm et al. (Eds.): UbiComp 2007, LNCS 4717, Springer Verlag, Berlin Heidelberg 2007, s. 304–317.
5. Bilski T.: Data Security in Emerging Wireless Technologies, Information Systems Architecture and Technology – Networks Architecture and Aplications, [Editors L. Borzemski, A. Grzech, J. Świątek, Z. Wilimowska], Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2013, s. 119–128.
6. Bilski T.: New Threats and Innovative Protection Methods in Wireless Transmission Systems. Journal of Telecommunications and Information Technology, Instytut Łączności, 3 numer 2014 roku (zgłoszono do druku).
7. Goodrich M.T., Sirivianos M., Solis J., Tsudik G., Uzun, E.: Loud and clear: human-verifiable authentication based on audio, Proceedings of the IEEE International Conference on Distributed Computing Systems (ICDCS), 2006, s. 1–10.
8. Kortvedt H., Mjolsnes S.: Eavesdropping Near Field Communication. The Norwegian Information Security Conference (NISK), Listopad 2009.
9. Laur S., Nyberg K.: Efficient mutual data authentication using manually authenticated strings. Proceedings of Cryptology and Network Security (CANS), 2006, s. 90–107.
10. Madhavapeddy A., Scott D., Sharp R., Upton, E.: Using visual tags to bypass Bluetooth device discovery. Proceedings of the ACM Mobile Computing and Communications Review (MC2R), 2005, s. 41–53.

11. Martinovic I., Gollan N., Cappellaro L., Schmitt J.: Chaotic communication improves authentication: protecting WSNs against injection attacks. Security and Communication Networks, Security Comm. Networks, Wiley, 2009, s. 117–132.
12. Martinovic I., Pichota P., Schmitt J.B.: Jamming for Good: A Fresh Approach to Authentic Communication in WSNs, WiSec'09 Zurich, March 16–18, 2009.
13. Mayrhofer R., Welch M.: A Human-Verifiable Authentication Protocol Using Visible Laser Light. Second International Conference on Availability, Reliability and Security (ARES'07), 2007.
14. McCune J. M., Perrig A., Reiter M. K., Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication, International Journal of Security and Networks Special Issue on Secure Spontaneous Interaction. 4(1-2), 2009, s. 43–56.
15. Nandakumar R., Chintalapudi K. K., Padmanabhan V. N., Venkatesan R., Dhwani: Secure Peer-to-Peer Acoustic NFC, SIGCOMM'13, August 12–16, Hong Kong 2013, http://research.microsoft.com/pubs/192134/Paper325Dhwani.pdf.
16. Premnath S. N, Jana S., Croft J., Gowda P. L., Clark M., Kasera S. K., Patwari N., Krishnamurthy S.V., Secret Key Extraction from Wireless Signal Strength in Real Environments, IEEE Transactions on Mobile Computing, Vol. 12, No. 5, May 2013, s. 917–930.
17. Rajagopal S., Roberts R.D., Lim S-K.: 802.15.7 Visible Light Communication: Modulation Schemes and Dimming Support, IEEE Communications Magazine, March 2012, s. 72–82.

Wpłynęło do Redakcji 9 kwietnia 2014 r.

Abstract

The paper presents out-of-band authentication methods. The methods are necessary in the case of many wireless transmission systems. Such common authentication methods as public key cryptography or trusted third party are widely used but they have some requirements, e.g. it is necessary that some forms of trust between subjects already exist. The requirements may not be fulfilled in every case of communication.

Out-of-band authentication model is based on additional channel (usually with limited range and limited throughput). The secondary channel is used to send authentication data (e.g. public key) in such a way that user of the device is able to verify the source of transmitted data. The secondary channel may be based on: electrical contact between two devices, infrared transmission, NFC, transmission in visual spectrum (Seeing is Believing method),

transmission with acoustic waves (Loud&Clear method). There are standards, experimental works and implementations of the different channels for out-of-band authentication.

Each system has some drawbacks and advantages (e.g. long time of the process, some requirements related to the device functions). An important issue is related to human-assisted device authentication – human is responsible for a part of authentication process. The risk related to human errors is relatively high.

Adres

Tomasz BILSKI: Politechnika Poznańska, Instytut Automatyki i Inżynierii Informatycznej, pl. Skłodowskiej-Curie 5, 60-965 Poznań, Polska, tomasz.bilski@put.poznan.pl.