Krystian Gembala, Tomasz Piesiur

Bezpieczeństwo kart elektronicznych w e-biznesie

Ekonomiczne Problemy Usług nr 57, 647-654

2010

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 597 EKONOMICZNE PROBLEMY USŁUG NR 57 2010

KRYSTIAN GEMBALA, TOMASZ PIESIUR
Akademia Ekonomiczna w Katowicach
krystian.gembala@ae.katowice.pl, tomasz.piesiur@ae.katowice.pl

BEZPIECZEŃSTWO KART ELEKTRONICZNYCH W E-BIZNESIE

We współczesnym świecie w każdej sekundzie ludzie wymieniają się ogromną ilością różnych informacji, które są aktywami firmy i w związku z tym niezwykle cennym towarem. Nawet nie zdajemy sobie sprawy z tego, że funkcjonując w życiu codziennym, odbieramy i wysyłamy setki danych, które są narażone na ujawnienie.

Dziś już nie tylko firmy są narażone na straty związane z wyciekiem informacji. Każdy z nas używa dokumentów, które stanowią nie lada pokusę dla wychwytujących informację. Adresy, numery kart kredytowych czy hasła dostępu do usług internetowych to między innymi dane, które należy chronić i zabezpieczać w możliwie najlepszy sposób. Niestety jak szybko następuje rozwój w dziedzinie bezpieczeństwa, tak szybko też doskonalą się techniki kradzieży. Aby temu zapobiec, opracowywane i ulepszane są coraz to nowe metody przekazywania informacji w sposób ukryty. Nie zdajemy sobie sprawy z tego, że zwykłe kody kreskowe, które oglądamy codziennie na różnych produktach, mogą zawierać nawet informacje strategiczne. Robiąc zakupy za pomocą karty kredytowej, nie zastanawiamy się nad tym, ile skomplikowanych procesów zachodzi w ciągu kilkunastu sekund, zanim otrzymamy potwierdzenie transakcji. Wszystkie te zabezpieczenia mają na celu ochronę dobra, jakim jest informacja.

W e-biznesie coraz częściej realizuje się transakcje bezgotówkowe z wykorzystaniem e-pieniędzy. Transakcje te przeprowadza się za pomocą kart pamięci zwanych kartami elektronicznymi.

Wraz z pojawieniem się kart elektronicznych jako środka płatniczego uwierzytelniającego pojawił się problem właściwego zabezpieczenia nie tylko kart, ale również czytników kart, a także systemów realizacji obsługi transakcji.

Aby zabezpieczyć informacje, przechowywane na kartach elektronicznych, przed przypadkowym bądź umyślnym zniszczeniem, modyfikacją, nieuprawnionym ujawnieniem, konieczne stało się zastosowanie odpowiednich mechanizmów kontrolnych. Karta stanowi element większego systemu i konieczne stało się zadbanie nie tylko o bezpieczeństwo samej karty, ale także pozostałych elementów systemu. W tabeli 1 przedstawiono wybrane, najczęściej stosowane mechanizmy uwierzytelniania użytkownika wraz z ich zaletami i wadami.

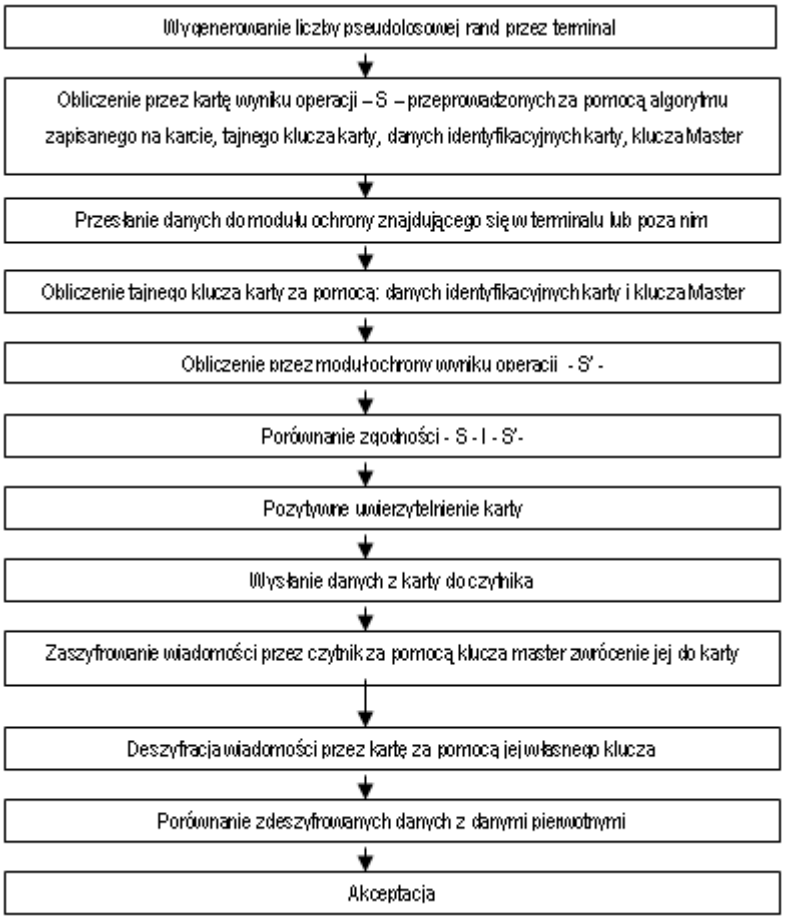
Tabela 1

Mechanizmy uwierzytelniania użytkownika

RODZAJ MECHANIZMU	OPIS	ZALETY	WADY
PIN	Porównanie zgodności wprowadzonego za pomocą klawiatury numeru z zapisem znajdującym się na chronionym obszarze pamięci karty.	Zastosowanie licznika błędów powoduje, że niemożliwe jest wprowadzenie wszystkich kombinacji numeru PIN.	Konieczność pamiętania PIN; możliwość sczytania przez inne osoby PIN za pomocą zmodyfikowanych terminali; możliwość uzyskania PIN bezpośrednio od użytkownika.
ROZPOZNAWANIE GŁOSU	Wypowiedzenie sentencji wybranej przez terminal lub określonej przez użytkownika.	Możliwość zastosowania na zewnątrz budynków; możliwy brak konieczności zapamiętywania określonych haseł.	Duży współczynnik odrzucenia; brak odporności na naturalne zmiany głosu; możliwość odtworzenia głosu przez niepowołane osoby.
WERYFIKACJA PODPISU	Rejestracja cech związanych ze składaniem podpisu, takich jak: siła nacisku, prędkość i przyśpieszenie, wykrywanie ruchu, względne tory.	Niski współczynnik odrzucenia.	Średnia czułość systemu na nastawienie użytkownika; możliwość zastosowania jedynie wewnątrz budynków; czasochłonność.
DYNAMIKA PODPISU SKŁADANEGO NA KLAWIATURZE	Rozpoznanie użytkownika na podstawie sposobu pisania na klawiaturze za pomocą badania korelacji między naciskanymi klawiszami.	Prosta technika, niezawodność; brak dodatkowego sprzętu, niska cena.	-
ODCISK PALCA	Sczytanie odcisków za pomocą urządzeń optycznych i ultradźwiękowych oraz czytników ciepła.	Bardzo niski współczynnik odrzucenia, co pozwala na zastosowanie w systemach wymagających wysokiego bezpieczeństwa; krótki czas weryfikacji; małe czytniki.	Duża wrażliwość systemu, co uniemożliwia jego zastosowanie przy dużej liczbie użytkowników; możliwość stosowania głównie wewnątrz budynków.
ROZPOZNAWANIE KSZTAŁTU DŁONI I GŁOWY	Metoda podobna do metody wykorzystującej odcisk palca.	Wysoka precyzyjność, co pozwala na zastosowanie w systemach wysokiego ryzyka; jedno urządzenie do obu metod.	-
WZÓR SIATKÓWKI OKA	Sczytanie wzoru siatkówki oka przez skaner.	Niezawodność, możliwość stosowania na zewnątrz budynków	Błędna identyfikacja przy niektórych chorobach oczu.
WZÓR TĘCZÓWKI OKA	Skanowanie tęczówki oka.	Największa niezawodność wśród metod identyfikacji dzięki 250 niepowtarzalnym cechom tęczówki; odporność na próby fałszerstwa dzięki dodatkowym badaniom, m.in. ciśnienia krwi i reakcji źrenicy na światło.	-
ROZPOZNAWANIE TWARZY	Metoda podobna do metody wykorzystującej odcisk palca.	Możliwość ustalenia tożsamości.	Wysoka zawodność.

Źródło: Opracowanie własne na podstawie [KuMo2002].

Mechanizm uwierzytelniania podmiotów polega na sprawdzeniu przez system, czy użyta karta jest autentyczna lub też na sprawdzeniu przez kartę autentyczności obsługującego ją systemu. W tym celu stosuje się symetryczne lub asymetryczne systemy kryptograficzne. Na rysunku 1 przedstawiono przykładowy przebieg procedury uwierzytelniania karty za pomocą systemu klucza.



Rys. 1. Procedura uwierzytelniania karty za pomocą systemu symetrycznego

Źródło: Opracowanie własne na podstawie [KuMo2002].

Inna z metod uwierzytelniania danych polega na dodaniu do wiadomości dodatkowej informacji CRC (ang. Cyclic Redundancy Check – cykliczny kod nadmiarowy). Odbiorca po dodaniu CRC porównuje informację i gdy choć jeden bit będzie odmienny, dane nie uzyskają akceptacji.

Innym mechanizmem uwierzytelniania kart elektronicznych jest szyfrowanie symetryczne, polegające na zaszyfrowaniu tekstu za pomocą klucza kryptograficznego, a następnie zdeszyfrowaniu go przez odbiorcę za pomocą tego samego klucza. Ten rodzaj zabezpieczenia poufnych informacji zdaje egzamin tak długo, dopóki klucz pozostanie tajny.

Kolejnym mechanizmem uwierzytelniania kart elektronicznych jest szyfrowanie asymetryczne (podpis elektroniczny), w Polsce jeszcze bardzo rzadko stosowane, ale dzięki swoim możliwościom coraz częściej wykorzystywane w celu poprawy bezpieczeństwa kart elektronicznych. Polega ono na użyciu nie jednego, ale dwóch kluczy:

- publicznego – podanego do publicznej wiadomości,
- prywatnego – znajdującego się tylko w posiadaniu użytkownika,
- które są ze sobą powiązane.

Dzięki takiemu rozwiązaniu praktycznie nie jest możliwe odgadnięcie klucza deszyfrującego, ponieważ wymaga to bardzo złożonych i czasochłonnych obliczeń.

Zarówno szyfrowanie symetryczne, jak i asymetryczne odbywa się z zastosowaniem algorytmów kryptograficznych, takich jak:

- DES (ang. Data Encryption Standard – standard szyfrowania danych) – symetryczny, do szyfrowania i deszyfrowania używa się tych samych kluczy czytanych w odwrotnej kolejności, łatwy do złamania, szyfruje bloki danych o długości 64 bitów,
- 3DES – symetryczny, szyfrowanie odbywa się za pomocą trzykrotnego powtórzenia algorytmu DES,
- IDEA (ang. International Data Encryption Algorithm) – symetryczny szyfr blokowy wykorzystujący nie permutacje, ale operacje algebraiczne, szyfr ten nigdy nie został złamany,
- AES (ang. Advanced Encryption Standard, zwany również Rijndael) – symetryczny szyfr blokowy, operuje na bloku danych o zmiennej długości i używa w tym celu kluczy także o zmiennej długości,
- RSA (Rivest – Shamir – Adleman) – asymetryczny, jeden z najpopularniejszych, oparty na rozkładzie na czynniki (faktoryzacji) dużych liczb, bardzo trudny do deszyfrowania,
- ECC (ang. Elliptic Curve Cryptography) – asymetryczny, wykorzystujący krzywe eliptyczne, poziom bezpieczeństwa zbliżony do algorytmu RSA,
- ECDSA (ang. Elliptic Curve DSA) – asymetryczny algorytm szyfrowania oparty na krzywych eliptycznych,
- protokół uzgadniania kluczy Diffiego-Hellmana – polega na wylosowaniu przez obie strony klucza, który jest znany jedynie im i służy do szyfrowania wiadomości, jest to jeden z najstarszych algorytmów kryptograficznych,

- SHA-1 (ang. Secure Hash Algorithm) – funkcja skrótu, używana do obliczania skrótu dla dowolnej wiadomości lub pliku danych dostarczonego na wejściu,
- MD5 (ang. Message-Digest algorithm 5 – Skrót Wiadomości wersja 5) – funkcja skrótu generująca 128-bitowy skrót dla dowolnej wielkości wiadomości.

Oprócz zabezpieczenia danych, przechowywanych na karcie elektronicznej, ważne jest także zabezpieczanie układu scalonego karty. Każdy układ ma rozpisane skrajne warunki potrzebne do jego poprawnego funkcjonowania, jednak układy produkowane dla kart elektronicznych muszą posiadać funkcję, która zabezpieczy dane w przypadku niespełnienia wymogów bezpiecznej pracy przed ich odczytaniem. Oprócz naturalnych zaburzeń, mogących wystąpić podczas użytkowania karty, układy są narażone na ingerencje w celu odczytania danych. W tabeli 2 przedstawiono sposoby uzyskania dostępu do pamięci karty.

Informacje o zabezpieczeniach stosowanych przez producentów są trudne do uzyskania, natomiast informacje o pełnym zabezpieczeniu oraz sposobach jego wykonania są pilnie strzeżone.

Także podczas dostawy układów elektronicznych istnieje obawa przed niepowołanym dostępem do danych na nich zawartych. W celu zapobieżenia takim sytuacjom układy zabezpiecza się kodem transportowym, który jest znany jedynie przez producenta i dostawcę. Każda nieudana próba sprawdzenia kodu jest zliczana przez licznik i po przekroczeniu dopuszczalnej liczby pomyłek układ zostaje zablokowany.

Dostawca karty w procesie personalizacji wprowadza dane dotyczące producenta, dostawcy, a także bezpośredniego właściciela. Są to między innymi klucze: główny klucz systemu – master, klucz dostawcy, numer PIN oraz indywidualny klucz karty. Najważniejszym kluczem zapisanym na karcie jest klucz master, który zazwyczaj znajduje się w posiadaniu dostawcy karty. Do jego zadań zaliczyć można m.in.: przyznawanie zezwoleń na wykonanie pewnych rozkazów, tj. częściowe lub całkowite kasowanie zawartości karty (z wyjątkiem obszaru producenta), reaktywacja numeru PIN, ładowanie elektronicznej portmonetki lub wykorzystanie funkcji szyfrowania / deszyfrowania. Klucz ten jest też wykorzystywany w procesie uwierzytelniania karty. Reaktywacja kodów PIN realizowana przy wykorzystaniu rozkazów chronionych kluczem master polega na odblokowaniu karty po przekroczeniu dozwolonej liczby kolejnych niepoprawnych wprowadzeń tajnego kodu. Nie oznacza to jednakże wymazania kodu i wydania nowego, lecz umożliwienie przeprowadzenia kolejnych prób. Klucze master są przechowywane zazwyczaj w postaci zaszyfrowanej. Natomiast użytkownik karty, w zależności od jej rodzaju, może posiadać od jednego do kilku kluczy, które umożliwiają mu dostęp do odrębnych funkcji.

Tabela 2

Metody uzyskiwania dostępu do pamięci karty

	METODY UZYSKIWANIA DOSTĘPU DO PAMIĘCI KARTY	OPIS I SPOSOBY PRZECIWDZIAŁANIA
DOSTĘP NIEPROFESJONALNY	**Modyfikacje prądu kasującego pamięć**	Modyfikacja połączeń układu scalonego umożliwia zablokowanie kasowania zawartości pamięci. Stosowane w kartach telefonicznych i telewizyjnych.
	Śledzenie poboru mocy	Mierzenie poboru mocy za pomocą programu umożliwia ustalenie zapisywanych informacji. Przeciwdziałanie: generowanie dziwnych poborów lub wykonywanie sztucznych operacji przez mikroprocesor.
	Zmiana napięcia zasilającego	Umożliwia skasowanie obszarów pamięci, blokadę operacji kasowania lub umożliwienie dostępu do chronionych obszarów pamięci. Przeciwdziałanie: odmowa pracy karty przy zmianie napięcia lub własne zasilanie karty.
	Zmiana częstotliwości	Umożliwia analizę sygnałów. Przeciwdziałanie: reakcja na przekroczenie minimalnej częstotliwości zegara, np. „uśpienie" układu.
	Częściowa blokada stanu układu	Powoduje destabilizację układu lub złamanie kluczy kryptograficznych. Przeciwdziałanie: taktowanie karty jej własnym zegarem.
	Kasowanie pamięci	Kasowanie za pomocą światła UV i promieniowania X oraz odczytywanie danych z karty za pomocą laserów UV. Przeciwdziałanie: stosowanie detektorów promieni UV, które mogą kasować pamięć w razie awarii, stosowanie liczników prób kasowania pamięci.
	DFA (ang. Differential Fault Analysis)	Wykorzystanie odmiennej pracy karty w warunkach ekstremalnych ułatwiające złamanie klucza kryptograficznego.
	Dostęp fizyczny	Uzyskiwany za pomocą wytrawienia z plastiku kwasem azotowym układu elektronicznego i jego połączeń. Przeciwdziałanie: stosowanie detektorów światła oraz detektorów połączeń układu scalonego, odmowa pracy po usunięciu obudowy ochronnej.
DOSTĘP PROFESJONALNY	**Odczytywanie zawartości pamięci**	Możliwe poprzez warstwowe zdejmowanie półprzewodnika. Przeciwdziałanie: „plątanie" adresów logicznych i fizycznych, atrapy komórek pamięci.
	Efekt Schatky'ego	Po wytrawieniu układu każda warstwa jest szlifowana i rozpyla się na niej warstwę metaliczną, co pozwala na poznanie struktury układu.
	Skanowanie z niobkiem litu	Skanowanie aktywności elektrycznej układu bez zasilania. Na wybranym elemencie układu kładzie się kryształki niobku litu i w przypadku aktywności tego elementu ulegają zmianie właściwości optyczne kryształu. Metoda bezinwazyjna opatentowana przez IBM.
	Analiza optycznej aktywności półprzewodników układu	Odbywa się za pomocą laserów IR (podczerownych). Metoda opatentowana przez Sandia National Laboratories.
	Podział układu	Podział na mniejsze części, które poddaje się analizie. Metoda opracowana na Uniwersytecie w Cambridge.
	Modyfikacja struktury mikroukładu karty (FIB – ang. Focussed Ion Beam)	Odbywa się za pomocą przerywania już istniejących ścieżek, tworzenia nowych i przebijania się przez warstwy mikroukładu. Przeciwdziałanie: kleje mocujące układ (kleje dekonstrukcyjne), detektory napięcia zasilania lub detektory oświetlenia.

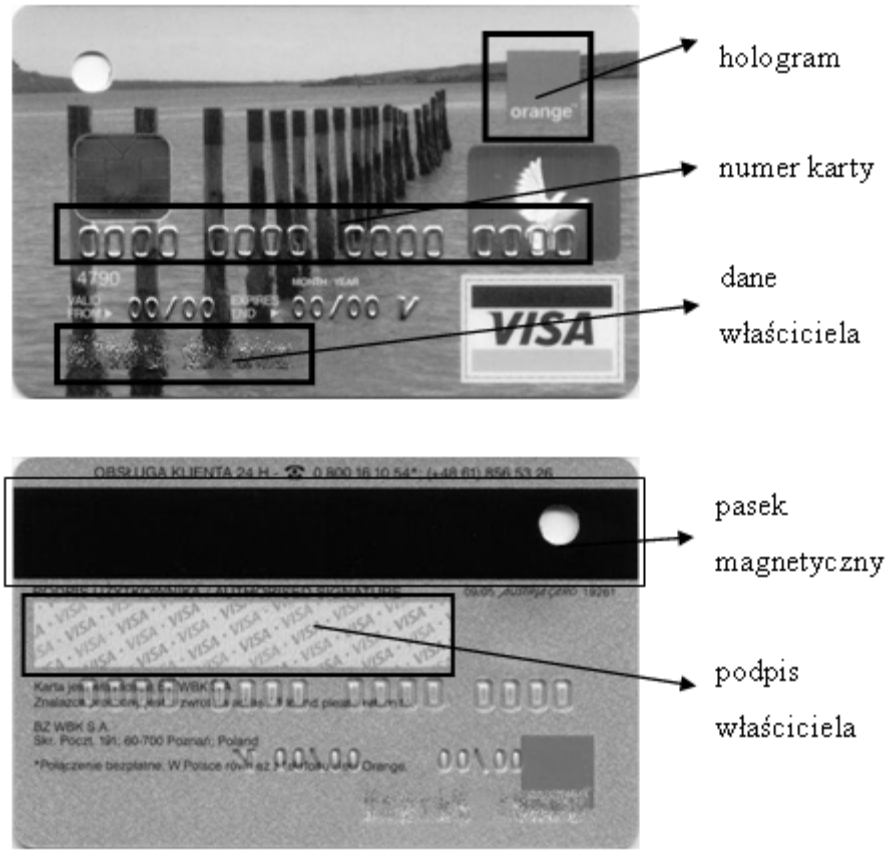
Źródło: Opracowanie własne na podstawie [KuMo2002].

Dodatkowo dla zwiększenia bezpieczeństwa w kartach płatniczych stosuje się proste metody zabezpieczeń możliwe do weryfikacji przez człowieka, tj.:

- numer karty – tłoczony, drukowany lub naniesiony laserowo,
- dane właściciela karty,
- typ karty,

- podpis właściciela,
- zdjęcie właściciela,
- hologram,
- symbole widoczne w świetle ultrafioletowym.

Na rysunku 2 przedstawiono niektóre metody zabezpieczeń kart elektronicznych.



Rys. 2. Przykładowe zabezpieczenia kart elektronicznych

Źródło: Galeria kart, [online]. Dostępny w Internecie: http://www.karty-online.net/gal1.php

Sposobami, które pozwalają zmniejszyć prawdopodobieństwo wystąpienia ataku, a także zmniejszyć straty, jeśli już do ataku dochodzi, są:

- maksymalizacja kosztów ataku – polegająca na zastosowaniu w karcie trudnych do sforsowania zabezpieczeń,

- minimalizacja wartości karty – sytuacja, w której koszt poniesiony na złamanie zabezpieczeń karty jest wyższy od ewentualnych zysków,
- budowanie wzajemnego zaufania poszczególnych elementów systemu, a także potwierdzania ich uprawnień do interakcji.

Dzisiaj nikt już nie kwestionuje roli kart elektronicznych w biznesie. Rozwój e-gospodarki oprócz ogromnych korzyści niesie ze sobą także ogromne zagrożenia. Są to nowe rodzaje niebezpieczeństw, często nierozumiane i niedoceniane. Największą przeszkodą w osiągnięciu potrzebnego poziomu bezpieczeństwa jest zbyt duże tempo zmian i stopni zaawansowania zagrożeń związanych z IT. Ponad połowa użytkowników uważa, że nie ma wystarczających możliwości, aby sprostać rosnącym zagrożeniom. Aby zapewnić prawidłowe funkcjonowanie e-biznesu, należy sprawnie i efektywnie zarządzać bezpieczeństwem transakcji. Należy pamiętać też, że eliminowanie zagrożeń to proces ciągły i niekończący się.

Literatura

1. Kubas, M., Molski, M., *Karta elektroniczna – bezpieczny nośnik informacji*, Warszawa, MIKOM, 2002.
2. Andrukiewicz E.: *Bezpieczeństwo systemów informacyjnych*, PCkurier 25/1998.
3. Ernst & Young: *Globalny raport o bezpieczeństwie informatycznym 2002*.
4. http://www.prim.com.pl/referaty.htm (08-12-2003).
5. http://www.kartyonline.net/gal1.php

ELECTRONIC CARD SECURITY IN E-BUSINESS

Summary

This paper describes the mechanisms used to control the security of information stored on electronic cards. Non-cash transactions with the usage of so-called "e-money" are performed with these cards. The advantages and disadvantages of various cardholder's authentication mechanisms are compared and a schematic procedure for identification is shown. Apart from the security of the data, the circuits themselves are also protected. The paper lists the methods of accessing the card's memory and describes the ways to overcome malicious trials of obtaining information sewn on a chip card.

Translated by Krystian Gembala and Tomasz Piesiur