

Bezpieczeństwo systemów komputerowych

RFID

Marcin Peczarski

Instytut Informatyki Uniwersytetu Warszawskiego

14 grudnia 2009

Wykorzystano materiały ze strony *<http://www.rfid.citi-lab.pl>*.

Coś więcej niż radiowy kod paskowy lub system antykradzieżowy

- ▶ Radio Frequency IDentification – system kontroli oparty o zdalny, za pomocą fal radiowych, odczyt i zapis danych
- ▶ Nie mylić ze sklepowymi systemami antykradzieżowymi, wykorzystującymi zjawisko rezonansu:
 - ▶ klips z obwodem rezonansowym (cewka i kondensator), który, znalazłszy się w zmiennym polu elektromagnetycznym o częstotliwości drgań własnych, pobiera energię;
 - ▶ system magnetoakustyczny – naklejka z namagnesowanymi blaszkami, które, znalazłszy się w zmiennym polu elektromagnetycznym o odpowiedniej częstotliwości, emitują ultradźwięki, wykrywane przez mikrofon.

Zastosowania

- ▶ Paszporty biometryczne
- ▶ Opłaty transportowe
- ▶ Identyfikacja zwierząt
- ▶ Identyfikacja książek w bibliotece
- ▶ Identyfikacja osób w systemach kontroli dostępu
- ▶ Rejestracja czasu pracy
- ▶ Identyfikacja towarów
- ▶ Identyfikacja przesyłek kurierskich
- ▶ Immobilizery i piloty samochodowe
- ▶ Piloty otwierające bramy

Składniki systemu RFID

- ▶ Czytnik zawierający nadajnik i dekodery
- ▶ Antena
- ▶ Transpondery zwane znacznikami (ang. tags)

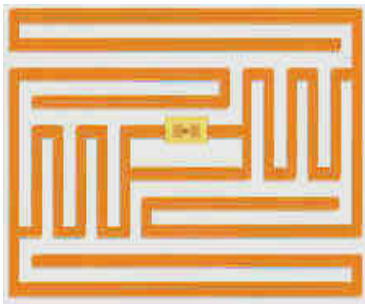
Czytniki

- ▶ Stacjonarne
- ▶ Przenośne
- ▶ Zintegrowane



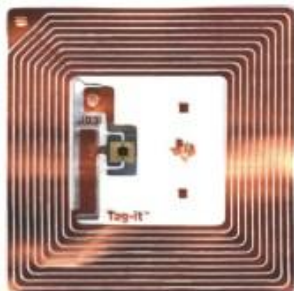
Znaczniki

- ▶ Aktywne – własne źródło zasilania, możliwość inicjowania komunikacji
- ▶ Pasywne – bez własnego źródła zasilania
- ▶ Półpasywne – wewnętrzne źródło tylko do zasilania mikroprocesora
- ▶ Rozmiary od $0,4 \times 0,4$ mm
- ▶ Postać nalepki, żetonu, nitu itp.
- ▶ Unikalny identyfikator

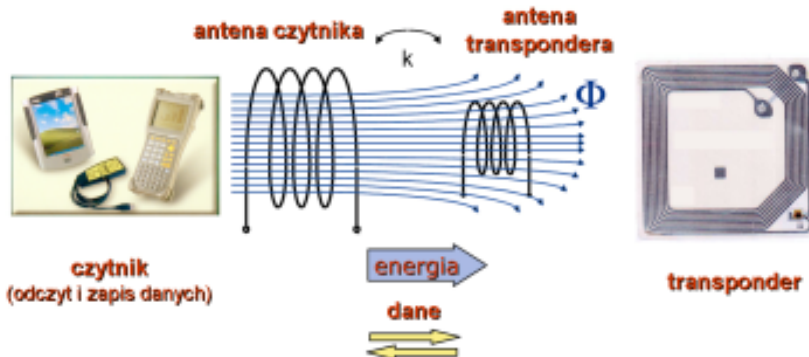


Znaczniki, cd.

- ▶ Tylko do odczytu (ang. read-only)
- ▶ Jednokrotnego zapisu i wielokrotnego odczytu (ang. worm – write once, read many)
- ▶ Wielokrotnego odczytu i zapisu (ang. read-write)



Znaczniki (pół)pasywne



- ▶ Zasilane za pomocą pola elektromagnetycznego wytwarzanego przez antenę
- ▶ Odpowiedź wysyłana po zgromadzeniu przez kondensator wystarczającej ilości energii

Zasada działania znaczników (pół)pasywnych

► Czytnik

- wytwarza zmienne pole elektromagnetyczne wokół anteny;
- wysyła żądanie identyfikacji;
- wykrywa zaburzenia pola elektromagnetycznego wywołane przez znacznik;
- dekoduje uzyskany sygnał.

► Znacznik

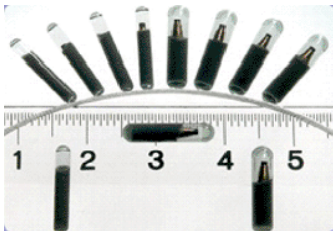
- znalazłszy się w polu elektromagnetycznym czytnika, zaczyna ładować kondensator, korzystając z napięcia elektrycznego indukowanego w cewce anteny odbiorczej;
- po zgromadzeniu ładunku elektrycznego wystarczającego do zasilania układów elektronicznych rozpoczyna wysyłanie informacji.
- transmituje dane, modulując pole elektromagnetyczne przez zwieranie i rozwieranie cewki, co powoduje chwilowe zmiany tłumienia sygnału emitowanego przez antenę czytnika.

Częstotliwości pracy i zasięgi

- ▶ 125 – 134 kHz, tylko odczyt z odległości kilkunastu centymetrów
- ▶ 13,56 MHz, odczyt i zapis informacji, zasięg do ok. jednego metra
- ▶ 433 MHz, 868 – 956 MHz, 2,45 GHz, 5,8 GHz, zasięg do kilku metrów, niemożliwy odczyt przez ciecz i z powierzchni metalu

Zagrożenia, implanty RFID

- ▶ Wszczepianie ludziom implantów budzi wątpliwości natury prawnej, moralnej i zdrowotnej. „The Truth Is Out There”.



- ▶ Identyfikowanie w ten sposób zwierząt spotyka się z mniejszymi zastrzeżeniami.

Zagrożenia, cd.

- ▶ Jeśli obok samochodu firmy kurierskiej, korzystającej z RFID w celu usprawnienia dostarczania przesyłek, przejdzie osoba z czytnikiem, może poznać zawartość paczek, ich przeznaczenie oraz odbiorców.
- ▶ Zdalna identyfikacja towarów umożliwia obserwowanie zachowań klientów w sklepach.
- ▶ Dokumenty korzystające z technologii RFID (bilety komunikacji miejskiej, paszporty) ułatwiają naruszanie prywatności.

Zabezpieczenia w RFID

- ▶ PIN
- ▶ Identyfikacja biometryczna
- ▶ Pseudolosowe ID
- ▶ Polecenie KILL
- ▶ Blokowanie znaczników
- ▶ Kontrolowanie poziomu energii
- ▶ Klatka Faradaya
- ▶ Uszkadzanie anteny
- ▶ Szyfrowanie

PIN

- ▶ Uwierzytelnianie dostępu do znacznika za pomocą kodu PIN
- ▶ Podawany przed każdym odczytem przez użytkownika za pomocą klawiatury sprzężonej z czytnikiem
- ▶ Skuteczność podobna, jak w przypadku kart płatniczych, choć, z uwagi na transmisję radiową, wymaga dodatkowych zabiegów

System identyfikacji biometrycznej

- ▶ Rolę kodu dostępu (PIN) pełni wzorzec biometryczny:
 - ▶ tęczówka oka,
 - ▶ linie papilarne palca,
 - ▶ profil DNA.

Pseudolosowe ID

- ▶ Znacznik RFID ma zapisany tylko niewiele znaczący pseudolosowy identyfikator.
- ▶ Baza danych zawiera identyfikatory i powiązane z nimi dane.
- ▶ Samo odczytanie identyfikatora nie ujawnia żadnej wrażliwej informacji.
- ▶ Jednak wycieknięcie takich informacji z bazy danych jest tylko kwestią czasu.

Polecenie KILL

- ▶ Unicestwia znacznik RFID.
- ▶ Następuje całkowita i nieodwracalna dezaktywacja znacznika.
- ▶ Podczas komunikacji znacznik może znajdować się w jednym z 7 stanów:
 - ▶ stan gotowości,
 - ▶ wstrzymania,
 - ▶ odpowiedzi,
 - ▶ potwierdzenia,
 - ▶ otwartym,
 - ▶ zabezpieczonym,
 - ▶ śmierci, do którego przechodzi po otrzymaniu zweryfikowanego polecenia KILL.
- ▶ Dzięki jego zastosowaniu np. klient wychodząc ze sklepu, ma pewność, że znacznik już nie wysyła sygnałów.
- ▶ Jednak jest to polecenie nieodwracalne, co znacznie zawęży możliwość jego stosowania.

Blokowanie znaczników

- ▶ Kolejnym sposobem zabezpieczeń jest blokowanie na trwałe znaczników.
- ▶ Czytnik bez zezwolenia nie może zeskanować RFID.

Kontrolowanie poziomu energii

- ▶ Jeżeli poziom energii jest zbyt mały lub zbyt duży, można podejrzewać, że dokonywana jest próba nieuprawnionego odczytu i wtedy taka próba powinna być zignorowana.
- ▶ Zabezpieczenie polega na ustawieniu odpowiedniej odległości odczytu, np. na ok. 15 cm.

Klatka Faradaya

- ▶ Nie pozwala ona na transmisję radiową w jej obrębie.
- ▶ Pojawiły się w sprzedaży portfele działające na tej zasadzie.
- ▶ Zamknięty portfel blokuje odczyt danych z umieszczonych w nim dokumentów.
- ▶ Aby odczytać zawartość np. karty płatniczej, trzeba otworzyć portfel.

Uszkadzanie anteny

- ▶ Jest skuteczną metodą unicestwiania znaczników.
- ▶ Po złamaniu anteny można dokonać odczytu tylko z bardzo bliskiej odległości.
- ▶ Uszkodzenia anteny dokonuje się np. przez pociągnięcie nitki, która wyprowadzona jest na zewnątrz znacznika.

Szyfrowanie

- ▶ Najbardziej uniwersalny sposób zabezpieczania
- ▶ Wszystkie poprzednie to półśrodki
- ▶ Problem to mała moc obliczeniowa mikroprocesorów stosownych w znacznikach
- ▶ Dotychczas brak zadowalających algorytmów
- ▶ Pojawiające się co jakiś czas doniesienia o złamaniu kolejnych zabezpieczeń

Zupełnie losowo wybrane przykłady złamania

- ▶ F. D. Garcia i in., Dismantling MIFARE Classic, ESORICS 2008, LNCS 5283, 97–114.
<http://www.securitystandard.pl/news/169499/Dziurawe.karty.RFID.html>
<http://www.sos.cs.ru.nl/applications/rfid/2008-esorics.pdf>
<http://www.sos.cs.ru.nl/applications/rfid/2008-esorics-slides.pdf>
- ▶ S. Indesteege i in., A Practical Attack on KeeLoq, EUROCRYPT 2008, LNCS 4965, 1–18.
<http://www.cosic.esat.kuleuven.be/keeloq/>
<http://www.cosic.esat.kuleuven.be/publications/article-1045.pdf>
<http://www.cosic.esat.kuleuven.be/keeloq/keeloq-slides.pdf>
- ▶ T. Eisenbarth i in., Physical Cryptanalysis of KEELoQ Code Hopping Applications.
<http://eprint.iacr.org/2008/058>