Zygmunt Ryznar

Bezpieczeństwo bankowości internetowej

(stan na rok 2002)

Świadomość zagrożeń jest niewielka

Światowa sieć internetowa WWW składa się z tysięcy fizycznych sieci komputerowych i działa w niej wiele firm operatorskich (3500 tylko w USA) oraz ponad 100 milionów użytkowników. Ruch komunikacyjny jest więc w niej ogromny i miejsc do ewentualnego ataku hakerskiego jest wiele. O słabości całej sieci decydują nasłabsze jej ogniwa (przez nie można wprowadzić konia trojańskiego), każdy węzeł sieci musi podlegać tym samym rygorom, najlepiej zabezpieczać już na poziomie terminali i stacji roboczych (czyli tam gdzie można wejść do systemu). Rozwój łączności radiowej, satelitarnej stwarza szerokie możliwości omijania konieczności fizycznego podłączania się do okablowania sieci.

Internetu na początku używano głównie do celów marketingowych, a potem rosło jego użycie do transakcji w ramach rozwijającego się handlu elektronicznego e-commerce bankowych (wg szacunków IDC w roku 2002 wartość transakcji zawieranych za pośrednictwem internertu sięgnie 327 mlrd dolarów rocznie). *Tymczasem bezpieczeństwo transakcji elektronicznych przedstawia jak na razie wiele do życzenia.* Wg Reutersa przestępstwa internetowe *(cybercrimes)* dotknęły w 2000 roku 2/3 firm brytyjskich. Najczęstszymi rodzajami nadużyć było hakerstwo, wirusy i przestępstwa związane z kartami płatniczymi. FBI i SANS Institute opracowały w 2001 roku listę 20 głównych luk bezpieczeństwa (vulnerabilities) systemów podłączanych do internetu.

Swiadomość konieczności stosowania zabezpieczeń w sieciach internetowych w firmach nie jest wysoka, zaś często ryzyko niedostatecznego zabezpieczenia świadomie wkalkulowane jest w koszty biznesu. Wg ankiety rozpisanej przez Datapro w połowie lat 90-tych tylko 15% respondentów stosowało szyfrowanie a 28% firewall . Wg analityków firmy Gartner do roku 2001 rządy i biznes będą łożyć na zabezpieczenie informacji 10 razy więcej środków niż obecnie (amerykańskie firmy wydają na to 1% dochodów). Wg tego samego źródła do 2004 roku 80% przedsiębiorstw będzie używało internetu jako organicznej części swego biznesu i połowa z nich będzie ponosić poważne konsekwencje finansowe incyndentów w sieci internetowej.

Przykłady zrealizowanych zagrożeń

a)Znane są fakty udanych ataków hakerów na strony Białego Domu, Senatu, FBI i armii amerykańskiej.
b)Kiedy w lipcu 1997 roku awarii uległ serwer InterNIC ogromna liczba łączy na całym świecie przestała działać.
c)Na początku lutego 2001 roku "włamano" się do serwerów obsługujących Światowe Forum Gospodarcze w Davos i ukradziono bazę danych osobowych, zawierającą m.i. adresy poczty elektronicznej i numery kart płatniczych, po czym dokonano szeregu nielegalnych operacji finansowych. W wyniku tego musiano zablokować wiele kart płatniczych.
d)W Waszyngtonie w październiku 2001 roku hakerzy przejęli bazę fimy handlującej elektronicznie, zawierającą informacje zakupowe łącznie z numerami kart płatniczych Visa i dokonali szeregu transakcji na ich konto. W wyniku tego zastosowano radykalny środek ratunkowy polegający na wycofaniu dotychczasowych kart i zastąpieniu ich nowymi.
e)29 stycznia 2001 roku ogłoszono, iż moduł BIND w serwerach DNS zawiera przeoczenia umożliwiające wychwytywanie adresów przez hackerów, co spowodowało zagrożenie dla każdej instytucji posiadającej strony internetowe lub korzystającej z poczty elektronicznej.
e)W kwietniu 2001 roku opublikowano, iż w serwerze Windows2000 współpracującym z usługami internetowymi (IIS) wykryto błąd pozwalający hakerowi przesłanie na serwer dowolnej aplikacji i jej uruchomienie.
e)W połowie 2001 roku wykryto błąd w oprogramowaniu IOS firmy CISCO, umożliwiający krakerom - poprzez żądanie okreslonego URL z serwera - ominięcie procedury autentyfikacji i działanie na najbardziej uprzywilejowanym poziomie 15, pozwalającym na przejęcie kontroli nad routerami i switchami używającymi IOS oraz protokołu HTTP.

Raporty o włamaniach (incindents) i podatności systemów na włamania (vulnerabilities) publikowane są przez CERT (Community Emergency Response Teams)Cordination Center (zlokalizowanym w Carnegie Melon University) i dane te charakteryzuje silna tendencja wzrostowa (w 1999 roku 9859 włamań, 2000-21756, w I kw 2001-7456). Od roku 1988 odnotowano 54758 włamań oraz 3229 błędów w zabezpieczeniach.

Zabezpieczenia

Konieczność zabezpieczeń dotyczy głównie fizycznych adresów telekomunikacyjnych IP, przesyłanych informacji oraz autentyfikacji uzytkowników.

W pakietach sieciowych TCP/IP (stosowanych w internetowym protokole HTTP) znajdują się adresy, które mogą się stać przedmiotem penetracji zawodowych włamywaczy. Zwykle są to adresy źródła i przeznaczenia, niejednokrotnie skomplikowane (np. zagnieżdżone) przez złożoność routingu sieciowego i dlatego podawane są też adresy węzłów/przełączników na drodze połączeń międzysieciowych. W przypadku internetu numeryczne adresy IP przechowywane są w serwerach nazw domen DNS, w których najprościej mówiąc nazwie przyporządkowany jest numer umożliwiający rozsyłanie informacji emailowych po sieci do miejsca przeznaczenia i dostęp do stron internetowych. 29 stycznia 2001 roku ogłoszono, iż moduł BIND dokonujący tej konwersji zawiera przeoczenia umożliwiające wydostawanie adresów przez hackerów, co spowodowało zagrożenie dla każdej instytucji posiadającej strony internetowe lub korzystającej z poczty elektronicznej.

Ochrona adresów (4 liczb oddzielonych kropkami np.124.139.578.99) zawartych w pakietach IP następuje poprzez ich ukrywanie (tunelowanie), zas ochrona przed atakami intruzów jest możliwa poprzez firewall i mechanizmy wbudowane do routerów (filtrowanie wg kombinacji adresu docelowego, źródłowego, numeru protokołu oraz numeru portu). Mechanizm NAT (Network Address Translation) pozwala na dzielenie jednego adresu IP przez wiele komputerów w sieci lokalnej a równocześnie zabezpiecza przed programami skanującymi adresy IP (mogą one rozpoznać tylko router NAT a nie adresy lokalnych komputerów). Poza pakietami typu IP, w sieciach internetowych występują również pakiety ICMP, TCP, UDP, charakteryzujące się odmiennymi strukturami.

Transakcje internetowe wymagają zabezpieczenia, które pozwoli na stwierdzenie autentyczności (non-repudiation) osoby dokonującej transakcji. Wśród zabezpieczeń najpopularniejsze staje się tworzenie ścian zaporowych (firewalls) mających na celu wykrycie nieuprawnionych użytkowników sieci oraz generowanie przez serwer bezpieczeństwa "biletów" (tokenów) użytkownika z hasłami ważnymi tylko na przeciąg jednej sesji. W transmisji danych obowiązuje zasada kodowania danych.

Treść transakcji powinna być ukryta przed osobami niepowołanymi. Komunikaty powinny być kompresowane, szyfrowane rozmaitymi metodami (kluczami i "hashami") i sygnowane podpisem elektronicznym oraz/lub tokenem aby maksymalnie utrudnić dostęp osobom niepowołanym (hakerom itp). Tokeny stosowane są m.i. w bankowych usługach internetowych Pekao SA, PKO BP i Lukas Banku. Uruchomienie tokena wymaga znajomości cyfrowego (np. 6-znakowego) kodu, który właściciel tokena powinien ustalać sobie sam. Po kilku nieudanych próbach token jest zwykle automatycznie blokowany. Token jest to unikatowy ciąg cyfr istniejący tylko podczas wykonywania transakcji (sesji) przez prawowitego klienta. Nazwą tą określane jest również urządzenie kryptograficzne do generowania takiego ciągu cyfr.

Podstawową metodą zabezpieczania treści wiadomości pozostaje szyfrowanie (kryptografia) danych za pomocą tzw. kluczy i złożone algorytmy "routowania" (mające na celu ukrycie drogi przebiegu informacji) oraz ciągła weryfikacja wszystkich procesów pojawiających się w sieci.

Istnieje wiele algorytmów szyfrowania, klasyfikowanych jako symetryczne lub asymetryczne. W metodzie symetrycznej do kodowania i rozkodowania używa się tego samego - generowanego - klucza tajnego. W algorytmie asymetrycznym komunikat po stronie wysyłającej jest szyfrowany dwoma kluczami: prywatnym (tajnym) strony wysyłającej oraz publicznym (jawnym) kluczem strony odbierającej.

Asymetryczność polega na tym, iż strona odbierająca używa do rozszyfrowania swój klucz prywatny (jako podstawa rozszyfrowania swojego klucza publicznego i publiczny klucz nadawcy (jako podstawa weryfikacji podpisu elektronicznego nadawcy). Para kluczy (prywatny i publiczny) znajduje

się we wzajemnej zależności matematycznej - takiej, że na podstawie klucza prywatnego łatwo oblicza się odpowiadający mu klucz publiczny, natomiast odwrotna zależność ("złamanie" klucza prywatnego na podstawie klucza publicznego) jest prawie niemożliwa do wykrycia - "prawie" gdyż zdarzył się przypadek odczytania klucza prywatnego OpenPGP) przez czeskich kryptologów z firmy Decros/ICZ.

W praktyce - w celu przyśpieszenia transmisji danych - stosowane jest szyfrowanie hybrydowe, używające obu powyższych metod. Polega to na kodowaniu pełnej treści komunikatu za pomocą metody symetrycznej, np. przy użyciu klucza 128 bitowego,8 oraz stosowaniu szyfrowanych asymetrycznie elementów: skrótu elektronicznego i podpisu elektronicznego,. Skrót elektroniczny jest obliczany w taki sposób aby zapewnić spójność informacji, czyli wykryć ewentualne zmiany jakie mogą zajść podczas transmisji (w wyniku błędów przesyłania lub umyślnego zniekształcenia przez włamywacza). Po odebraniu i rozszyfrowaniu komunikatu skrót ten jest obliczany, a następnie porównywany ze skrótem odszyfrowanym z podpisu. Podpis cyfrowy polega na szyfrowaniu skrótu wiadomości kluczem prywatnym nadawcy, zaś do jego odczytania niezbędne jest posiadanie przez odbiorcę klucza publicznego nadawcy. Warunkiem posługiwania się metodą asynchroniczną jest więc znajomość kluczy publicznych strony drugiej. Klucze te udostępniane powinny być przez centrum autoryzacyjne (Certification Authority) dysponujące bazą kluczy jawnych. Klucze udostępniane być mogą też przez internetowe serwery kluczy publicznych np. pgp-public-keys@keys.pgp.net. Właściciel klucza publicznego może usunąć swój "złamany" klucz i wprowadzić nowy.

Do najbardziej znanych metod należą: symetryczne algorytmy DES (DES - Data Encryption Standard- został wprowadzony przez Rząd Federalny USA) i jego odmiana Triple-DES, IDEA,RC2,RC4 oraz asymetryczny algorytm RSA RSA Rivest-Shamir-Adleman (twórcy kryptosystemu). W systemie RSA klucze (publiczny i prywatny) są funkcjami pary dużych (100-200 cyfrowych) liczb pierwszych.. Metody szyfrowania danych stale ulegają doskonaleniu ze względu na zdarzające się ich "złamania" przez hakerów. Przykładowo, w 1994 roku złamano 128 bitowy publiczny klucz RSA, w związku z powyższym opracowane są klucze ponad 1024 bitowe (do 4096 bitow w Open PGP). *Skrótowo tłumacząc, klucz publiczny odbierającego służy do szyfrowania wiadomości przez nadającego, natomiast klucz prywatny odbierającego- wraz z kluczem publicznym nadającego - służy do deszyfracji wiadomości szyfrowanej jego kluczem publicznym.* Klucz prywatny odbierającego jest więc warunkiem poprawnego odczytania wiadomości. Klucz prywatny nadającego jest używany do tworzenia podpisu elektronicznego nadawcy i uczestniczy również w szyfrowaniu, stąd aby sprawdzić autentyczność podpisu odbierający musi posiadać klucz publiczny nadającego.

Podpis elektroniczny obliczany jest w standardzie PGP przez funkcje "hash" (np. Message Digest 5 - MD5 lub Secure Hash Algorithm 1 - SHA1) dla skrótu elektronicznego wiadomości i następnie szyfrowany przez klucz prywatny RSA lub/oraz DSA. Skrót elektroniczny posiada stałą długość (najczęściej 16-20 bajtów) i w uproszczeniu jest odpowiednikiem sumy kontrolnej lub kodu kontrolnego CRC. Podpis elektroniczny towarzyszy wiadomości. Jest on po stronie adresata rozszyfrowywany kluczem publicznym nadawcy i odbiorca w ten sposób otrzymuje skrót ustalony przez nadawcę. W celu uzyskania pewności, że zarówno nadawca jak i wiadomość są autentyczne, adresat oblicza wg tego samego algorytmu we własnym zakresie skrót wiadomości i dopiero jeśli oba te skróty są identyczne wiadomość może być akceptowana.

Klucze publiczne przechowywane w repozytorium certyfikatów składają się z części nagłówkowej (nazwy właściciela i daty utworzenia) i materiału kodowego, natomiast klucze prywatne szyfrowane są dodatkowym hasłem (na wypadek kradzieży).

W celu zabezpieczenia transmisji danych protokół HTTP wzbogacany jest o mechanizmy szyfrujące, np. SSL (Secure Socket Layer) stosujący cyfrowe certyfikaty i podpisy, szyfrowanie symetryczne i niesymetryczne skompresowanych danych i zabezpieczenie przed zmianami poprzez kody MAC (Message Authentication Code).

W bankowych serwisach internetowych (też w Polsce) wykorzystywane jest symetryczne szyfrowanie wiadomości wg protokołu SSL (Secure Sockets Layer), zazwyczaj w Europie (USA i Kanada nie posiadają ograniczeń w dostępie do długich kluczy szyfrowania) przy użyciu klucza 128 bitowego oparte na standardzie SGC (Server Gated Cryptography), umozliwiającym wykorzystanie przeglądarek szyfrujących 40-bitowo do obsługi transakcji szyfrowanych 128-bitowymi kluczami. Poza szyfrowaniem transakcja jest sygnowana podpisem elektronicznym oraz/lub tokenem.

Bankowe usługi internetowe zabezpieczane są w różnorodny sposób:

- ściany zaporowe (firewall)
- certyfikat potwierdzający połączenie autentycznego użytkownika z autentyczną witryną banku (poprzez pary publicznych i prywatnych kluczy o długości co najmniej 1024 bitów, czyli kryptografię niesymetryczną np.algorytmem RSA)
- zabezpieczenie transmisji poprzez szyfrowanie wiadomości (np. 128-bitowym protokołem SSL)
- hasło zabezpieczające do klucza prywatnego
- stosowanie wirtualnej klawiatury do wprowadzania haseł
- identyfikator użytkownika (nadany przez bank)
- hasło użytkownika i blokowanie dostępu po kilku probach podania niewłaściwego hasła
- autentyfikacja poprzez "powitalne uściśnięcie rąk" (handshaking) polegające na wymianie ustalonych (i przepuszczanych przez funkcje "hashowania") komunikatów pomiędzy serwerem a użytkownikiem
- klucz sesyjny lub transakcyjny (token) do zabezpieczenia transmisji, generowany np. technologią kryptografii symetrycznej kluczem o długości 128 bitow
- sygnowanie transakcji podpisem elektronicznym.

Usługi internetowe w polskich bankach zabezpieczane są z wykorzystywaniem większości powyższych możliwości. Niektóre banki (mBank) stosują dodatkowe zabezpieczenia w postaci predefiniowanych przelewów (i na wcześniej zdefiniowane konto) i jednorazowych haseł na inne przelewy. BPH stosuje losowo dobierane znaki hasła aby utrudnić podsłuchiwanie haseł przez konia trojańskiego. W systemach BPH i BŚK uzytkownicy identyfikowani są nie tylko podczas logowania, lecz również przed wykonaniem każdego przelewu. Uchwalona 27 lipca 2001 roku przez Sejm ustawa o podpisie elektronicznym stworzyła nowe możliwości wzmocnienia bezpieczeństwa.

Podsumowanie stanu rzeczy

Metody zabezpieczeń:

◊ *firewall (zapora ogniowa, ściana zaporowa)* stwarzający zaporę dla hackerów i innych nieupoważnionych osób.
Generalnie "ściany zaporowe" można podzielić na 3 grupy: działające na poziomie pakietów danych (nie przechowywują one informacji kto z kim rozmawiał), na poziomie IP (przechowywany jest szczegółowy protokół połączenia) i proxy (pamiętające historię połączeń, włączając e-maile i wykonywane strony internetowe).

◊ stosowanie w sieci IP (Internet Protocol) metody szyfrowania ESP (Encapsulating Security Payload) w wersji “transport made” zgodnej z dokumentem RFC1827, polegającej na tym, że szyfrowaniu podlega nie tylko pakiet danych lecz również adresy nadawcy i odbiorcy oraz nagłówek autentyfikacyjny W prywatnych sieciach wirtualnych (VPN) stosuje się tzw. tunelowanie (obudowanie/umieszczanie pakietów IP w innymi datagramach), mające na celu stworzenie bezpiecznego połączenia pomiędzy dwoma punktami znajdującymi się w tej samej sieci. Ulegają wówczas utajnieniu adresy obu stacji.

◊ stosowanie bezpiecznych metod przesyłania elektronicznych komunikatów w dziedzinie biznesu elektronicznego (electronic commerce): X12.58 EDI, S/MIME i PGP/MIME /, SET, TLS/ SSL SSH, IPSec, certyfikaty X.509 (standard podpisu elektronicznego), ANSIX9F1(norma ta narzuca minimalne długości 1024 bitów dla RSA i DH.). Wg badań przeprowadzonych przez NAI Labs w czerwcu 2000 roku oferta produktów kryptograficznych o zasięgu światowym (worldwide) obejmowała 1675 pozycji. 849 pozycji - a więc połowę - opracowano poza USA. W co najmniej 249 produktach zastosowano mocne algorytmy kryptograficzne - Triple DES, IDEA, BLOWFISH, RC5, CAST.

◊ stosowanie programów z zakresu sztucznej inteligencji typu “intrusion detection” do wykrywania prób włamań i włamań dokonanych do sieci i systemów komputerowych.

◊ w przypadku transakcji dokonywanych za pośrednictwem kart płatniczych zaleca się stosowanie kart chipowych a nie magnetycznych., gdyż te drugie jest łatwo skopiować za pomocą łatwo dostępnych i stosunkowo tanich (za kilkaset dolarów) urządzeń. W Polsce w 2000 roku wartość transakcji dokonanych kradzionymi lub sfałszowanymi kartami magnetycznymi stanowiła 0.15% łącznej wartości operacji tego kanału płatniczego

Szyfrowanie danych i technologia podpisów elektronicznych są podstawowymi metodami zabezpieczania transakcji elektronicznych. Czołowe firmy obsługujące karty płatnicze (Visa, MasterCard, Europay) oraz szereg firm software'owych utworzyły konsorcjum SET (Secure Electronic Transaction), ktorego celem było opracowanie i wdrożenie protokołu finansowych transakcji w internecie i innych otwartych sieciach. W Europie sprawami bezpieczeństwa sieci zajmują się stowarzyszenia CAFE (Conditional Access For Europe) i SEMPER (Secure Electronic Market Place for Europe). W 2001 roku Komitet Bazylijski d/s Nadzoru Bankowego (Basel Committe on Banking Supervision) wydał raport na temat zarządzania ryzykiem w bankowości elektronicznej ("Risk Management Principles for Electronic Banking").