Problematika Internetového bankovnictví v ČR a jeho bezpečnosti

Problems of Internet banking at Czech republic and its security

Dagmar Brechlerová

Adresa autorky:

RNDR. Dagmar Brechlerová, Česká zemědělská univerzita, PEF - KIT, Praha 6 - Suchdol, 165 21, tel.: 02 2438 2356, e-mail: brechlerova@pef.czu.cz

Anotace:

Nabídka Internetového bankovnictví v ČR se rozšiřuje. Příspěvek se zabývá základními otázkami Internetového bankovnictví a otázkou jeho bezpečnosti.

Summary:

There is possibility to use an Internet banking in the Czech republic now. This contribution deals with basic questions of Internet banking and with questions of security of Internet banking.

Klíčová slova:

šifrování, symetrické šifrování, veřejným klíč, soukromý klíč, banka, Internet

Key words:

cryptography, symmetric cryptography, public key, private key, bank, Internet

Bankovnictví můžeme v zásadě rozdělit do dvou typů: **bankovnictví přímé a bankovnictví pobočkové.** V bankovnictví pobočkovém musí klient banku osobně navštívit a zde u přepážky komunikovat (bohužel občas ještě s málo vstřícným zaměstnancem banky). Je tedy možno banku navštívit pouze v pracovní době a v jejím sídle. To může zejména na venkově vzhledem ke vzdálenosti i nevhodným otvíracím dobám (Komerční banka - obvykle do 17 hodin) představovat ztrátu času a peněz. Zde si tedy vlastně banka diktuje, kdy a kde

bude svým zákazníkům služby poskytovat. V zemědělství např. v době vrcholící sklizně může být tato návštěva velmi problematická.

Uvedené problémy času i místa (nebo alespoň času nebo místa) odstraňuje bankovnictví přímé. Zde je možno komunikovat s bankou obvykle několika různými způsoby, různými telekomunikačními kanály. Pro osobní návštěvu zůstávají zachovány i pobočky. Zde odpadají návštěvy banky a bankovní služby jsou přístupné kdykoliv, tedy kdy se to hodí zákazníkovi a nikoliv bance. Navíc služby poskytované přímým bankovnictvím jsou často i levnější pro zákazníka i pro banku. Dle [1] v USA náklady na jednu transakci (pro banku) činí:

Pobočka	1,07$
Telefon	0,54$
Internet	0,01$

Porovnání nákladů Internetového bankovnictví pro klienty viz [2] . Dalším velmi výrazným kladem zejména u Internetové banky je v některých případech možnost (a navíc levné) komunikace ze zahraničí. Internetové bankovnictví dále umožňuje různé nové typy bankovních služeb, ale tato oblast není předmětem zájmu našeho příspěvku.

Vzhledem k výše uvedeným skutečnostem se přímé bankovnictví a to zejména Internetové v následujích letech bude zcela jistě rychle rozvíjet a proto se v našem příspěvku budeme věnovat tomuto bankovnictví. V současné době je jedním z problémů určitá nedůvěra v bezpečnost transakcí po Internetu. Neznalost základních pojmů, které často ani pracovníci bank nejsou schopni vysvětlit, totiž někdy vede k odmítání tohoto způsobu komunikace s bankou. Proto jsme např. na naší fakultě zavedli volitelný předmět Bezpečnost dat, který zájemce mimo jiné seznamuje s danou problematikou.

Bezpečnost:

Základním požadavkem pro jakékoliv bankovní služby je jejich bezpečnost. Je nutno jednak zajistit citlivá data před zneužitím, napadením atd. a dále při přímém bankovnictví nějakým způsobem nahradit identifikaci klienta v pobočkovém bankovnictví.

Kde musí Internetová banka bezpečnost zajistit:

Při vztahu s klientem musí Internetová banka zajistit:

důvěrnost dat - šifrováním

autentizaci protistrany - šifrování

prokazatelnost - digitální popis

integrita - certifikace dat

Proti průniku zvenku do banky:

filltry, proxy servery, firewally, nastavení přístupových práv

Uvnitř banky:

organizační opatření, přístupová práva, pravidlo 4 oči (při každé operaci 2 osoby)

Uvedené operace je možno provádět řadou způsobů, ale je nutné je bezpodmínečně zajistit. Zde nutno podotknout, že tolik obávané napadení dat není obvykle způsobeno mladými hackery (jak se veřejnost domnívá) , ale z 80% zaměstnanci banky. A proti tomu jsou nechráněny všechny banky stejně. Zde již bezpečnost spočívá v různých organizačních opatřeních a dodržování bezpečnostních norem ze strany banky, což je často podceňováno.

Bezpečnost vzhledem ke klientům je zajištěna převážně šifrováním a banky často u nabízených produktů hovoří o zabezpečení jednotlivými typy šifer, aniž blíže klientům vysvětlí, o co se vlastně jedná. Proto dále věnujeme pozornost šifrování a problémům se šifrováním.

Šifrování je dnes v zásadě dvojího druhu: symetrické (s tajným klíčem)

s veřejným klíčem (asymetrické)

Symetrické šifrování: odesílatel i příjemce mají stejný tzv. klíč (obvykle řadu čísel) , které použijí k nějaké matematické operaci (operacím), kterou aplikují na odesílaná data. Tato data se tak stanou nečitelná. Příjemce užije stejný klíč a aplikací stejných operací dostane původní data. Nejznámějším a nejpoužívanějším zástupcem tohoto druhu šifer je šifra DES, která je v USA uznána jako standard, z USA je dovoleno vyvést 56 bitů dlouhou šifru. U DESu se jsou užité matematické operace substituce, permutace a logické operace. Další typy: Triple Des, IDEA aj. Výhodou těchto šifer je jejich rychlost, nevýhodou nutnost předat nějakým způsoben tajný klíč. Dále pro n klientů musím mít n klíčů, protože pro danou dvojici musí být klíč jedinečný. Dalším problémem je autentizace: jak vyřešit problém

původce zprávy. Tedy symetrická kryptografie řeší otázku bezpečnosti dat, ale ne odmítnutí odpovědnosti.

Šifrování s veřejným klíčem (asymetrická kryptografie): existují dva klíče - veřejný a soukromý. Zde se jedná o aplikaci dvou opačných matematických operací, pomocí jedné jsme schopni data zašifrovat, pomocí druhé odšifrovat. Klient má svůj soukromý klíč, který nezveřejňuje a naopak chrání (trezor, čipová karta) a veřejný klíč, který může znát každý. Stejně tak druhá strana (např. banka). Klient data zašifruje svým soukromým klíčem a pošle bance, ta je rozšifruje veřejným klíčem klienta. Problémem je to, že zpráva není důvěrná, přečte si ji každý, kdo zná veřejný klíč, ale je podepsaná. Zde řeším integritu dat a neodmítnutelnost, ale ne důvěrnost. Zde je typickým představitelem šifra RSA, která má ale tu nevýhodu, že je velmi pomalá. V softwarové podobě 100 krát a v HW podobě až 1000 krát než symetrické šifry. Proto se ve skutečnosti často šifry kombinují včetně využití dalších matematických prostředků (hash funkce), a asymetrická kryptografie se užívá pouze pro podepsání a předání klíčů pro symetrickou kryptografii. Celkově jsou tyto kombinace nazvány tzv. **protokoly,** kterých je velké množství.

Možná kombinace symetrického a nesymetrického šifrování a hash funkcí je následující protokol: klíč pro symetrické šifrování je zašifrován veřejným klíčem adresáta, zpráva samotná je zašifrována tímto symetrickým klíčem, ze zprávy je navíc spočtena hash hodnota a ta je zašifrována soukromým klíčem odesílatele, čili je digitálně podepsána. Tento komplex pak může projít přes sítě Internetu bez nebezpečí prozrazení. Příjemce (např. banka) si nejprve svým soukromým klíčem rozšifruje symetrický klíč, tímto symetrickým klíčem si rozšifruje zprávu. Ze zprávy poté jestě spočte dohodnutým způsobem hash hodnotu a tu porovná s odeslanou hash hodnotou, (kterou rozšifroval veřejným klíčem odesílatele). Pokud obě hash hodnoty si odpovídají, je tímto způsobem zajištěna jak bezpečnost, tak integrita, tak autentizace.

Krátká zmínka o šifrování měla pouze ukázat, že i Internet jde zabezpečit (lépe než např. telefon) vhodným užíváním šifrování. Klient se těchto operací nemusí nijak obávat, protože pro něj jsou zabezpečeny používaným softwarem a je již věcí banky, aby užitý software splňoval určitá bezpečnostní kritéria.

Protože Internetové bankovnictví jistě čeká i v ČR velký rozvoj, podáváme přehled těchto služeb na našem trhu. **Nabízené produkty Internetového bankovnictví (situace ke dni 1.7.1999) a postup přidělení bezpečnostních klíčů:**

IPB od 2/1999

Postup připojení: základní vklad 1000 Kč, nutný výpis z obchodního rejstříku či živnostenský list, od IPB klient dostane instalační CD - ROM, nainstaluje do svého počítače, na disketu se vygeneruje žádost o bezpečnostní certifikát, tuto disketu klient odnese do IPB, zde přidělen certifikát, ten si přehraje do svého počítače

Expandia banka od 4/1998

Postup připojení: žádost možno odeslat po Internetu, poté nutná osobní návštěva tzv. Klientského centra (tj. pobočky), zde uzavřena smlouva, klient dostává tzv. elektronický klíč; možnost osobních i firemních účtů

Citibank od 4/1999

nutný roční obrat 50 milionů Kč, při osobní návštěvě předány kódy a hesla

Z výše uvedených skutečností vyplývá, že pro soukromé osoby (které nevlastní živnostenský list) tuto službu k 1.7 .1999 poskytovala pouze Expandia. V současné době (říjen 1999) nabízí Internetové bankovnictví také Raiffeisenbank (do 30.11.1999 verze zdarma), Komerční banka předpokládá po pilotním projektu, který právě probíhá , nasazení Internetového bankovnictví až po 1. 1. 2000. Dá se předpokládat, že další banky jistě nezůstanou stranou a během krátké doby jistě Internetové bankovnictví bude patřit k běžně nabízené službě .

Jaké jsou současné a očekávané problémy v zajištění bezpečnosti pomocí kryptografických metod:

1. možnost prolomení některých typů šifer (zejména spojené s možností propojení výkonných počítačů na Internetu), např. DES s 40 bity lze prolomit za 4 hodiny s 1200 propojenými průměrnými počítači. Proto musí být důsledně řešena pravidelná změna klíče, případně užívány delší klíče či jiné typy šifer; jak jsme již podotkli, toto musí řešit banka zavedením vhodného systému.

2. neexistence právní podpory pro některé aplikace šifer (neexistence zákona o digitálním podpisu), u nás je zatím pouze několik návrhů.

3. u nás neexistence oficiálních certifikačních autorit, které pečují o výměnu a správu klíčů. Jejich funkce je zakotvena právě v návrhu zákona o digitálním podpisu, kde je navrženo vytvoření Národního certifikačního úřadu a dalších certifikačních autorit. Např. IPB využívá organizace I.CA., ale její funkce není zatím řešena zákonem.

4. určitá nedůvěra v bezpečnost transakcí po Internetu, která vyplývá z neznalosti základních pojmů, které často ani pracovníci bank nejsou schopni vysvětlit. To někdy vede k odmítání tohoto způsobu komunikace s bankou. Zatím Internetové bankovnictví oslovuje zejména mladší generaci, u které patří práce s Internetem k běžné součásti života i v jiných oblastech.

5.celkově nízké znalosti pracovníků bank v oblasti bezpečnosti vůbec; nutnost jejich zvýšení.

V našem příspěvku jsme chtěli upozornit na novou formu bankovnictví a to bankovnictví Internetové. Tento druh bankovnictví se rychle rozvijí a jeho snadná dosažitelnot jej činí velmi vhodným například i pro pracovníky v zemědělství; po prolomení počáteční nedůvěry a dořešení některých zmíněných problémů se jistě stane běžnou součástí života, stejně jako třeba platební karty apod.

Literatura:

1. Kosirus Dd. a kol. : Elektronická komerce, Computer Press,1999

2. MF Dnes,1.7.1999

3.Schneider B.: Applied cryptography, Wiley 1998

4.Přádka M.: Seriál Banka na drátě, CHIP, 2 až 7 1999