STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Jadwiga ORYLSKA, Liwiusz SIEMIANOWSKI, Maciej NOSAL
Akademia Rolnicza w Szczecinie, Zakład Informatyki

BEZPIECZEŃSTWO TRANSAKCJI W BANKOWOŚCI INTERNETOWEJ

Streszczenie. Celem artykułu jest próba oceny bezpieczeństwa transakcji w bankowości internetowej.

Wskazano zagrożenia dla bezpieczeństwa transakcji. Opisano kwestie techniczne zachowania poufności i bezpieczeństwa transakcji, w tym szyfrowanie danych, podpis elektroniczny, certyfikacja, tokeny, metody identyfikacji klienta. Dokonano oceny stopnia skuteczności wykorzystywanych mechanizmów zabezpieczeń w polskich bankach internetowych.

Słowa kluczowe: bankowość internetowa, bezpieczeństwo transakcji.

THE INTERNET BANKING TRANSACTIONS SECURITY

Summary. The aim of the paper is an trial of assessment the transactions security in internet banking.

The review of used techniques of client identification was performed (including modern solutions as: electronic signature, tokens and simple entering the logname and user password). The example of technical structure of safe data maintenance, processing and transmission were specified (data encryptions, certification) The advantages/disadvantages of individual methods used in Polish internet banking were pointed.

Keywords: internet banking, transaction security.

1. Wprowadzenie

Bankowość internetowa (ang. Internet Banking) oznacza korzystanie z usług banku /oddziału elektronicznego (tzw. bank wirtualny) i prowadzenie transakcji (sprawdzanie stanu kont, zlecenia przelewu) przy wykorzystaniu do komunikacji sieci globalnej Internet.

Bankowość internetowa jest zbliżona do home bankingu, jednak klient wykorzystuje zwykłą przeglądarkę internetową. W home bankingu wymagane jest osobne bezpośrednie połączenie i specjalne oprogramowanie udostępniane przez bank

Zalety bankowości internetowej, w tym: możliwość korzystania z rachunku bankowego na dowolnym, podłączonym do Internetu komputerze, dodatkowe kanały elektroniczne (obok Internetu WAP), znacznie mniejsze w stosunku do banków tradycyjnych opłaty i prowizje oznaczają swobodny w czasie i przestrzeni dostęp do zgromadzonych na rachunku oszczędności oraz powodują wypieranie home bankingu.

Celem artykułu jest próba usystematyzowania i oceny skuteczności rozwiązań wykorzystywanych dla bezpieczeństwa transakcji w polskiej bankowości internetowej.

W artykule dokonano oceny bezpieczeństwa bankowości detalicznej, dla polskich klientów, bez uwzględnienia ofert skierowanych do klientów korporacyjnych. Oceniono banki świadczące usługi przez internetowy kanał dostępu na terytorium Polski (z pominięciem działających na ograniczonym obszarze banków spółdzielczych), jak: Bank Gospodarki Żywnościowej, Bank Przemysłowo-Handlowy PBK SA, Bank Zachodni WBK, Citibank, Deutsche Bank, Fortis Bank, ING Bank Śląski, Inteligo, LG Petro Bank, Lukas Bank, Mbank, MultiBank, Nordea, PeKaO SA, PKO BP, Volkswagen Bank Polska.

2. Potencjalne zagrożenia

Pojęcie bezpieczeństwa transakcji w systemie informatycznym funkcjonującym w Internecie należy rozumieć jako zastosowania możliwych i dostępnych zabezpieczeń technologicznych i metod organizacyjno-administracyjnych w celu ochrony transmisji przed przypadkowym lub celowym uniemożliwieniem, naruszeniem, przejęciem lub zniszczeniem. [2, 4].

Zagrożenia dla bankowości internetowej stanowią:

- ataki na serwery typu:
  - Denial of Service (DoS) – blokowanie/przeciążanie wybranych usług/zasobów sieciowych, jak procesy, miejsce na dysku, obciążenie procesora, modemy;
  - Ping of Death – przesyłanie pakietów przekraczających maksymalną dozwoloną długość, efektem czego następuje zawieszenie nie chronionego systemu;
  - SYN Flood – "zalanie" komputera setkami żądań nawiązania połączenia;
  - LAND Attack – przesyłanie pakietów z takim samym adresem i portem nadawcy oraz odbiorcy;

- IP Spoofing – przesyłanie pakietów ze sfałszowanym adresem źródłowym, przez co odbiorca błędnie identyfikuje nadawcę – tzn. podszywanie się pod inny komputer w sieci;
- wycieki przetwarzanych przez bank informacji, w tym poprzez niefrasobliwość klientów, najbardziej narażonych na potencjalną próbę przejęcia poufnych informacji,
- niewłaściwa konfiguracja mechanizmów ochronnych w przeglądarkach internetowych - użytkownik zmuszony jest do podejmowania decyzji w zakresie bezpieczeństwa, np. podczas instalacji pobranego z Internetu oprogramowania – niebezpieczeństwo infekcji wirusem lub wprowadzenia „konia trojańskiego",
- niedoskonałe algorytmy kryptograficzne o dostatecznie długich kluczach (128 bitów) w starszych, ale wciąż stosowanych wersjach przeglądarek,
- nie notyfikowane błędy oprogramowania użytkowego.

3. Metody zabezpieczeń

Najważniejsze metody zabezpieczeń transakcji w bankowości internetowej obejmują:

- szyfrowana transmisja danych,
- proste uwierzytelnienie,
- silne uwierzytelnienie,
- podpis elektroniczny.

Standardem szyfrowania danych w Internecie, wykorzystywanym przez wszystkie działające w Polsce banki, jest opracowany przez firmę Netscape protokół SSL (Secure Socket Layer zaimplementowany w najpopularniejszych przeglądarkach WWW - Netscape Communicator, MS Internet Explorer, Opera). Szyfrowanie odbywa się z wykorzystaniem algorytmów kryptograficznych: metoda kluczy symetrycznych i metoda kluczy niesymetrycznych [7].

Metoda kluczy symetrycznych opiera się na wykorzystaniu tego samego klucza do szyfrowania i deszyfrowania wiadomości. Zaletą metody jest szybkość i odporność na próby złamania bez pomocy klucza. Głównym niebezpieczeństwem jest możliwość przechwycenia klucza przy przekazywaniu odbiorcy, równoznaczna z utratą poufności transmisji.

Metoda kluczy niesymetrycznych polega na wykorzystaniu dwóch powiązanych kluczy: prywatnego (tajnego) i publicznego (jawnego). Dane szyfrowane są z pomocą klucza publicznego, nie wystarczającego do ich odtajnienia, odszyfrowane zaś kluczem prywatnym. Metoda zapewnia wysoki poziom bezpieczeństwa. Wadą jest złożoność i czasochłonność.

Metoda prostego uwierzytelnienia, tzw. identyfikator i hasło, wymaga od użytkownika podania określonych tajnych ciągów tajnych alfanumerycznych. Hasło jest narażone na przejęcie i wykorzystane przez osoby nieupoważnione, stąd metodę zalicza się do zapewniających stosunkowo niski poziom bezpieczeństwa.

Silne uwierzytelnienie opiera się na wykorzystaniu dodatkowych elementów zabezpieczających, jak token, certyfikat użytkownika, klucz prywatny. Token stanowi elektroniczne urządzenie uwierzytelniania użytkownika. Wykorzystuje algorytmy kryptograficzne (np. algorytm symetryczny, funkcja hashująca, generator pseudolosowy) oraz prywatne klucze kryptograficzne. W oparciu o klucz prywatny czas zsynchronizowany z serwerem i opcjonalnie inny ciąg cyfr generują hasło, które użytkownik wprowadza do odpowiednich formularzy na stronach WWW swojego banku.

Alternatywą dla drogich tokenów są listy jednorazowych haseł (ang. TAN - Transaction Authorisation Number) – specjalne karty zawierające listę jednorazowych kodów umożliwiających dokonanie transakcji na rachunku. Są wykorzystywane, gdy klient chce przeprowadzić operację ze zmianą salda – przelew-wpłata-wypłata. Zawierają listę jednorazowych kodów umożliwiających dokonanie transakcji. Każda lista TAN powiązana jest z nazwą i hasłem użytkownika. Niewykorzystane kody są zasłonięte substancją do ścierania (analogicznie jak karta konkursowa do losowania).

Podpis elektroniczny stanowi ciąg bitów dołączany do oryginalnej wiadomości. Uzależniony jest od klucza prywatnego nadawcy oraz od treści podpisywanych dokumentów. Identyfikacja nadawcy możliwa jest dzięki zaszyfrowaniu skrótu wiadomości/operacji bankowej kluczem prywatnym. Działanie podpisu elektronicznego opiera się na szyfrowaniu asymetrycznym, gdzie klucz prywatny należy do użytkownika rachunku, a publiczny do banku. Dane transakcji (np. jej kwota, numer rachunku, beneficjent) formatowane są w ciąg bitów, tzw. skrót – generowany przez funkcję wiążącą dane transakcji z charakterystyczną dla nich wartością liczbową z ustalonej dziedziny wartości.

Skrót posiada istotne dla identyfikacji autentyczności transmisji właściwości:

- zmiana treści wiadomości (operacji bankowej) pociąga za sobą niemożliwą do przewidzenia zmianę skrótu;
- niemożliwość odtworzenia oryginalnej wiadomości na podstawie skrótu,
- unikalność skrótu – funkcja generująca nie wytworzy identycznego skrótu dla dwóch różnych wiadomości,
- stała długość, niezależna od długości dokumentu.

Stosowanie systemu podpisów elektronicznych wymaga urzędów i ośrodków certyfikacji, np. Centrum Unizeto w Szczecinie [8] zobowiązanych do ponoszenia odpowiedzialności za

bezpośrednie i pośrednie szkody, będące wynikiem niezgodności weryfikacji. W Unizeto Centrum kwoty odszkodowań wahają się od 400 PLN do nawet 100.000 PLN.

Nośnikami kluczy publicznych wykorzystywanych w procedurze podpisu elektronicznego są certyfikaty [5]. Pozwalają one na potwierdzenie tożsamości posiadacza klucza prywatnego. Certyfikaty wydawane są przez specjalnie powołane do tego urzędy – tzw. Centra Certyfikacji. Krajowymi wystawcami certyfikatów są: Unizeto Centrum, TPInternet Signet, E-Telbank POLCERT oraz Krajowa Izba Rozliczeniowa. Możliwe jest również skorzystanie z instytucji tzw. zaufanej trzeciej strony (ang. Third Trusted Party), potwierdzającej prawdziwość zawartych w certyfikacie informacji i udostępnienie klucza publicznego. Zabezpieczeniem transakcji są również tzw. zapory ogniowe (ang. Firewalls), stanowiące sprzętowe i programowe systemy zabezpieczeń serwerów banku przed niepowołaną infiltracją.

Spotykane są dodatkowe formy ochrony/zabezpieczeń:

- indywidualne limity kwotowe – możliwość określenia przez klienta maksymalnej kwoty jednorazowej operacji wykonanej w banku internetowym i/lub wszystkich transakcji realizowanych jednego dnia; polecenie przekraczające limit nie zostanie wykonane;
- monitoring nieaktywności – wymuszanie ponownej identyfikacji użytkownika po dłuższym okresie bezczynności,
- blokada konta – zamknięcie dostępu do konta po kilkakrotnym nieprawidłowym logowaniu,
- rejestracja aktywności – zapis działań użytkownika (np. próby logowania do systemu, wykonywane operacje, adres IP użytkownika).

4. Zabezpieczenia w polskich bankach internetowych

Wydaje się, że poziom zabezpieczeń banków internetowych działających w Polsce nie jest jednakowy (tabl.1). Stosowane są wszystkie przedstawione metody od prostego uwierzytelniania do podpisu cyfrowego. Wszystkie banki poddane ocenie zapewniają transmisje danych na bazie protokołu SSL i 128-bitowy klucz w symetrycznym algorytmie szyfrowania.

Wykorzystanie identyfikatora i hasła użytkownika (CitiBank i LG Petro Bank) do rozporządzania kontem nie gwarantuje bezpieczeństwa. W CitiBanku identyfikatorem jest numer karty kredytowej. W procesie uwierzytelnienia użytkownika stosowany jest tzw. i-PIN liczący do 12 cyfr długości (w miejsce czterocyfrowego PIN karty kredytowej) Rozwiązanie ustępuje tokenom oraz podpisowi elektronicznemu. Podstawową wadą jest niezmienność stosowanych ciągów cyfrowych, co zwiększa ryzyko przejęcia hasła w perspektywie

czasowej, np. przez użycie programu typu "koń trojański". Konieczne jest stosowanie dodatkowych zabezpieczeń w postaci firewalli i programów antywirusowych. Zwiększa to koszty klientów oraz ogranicza dysponowanie rachunkiem bankowym do miejsc w pełni bezpiecznych (domu).

Metody uwierzytelniania z listą haseł jednorazowych wykorzystują: Inteligo, mBank, Multibank, Nordea, Deutsche Bank. Dodatkowe zabezpieczenia w postaci „zdrapek" zasłaniających niewykorzystane kody stosuje Deutsche Bank w przypadku kart Inteligo,. Brak wymienionego zabezpieczenia (np. w listach TAN mBanku) sprawia, że mogą one zostać powielone bez wiedzy użytkownika.

Rozpowszechnione zabezpieczenia w postaci tokenów (np. Lukas Bank, Volkswagen Bank Polska, PKO BP) uznać można za wystarczające [6]. Zaletą rozwiązań jest zwiększona mobilność użytkownika, który w łatwy sposób może korzystać z rachunku bankowego także na innych komputerach.

Bardzo dobrze zabezpieczone banki w autoryzacji transakcji wykorzystują podpis elektroniczny (Bank Śląski, BPH i Fortis Bank). Klucz prywatny jest przechowywany przez użytkownika (najlepiej na nośniku wymiennym). Istnieje możliwość przechowywania klucza na serwerze banku i tym samym korzystania z rachunku na innym komputerze. Dostęp do klucza prywatnego chroniony jest jednak tylko za pomocą dodatkowego hasła, co naraża na utratę poufności.

Dodatkowym zabezpieczeniem wykorzystywanym przez Fortis Bank jest wystawiany dla każdego klienta certyfikat. Jego autentyczność bank weryfikuje przy każdorazowej próbie otwarcia dostępu do rachunku. Certyfikat instalowany jest w przeglądarce WWW użytkownika.

Tablica 1

Zestawienie mechanizmów zabezpieczeń wykorzystywanych przez poszczególne banki

Nazwa banku adres WWW	Protokół transm.	Metody uwierzytelnienia		
		Proste	Silne	Dodatkowe
BGŻ www.bgz.pl	SSL/SGC	Użytkownik, hasło dostępu	Chroniony PIN'em token DigiPass	–
BPH www.bphpbk.pl	SSL/SGC	Użytkownik, maskowane hasło dostępu	Klucz prywatny chroniony hasłem	Podpis elektroniczny, klucz prywatny przechowywany w banku lub na dysku użytkownika
BZ WBK www.bzwbk.pl	SSL	Użytkownik, hasło dostępu	Chroniony PIN'em token DigiPass	–
CitiBank www.citibank.pl	SSL	Numer karty, i-PIN	–	–

cd. tablicy 1

Deutsche Bank www.deutsche-bank.pl	SSL	Identyfikator, numer karty kodów TAN, PIN	Lista jednorazowych haseł TAN; zastaw 10 pytań osobistych	–
Fortis Bank www.fortisbank.pl	SSL/SGC	Użytkownik, hasło dostępu	Klucz prywatny chroniony hasłem, certyfikat klienta wystawiony przez bank	podpis elektroniczny (160 bitów szyfrowanych kluczem DSA 512-bitowym), klucz prywatny na dyskietce
ING Bank Śląski www.ingbankonline.pl	SSL/SGC	Użytkownik, maskowane hasło dostępu	Klucz prywatny chroniony hasłem	Podpis elektroniczny, klucz prywatny przechowywany w banku lub przez użytkownika
Inteligo www.inteligo.pl	SSL	Użytkownik, hasło dostępu	Lista jednorazowych haseł TAN	–
LG Petro Bank www.lgpetro.com.pl	SSL	Użytkownik, hasło dostępu	–	–
Lukas Bank www.lukas.pl	SSL/SGC	Użytkownik, hasło dostępu	Token RSA SecureID	–
Mbank www.m-bank.com.pl	SSL/SGC	Użytkownik, hasło dostępu	Lista jednorazowych haseł TAN	–
MultiBank www.multibank.pl	SSL/SGC	Identyfikator, hasło dostępu (od 8 do 20 znaków – przynajmniej jedna cyfra i jedna litera)	Lista jednorazowych haseł (hasła 6-cyfrowe)	–
Nordea www.nordeabank.pl	SSL/SGC	Identyfikator (minimum 8 znaków), jednorazowe hasło dostępu	Lista jednorazowych haseł lub chroniony hasłem token – w zależności od wyboru klienta	–
Pekao S.A. www.pekao.com.pl	SSL/SGC	Użytkownik, hasło dostępu	Chroniony PIN'em token DigiPass	–
PKO BP www.pkobp.pl	SSL	Użytkownik, hasło dostępu (od 6 do 20 znaków)	Token ActiveCard	–
Volkswagen Bank Polska www.vwbankdirect.pl	SSL	Użytkownik, hasło dostępu	Token RSA SecureID	–

5. Wnioski

Wielość mechanizmów zabezpieczeń stosowanych w polskich bankach internetowych powoduje zróżnicowanie poziomu bezpieczeństwa.

Najwyższy stopień bezpieczeństwa transakcji zapewnia system z podpisem elektronicznym oraz tokeny i listy TAN. Zastosowania z prostym uwierzytelnieniem powinny ograniczać się do sprawdzania stanu rachunku bez wykonywania dyspozycji.

Konieczne jest przestrzeganie zasad bezpiecznego wykorzystania rachunku – tj. łączenie się ze sprawdzonych miejsc i komputerów z zainstalowanym oprogramowaniem przeciwwirusowym i firewall'em.

Wydaje się, że wysoka funkcjonalność i wygoda korzystania z banków wirtualnych będzie powodować stałe rozpowszechnianie tej formy bankowości. Konieczną determinantą jest jednak łatwiejszy – tańszy dostęp do Internetu i ewentualnych opłat certyfikacyjnych i autoryzacyjnych.

LITERATURA

1. Brzozowska K.: Banki i ich działalność. Akademia Rolnicza w Szczecinie, 2001.
2. Frąś J., Serdyński A.: Organizacyjne problemy bezpieczeństwa systemu informatycznego w instytucjach gospodarczych. Technologia informatyczna i systemy sieciowe w edukacji i przygotowaniu zawodowym, Uniwersytet Szczeciński, 2002.
3. Mańka J., Krupa W., Krupa K.: Strategia bezpieczeństwa informacji.. IV Konferencja „Ekonomiczne Aspekty Globalizacji Informacji", Instytut Informatyki w Zarządzaniu, Uniwersytet Szczeciński, 2001.
4. Orylska J.: Ochrona danych w systemach komputerowych, Informatyka w dydaktyce i zastosowaniach, Zeszyt nr 3, Akademia Rolnicza w Szczecinie, 2000.
5. Paluszyński W.: Infrastruktura klucza publicznego – szansą na stworzenie jednolitej platformy bezpieczeństwa dla e-commerce. Ekonomiczne Aspekty Globalizacji Informacji, Instytut Informatyki w Zarządzaniu, Uniwersytet Szczeciński, 2001
6. Rozdobutka P.: Bezpieczeństwo w bankowości internetowej. Akademia Rolnicza w Szczecinie, 2003, praca dyplomowa zrealizowana pod kierunkiem dra Liwiusza Siemianowskiego w Zakładzie Informatyki AR.
7. Ryznar Z.: Klucze zaufania. Gazeta Bankowa, 13-19 listopada 2001.
8. Unizeto Centrum, Kodeks Postępowania Certyfikacyjnego, http://www.certum.pl/CPS.

Recenzent: Dr inż. Marcin Skowronek

Wpłynęło do Redakcji 29 marca 2003 r.

Abstract

The aim ot the paper is an trial of assessment the transactions security in Polish internet banking. The existing dangers for data transmitting were specified. The review of used techniques of client identification was performed (including modern solutions as: electronic signature, tokens and simple entering the logname and user password).

The rules of decreasing risk of unauthorized bank account usage/password interception were also pointed. The example of technical solutions of safe data maintenance, processing and transmission were specified (data encryptions and certification). The advantages/disadvantages of individual methods were additionally pointed.

Adresy

Jadwiga ORYLSKA: Akademia Rolnicza w Szczecinie, Zakład Informatyki Ul. Monte Cassino 16, 70-466 Szczecin, Polska, orylska@ekon.ar.szczecin.pl , orylska@e-ar.pl

Liwiusz SIEMIANOWSKI: Akademia Rolnicza w Szczecinie, Zakład Informatyki Ul. Monte Cassino 16, 70-466 Szczecin, Polska, livius@erl.edu.pl, livius@e-ar.pl

Maciej NOSAL: Akademia Rolnicza w Szczecinie, Zakład Informatyki Ul. Monte Cassino 16, 70-466 Szczecin, Polska, maciej@erl.edu.pl