Študentská vedecká a odborná činnosť
Fakultné kolo, 29. apríl 2009
Fakulta elektrotechniky a informatiky STU Bratislava

Zabezpečenie internet banking-u a spôsoby ochrany komerčných bank a ich klientov

Bc. Martin Hrušovský *FEI STU v BA* *martin.hruso@gmail.com*

Abstrakt

Internet banking - pojem ktorý ešte pred dvomi desaťročiami nikomu nič nehovoril a dnes by sme si bez neho život už ťažko vedeli predstaviť. Platenie našich účtov za telefón, internát, internet, televíziu ako aj internetové obchody, bankomaty a post terminály sú len letmou odrodou možného využitia služby poskytovanej všetkými komerčnými bankami.
Peniaze už dávno neskrývame pod matracom, ale ich ukladáme v komerčných bankách.

1. Úvod

Internet banking zrýchlil naše životy, umožnil rýchly bezhotovostný transfér našich peňazí po celom svete. S bankomatovou kartou tak môžeme mať pri sebe bezpečne svoje peniaze kedykoľvek k dispozícii. Nové technológie však priniesli so sebou aj nové hrozby a na to, aby naše peniaze boli naozaj v bezpečí je vhodné byť o týchto hrozbách informovaný.
Zamykáme si svoje byty na niekoľko zámkov, do našich áut si nechávame inštalovať rôzne doplňujúce bezpečnostné zariadenia, ale ako si chránime naše peniaze? S rozvojom internetu a internetového bankovníctva narastá aj počet útokov, ktorých cieľom je zneužiť citlivé údaje užívateľov. Nie sme bezmocní, bezpečnosť ale musí dodržiavať každý, kto je zapojený do elektronickej komunikácie. Ako banka, tak aj jej klient.

2. Phishing a pharming

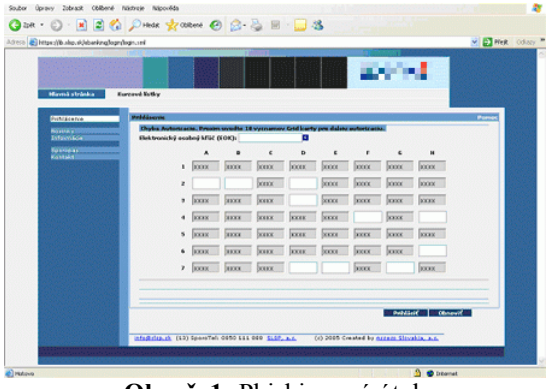
Slová, ktoré bežnému používateľovi internetu nič nehovoria. Za oboma výrazmi sa skrývajú formy zneužitia osobných údajov. Spôsoby hackerských pokusov ako získať citlivé osobné informácie od klienta banky - údaje o platobnej karte, jej číslo, PIN kód, prihlasovacie meno a heslo k nejakej službe, pozície z GRID karty. Veľmi jednoduchým a spoľahlivým riešením bránenia sa tomuto typu útoku je nepoužívanie grid karty na autentifikáciu, ale použite iného bezpečnejšieho autentifikačného nástroja.

Príklad phisingu - podvodný phishingový email, ktorý nie je priamo zameraný na banku, ale na kartovú spoločnosť VISA. Zneužité preto môžu byť osobné údaje a následne financie držiteľov kariet VISA vo všetkých bankách.

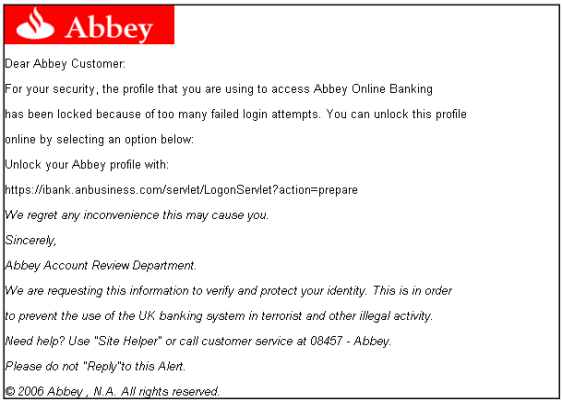
Podvodný e-mail:
Verified by Visa protects your existing Visa card with a password you create, giving you assurance that only you can use your Visa card online.
Simply activate your card and create your personal password. Youll get the added confidence that your Visa card is safe when you shop at participating online stores. You may activate now by entering your card number over our secure server. If your card issuer is participating in Verified by Visa (most issuers are) youll complete a brief activation process.
Youll verify your identity, create your Verified by Visa password and you are done.

Po kliku na tlačidlo „Activate Now“ je používateľ presmerovaný na podvodný server, ktorý od klienta požaduje v celkom profesionálnej forme zadanie diskrétnych údajov ako názov karty, číslo, dátum platnosti karty, CVV2 kód (ktorý sa používa pri platbách za nákupy uskutočnené cez internet), PIN kód karty. Na podvodnej stránke chýbal bezpečnostný certifikát SSL pre šifrovanú komunikáciu vystavený pre spoločnosť VISA (ikonka žltého zámku). Adresa stránky taktiež nezodpovedá adrese serverov, ktoré používa spoločnosť VISA.
Falošná stránka, ktorá je naprogramovaná na profesionálnej úrovni a vzbudzuje dojem, že sa klient nachádza na stránke spoločnosti VISA.

Príklady phishingu:



Obr. č. 1: Phishingový útok

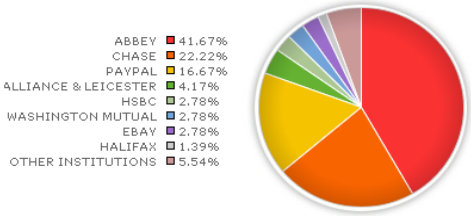


Obr. č. 2: Phishingový útok

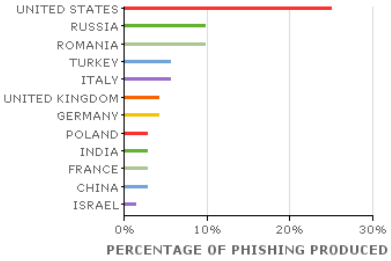
Štatistiky:

Na porovnanie uvádzam dve štatistiky phishingových útokov za dva rôzne týždne.

Týždeň končiaci 5. Aprílom 2009:

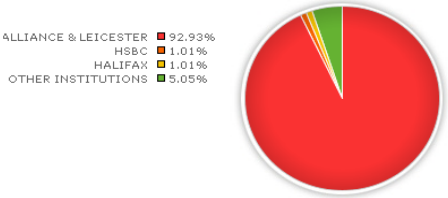


Obr. č. 3: Percentuálne rozloženie poľa cielenia phishingového útoku na americké finančné inštitúcie

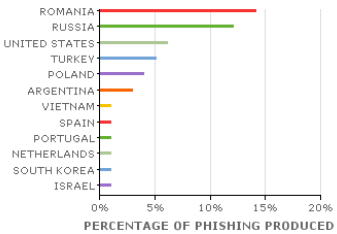


Obr. č. 4: Phishingové útoky podľa krajiny pôvodu v percentách

Týždeň končiaci 12. Aprílom 2009:



Obr. č. 5: Percentuálne rozloženie poľa cielenia phishingového útoku na americké finančné inštitúcie



Obr. č. 6: Phishingové útoky podľa krajiny pôvodu v percentách

3. Bezpečnostné predmety internet bankingu

Dnes sa na autentifikáciu a autorizáciu v internet bankingu používajú rôzne technológie a princípy. Najpoužívanejšie sú:

- Prihlasovacie meno a heslo
- Grid karta
- Generátory OTP (one-time-password)
- Elektronický podpis
- Biometrické nástroje.

4.1 Prihlasovacie meno a heslo

LOGIN, PIN, PID:

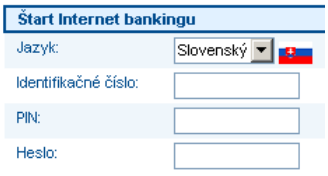
LOGIN z angl. Log In alebo ekvivalentu Sign In, Log On

PIN z angl. Personal Identification Number

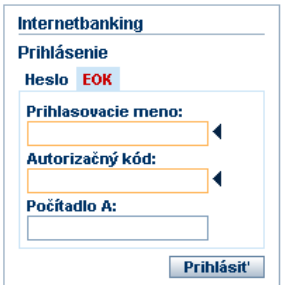
PID z angl. Personal Identifier

Prihlasovacie heslo slúži na autorizovaný prístup do aplikácií a oprávňuje prezerať informácie o účte, s ktorým má klient právo disponovať. Prihlasovacie meno (login) a heslo by v žiadnom prípade nemalo slúžiť na autentifikáciu, ale iba na autorizáciu. Dnes je však trendom, že v moderných aplikáciách je aj na autorizáciu použitý popri mene a hesle aj jeden z autentifikačných nástrojov.

Prihlasovacie údaje banka poskytuje pri zriaďovaní služby IB alebo pri vytváraní účtu ako jednu zo základných služieb poskytovaných klientovi.



Obr. č. 7 : Prihlásenie do internet bankingu bez dodatočnej autentifikácie.



Obr. č. 8: Prihlásenie do internet bankingu s dodatočnej autentifikácie.

4.2. GRID karta

Názov odvodený z angl. grid card, grid = mriežka
GRID karta je bezpečnostným predmetom, ktorý slúži na podpísanie - certifikáciu platobných príkazov a bankových operácií zadaných prostredníctvom služieb internetbankingu, mobilbankingu .
Používa sa pri tzv. dvoj-faktorovej autentifikácii (Two-Factor Authentication), kde prvým faktorom je niečo, čo vieme (something you know) - napr. PIN a niečo čo máme (something you have) - napr. grid kartu.
Bezpečnosť grid karty sa odvíja aj od počtu jej polí (zväčša 6x6, 7x7). Použitie je veľmi jednoduché, na základe výzvy systému zadá klient certifikačný kód zo súradníc pozície kódu v mriežke.

Výhody a nevýhody:

- ✓ Použitie pri aktívnych službách elektronického bankovníctva (internetbanking, mobilbanking ...)
- ✓ Jednoduchá manipulácia (má veľkosť platobnej karty, vmestí sa do peňaženky)
- ✓ Nízka cena (niekoľko desiatok centov, v závislosti od banky. Náklady banky na vydanie jednej karty sú cca 0,35 €)
- ✓ Zahraničné banky ju zväčša nevyužívajú
- ✗ Jej zneužitie závislé od uvedomelosti klientov banky
- ✗ Veľmi nízka, nepostačujúca bezpečnosť

Práve nízka bezpečnosť vedie grid kartu do záhuby. V budúcnosti jej majoritné postavenie ako autentifikačného nástroja určite prevezme, alebo už preberá iný, lepší a bezpečnejší autentifikačný nástroj. Kvôli jej jednoduchosti a všestrannosti jej používanie ešte bude nejaký čas trvať. Predpokladá sa však jej použitie ako doplnkového autentifikačného nástroja (internetbanking, mobilbanking ...).

	1	2	3	4	5	6
A	1234	5678	9012	2412	0000	1234
B	0000	1234	5678	9012	2412	0000
C	3333	0000	1234	5678	9012	3333
D	9012	3333	9999	1234	5678	9012
E	9999	5678	3333	1234	3333	5678
F	5678	9999	9999	0000	9999	5678

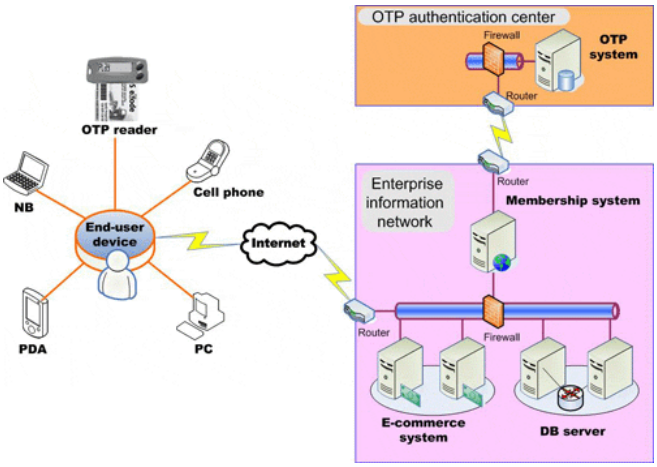
Obr. č. 9: Grid karta

4.3. Generátory OTP (one-time-password)

Rozdelenie:

- softvérové:
  - napr. Java calculator
- hardwarové:
  - SecurID Card
  - Active Token-y
  - Active Card
  - SMS Kľúč
  - Čítačka čipových kariet

Jednou z autentifikačných metód sa pri potvrdzovaní platby vygeneruje autentifikačný kód, ktorý sa overí so serverom. Ak sa kódy zhodujú, platba úspešne prebehne.



Obr. č. 10: Infraštruktúra OTP[10]

4.3.1 Softvérový generátor

Jedným z najľahšie implemetovateľných a najlacnejších riešení ako sprístupniť službu IB za pomoci OTP je softvérový generátor. Ten môže byť dostupný priamo cez web rozhranie na stránke banky, alebo ako samostatný program nainštalovaný na klientskej stanici. Výsledný validačný kód sa získa z kalkulátora po zadaní vstupných dát, ktoré môžu byť PIN, login, číslo účtu príjemcu, číslo účtu odosielateľa, posielaná suma, kód banky atď resp. ich kombinácia. Toto riešenie sa však v internet bankingu nevyužíva a jeho využitie sa ani nepredpokladá pre jeho nízke bezpečnostné ohodnotenie.

Výhody a nevýhody:

- ✓ Chráni pred phishingom (autentifikačný kód je vždy rôzny)
- ✓ Jednoduchosť prístupu
- ✓ Nízka cena

✓ Nenáročná implementácia

✘ Všetka autentifikácia a autorizácia je iba softvérová

Verejne dostupný softvérový kalkulátor:

✘ Nie sú oddelené komunikačné kanály

Kalkulátor na klientskej stanici:

✘ Nutnosť inštalovať ďalší softvér

✘ Nie je možné použiť službu na inom ako vlastnom PC (počítači s nainštalovaným softvérom)

4.3.2 SecurID Card, Active token

Token generuje každých 60 sekúnd nové čísl, ktoré je nutné zadať pri vstupe do internet bankingu a taktiež pri všetkých dôležitých operáciách. Token má formu malého zariadenia tvaru kreditnej karty, alebo napr. tvar malej kľúčenky, ktorá je pre svoju veľkosť veľmi skladná a je možné ju mať kedykoľvek pri sebe. Karta má na rozdiel od kľúčenky, okrem display-a aj klávesnicu. Tá jej umožňuje zadávať PIN, čo ju predurčuje aj k rozšírenému využitiu (prihlasovanie na terminál, VPN klienta ...).

Použitie token-nu je dnes veľmi rozšírené, elegantné riešenie s primeranou bezpečnosťou. Využívajú ho najmä firmy pre svojich zamestnancov. Bolo úspešne implantované a nasadené aj do internet bankingu, ale pre cenu token-u, jeho krátkej životnosti a existenciu bezpečnejších a lacnejších metód ochrany sa jeho ďalší rozvoj v internetovom bankovníctve nepredpokladá.

Výhody a nevýhody:

✓ Bezpečný spôsob autentifikácie pomocou OTP

✓ Viacúčelové využitie (IB, VPN ...)

✓ Chráni proti phishingu

✓ Token je ľahko nositeľný na kľúčoch, v kabelke ...

✘ Časovo obmedzené heslo

✘ Nechráni proti útoku Man-In-The-Middle

✘ Cenovo náročné

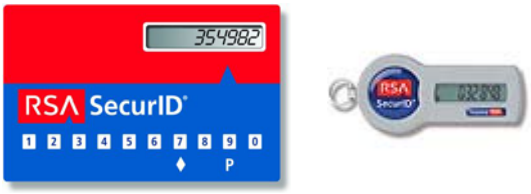
✘ Obmedzenosť použitia (napr. 2-3 roky)

✘ Ťažko realizovateľné masové používanie

✘ Náročná správa

✘ Zariadenie je neprenosné (Každý účet má vlastný token)

✘ Pri strate nás vydanie novej kalkulačky stojí peniaze a čas



Obr. č. 11: RSA SecurId Card a RSA Token

4.3.3 ActivCard

Pred pár rokmi sa komerčné banky už nechceli báť zneužitia grid kariet a implementovali ActiveCard, jeden z nástrojov OTP (okrem vyššie spomínaného token-u). Princíp je podobný ako u klasického token-u, tiež potrebuje „kalkulačku“, ktorá môže mať rôzne tvary. Rozdielny je ale princíp generovania autentifikačného kódu. Token generuje nový kód každých 60 sekúnd, bez ohľadu na to, či ho použijete alebo nie. V konečnom dôsledku tak použijete za jeho život iba niekoľko z celkového počtu vygenerovaných kódov. ActiveCard generuje kód na vyžiadanie po zadaní správnych údajov (PIN, login, číslo účtu príjemcu, číslo účtu odosielateľa, posielaná suma, kód banky atď. resp. ich kombinácia). Životnosť Activard je tak oveľa väčšia. Fakt, že hash-ovací algoritmus pri výpočte autentifikačného kódu použil napr. číslo posielaného účtu, chráni tak prevod peňažných prostriedkov pred útokom Man-In-The-Middle

Výhody a nevýhody:

✓ Bezpečný spôsob autentifikácie pomocou OTP

✓ Chráni proti phishingu

✓ Chráni proti útoku Man-In-The-Middle

✘ Kalkulačku treba mať pri vstupe do internet bankingu

✘ Cenovo náročné

✘ Náročné na správu

✘ Zariadenie je neprenosné (Každý účet má vlastnú kalkulačku)

✘ Pri strate nás vydanie novej kalkulačky stojí peniaze a čas

Využitie ActicCard ako moderného spôsobu zabezpečenia je veľmi vhodný variant najmä pre zákazníkov z veľkým počtom transakcií. Masové nasadenie pre všetkých klientov banky by bol však neakceptovateľný a drahý hazard.

Obr. č. 12: Rôzne druhy ActiveCards

4.3.4 SMS kľúč

Je veľmi používaný bezpečnostný predmet slúžiaci na certifikáciu platobných príkazov. Pri potvrdzovaní platobného príkazu Vám príde krátka textová správa s kódom na mobilný telefón. Kód má podobu viacmiestneho číselného reťazca a jeho platnosť je niekoľko minút od jeho vygenerovania. Platbu potvrdíte opísaním kódu do poľa na to vyhradeného na web stránke svojho IB. Systém overí správnosť hodnoty certifikačného kódu a oznámi stav spracovania transakcie. Ide o elegantnú a klientsky veľmi jednoduchú dvojstupňovú autentifikáciu.

Výhody a nevýhody:

✓ Bezpečný spôsob autentifikácie pomocou OTP

✓ Autentifikácia na princípe dvoch rozdielnych komunikačných kanálov

✓ Chráni proti phishingu

✓ Nenáročné na správu

✓ Užívateľsky akceptovateľné riešenie

✓ Univerzálne použitie pri aktívnych službách elektronického bankovníctva

✘ Musíme mať vlastný mobilný telefón

✘ Užívateľ musí mať mobilný telefón vždy pri potvrdzovaní príkazu

✘ Nechráni proti útoku Man-In-The-Middle

✘ Cenovo náročné pre banku

✘ V čase výpadku alebo vyťaženia siete je autentifikácia nedostupná

✘ Nutnosť byť v mieste pokrytia GSM signálom

4.3.5 Čítačka čipových kariet

V poslednom období sa viacero svetových, ale aj jedna zo slovenských bánk rozhodla využiť jedno z najlepších a najdostupnejších riešení pre dvojstupňovú autentifikáciu. Čítačka čipových kariet je jeden z nových nástrojov autentifikácie určený na bezpečnejšie prihlasovanie a potvrdzovanie platieb v internet bankingu. Čítačka čipových kariet nahradzuje doposiaľ používané autentifikačné nástoje, ako sú Grid karta, SecurID karta, ActiveCard, či SMS kód.
Čítačka sa neinštaluje, nenabíja a ani nepripája k inému zdroju (má vlastnú batériu). Je preto veľmi jednoduchá na používanie a každodenné nosenie. Existujú rôzne modely rôznej veľkosti. Čítačky rôznych bánk sú medzi sebou kompatibilné. Čítačka bez karty predstavuje len nepoužiteľnú kalkulačku, bez žiadnych zneužiteľných údajov. Je preto možné mať viac čítačiek, požičiavať si ich, alebo v prípade straty si jednoducho zaobstarať inú. Čítačke generuje kód na základe informácie z čipovej karty a parametra vykonávanej platby (PIN, login, číslo účtu príjemcu, číslo účtu odosielateľa, posielaná suma, kód banky atď, resp. ich kombinácie). Môže sa použiť aj na autentifikáciu do internet bankingu.

Výhody a nevýhody:

✓ Bezpečný spôsob autentifikácie pomocou OTP

✓ Autentifikácia na princípe dvoch rozdielnych komunikačných kanálov

✓ Chráni proti phishingu

✓ Chráni proti útoku Man-In-The-Middle

✓ Menej náročné na správu ako vyššie uvedené riešenia

✓ Cenovo menej náročné pre banku (pri odbere 200 000 ks je cena za kus cca 5 USD)

✓ Univerzálne použitie pri aktívnych službách elektronického bankovníctva

✓ Možnosť mať viac čítačiek alebo si ich požičiavať

✗ Užívateľmi len ťažko prijímané riešenie

✗ Nepraktické pri hromadnom prevode

✗ Ak chcem pracovať s internet bankingom musíme mať čítačku pri sebe

Obr. č. 13: Čítačky čipových kariet

4.4 Elektronický podpis

Používanie elektronického podpisu začína byť bežné aj v každodenných situáciách. Klient si zvolí, či si uloží vygenerovaný súkromný alebo verejný kľúč na disketu, disk počítača, alebo si ich uloží na čipovú kartu. Uloženie na čipovú kartu je vyššou úrovňou zabezpečenia kľúčov klienta. Elektronické transakcie potom podpisuje klient pomocou súkromného kľúča. Autentickosť digitálneho podpisu a integrita prenášaných informácií sa v banke overuje pomocou verejného kľúča klienta, ktorý má banka k dispozícii. Digitálny podpis sa používa na digitálne podpisovanie všetkých transakcií, ktoré vyžadujú overenie identity klienta bankou.

Výhody a nevýhody:

✓ Bezpečný spôsob autentifikácie

✓ Chráni proti phishingu

✓ Univerzálne použitie pri aktívnych službách elektronického bankovníctva

✓ Náročné na obsluhu

✗ Musíme mať vlastný nosič privátneho kľúča a chrániť si ho

✗ Cenovo náročné

4.5 Biometrické nástroje

Biometria je svojim princípom zatiaľ neprekonaný a najvierohodnejší spôsob autentifikácie. Pre jeho cenu, zložitú implementáciu a náročnosť masového nasadenia v internet bankingu je však toto riešenie iba hudba ďalekej budúcnosti.

5. Záver

Klient banky zväčša nemá na výber, aký spôsob zabezpečenia svojho konta v internet bankingu bude používať (ak odhliadneme na šifrované spojenie, na nainštalovaný antivírový program s najnovšou aktualizáciou a správne nakonfigurovaný firewall, čo považujem za samozrejmosť). Banka sa snaží presvedčiť klienta, že to ich riešenie je najlepšie a najbezpečnejšie. Rôzne spôsoby ochrany sa klientom ponúkajú aj podľa služieb, o ktorých využívanie majú záujem. Podnikateľským subjektom a obchodným spoločnostiam sa ponúkajú bezpečnejšie technológie, pretože ich tok peňazí je vyšší a internet banking aj častejšie využívajú, čo zvyšuje riziko zneužitia. Čítačka čipových kariet je zo spomínaných riešení najlepšia voľba pre klienta, ako aj pre banku. Práca s ňou je jednoduchá, je nahraditeľná a zabezpečuje vysoký štandard bezpečnosti. Možno očakávať jej rozšírené využitie v internet bankingu viacerými komerčnými bankami. V budúcnosti je možný rozvoj aj biometrie, ale v najbližšom desaťročí to nebude. Technologicky sa však môžeme priblížiť k akémusi spojeniu čítačky pamäťových kariet a samotnej karty. Ak by bolo možné vybaviť čipovú kartu displayom a dotykovou klávesnicou, ktoré budú integrované na jej tele pri zachovaní jej aktuálnej veľkosti, bolo by to prevratné riešenie.

6. Literatúra

[1] **DOSTÁLEK, L.:** Velký průvodce protokoly TCP/IP. Bezpečnost. Praha: Computer Press, 2003. ISBN: 80-7226-849-X

[2] **ELLIS, J., SPEED, T.:** The internet security. Guidebook. From planning to deployment. San Diego: Academic Press, 2001. ISBN: 0-12-237471-1

Oficiálne stránky bánk, denníkov a spoločností zaoberajúcich sa bezpečnosťou:

[3] http://www.tatrabanka.sk
[4] http://www.wikipedia.com
[5] http://www.vub.sk
[6] http://www.sme.sk
[7] http://www.mcafee.com
[8] http://www.marshal.com/
[9] http://www.dsl.sk
[10] http://www.otp.com.tw/
[11] http://www.slsp.sk
[12] http://www.barclays.co.uk/
[13] http://www.abbey.com/