AUTENTIZACE V PŘÍMÉM BANKOVNICTVÍ

Miloslav Hub
Ústav systémového inženýrství a informatiky, FES, Univerzita Pardubice

Abstract: Authentication in on-line banking
The aim of this text is to show how authentication is implemented in on-line banking industry. Czech banks are analyse as well as their on-line banking services. It is examined authentication of users´s identity of this services.

Klíčová slova: *autentizace, bezpečnost informací,dvoufaktorová autentizace, Internet banking, přímé bankovnictví*
Key words: *authentication, security of information, two-factor authentication, Internet banking, on-line banking*

1. Přímé bankovnictví

Mnoho bank v současné době nabízí klientům i jiné možnosti, jak přistupovat ke svým účtům, než osobní návštěvou své pobočky. Ve snaze získat konkurenční výhodu banky umožňují různými způsoby klientům ovládat své účty kdekoliv a kdykoliv, a to pomocí Internetu, mobilního telefonu či dokonce i pomocí jakéhokoliv telefonního přístroje. Pomocí přímého bankovnictví (někdy též nazývaného on-line bankovnictví) lze zjišťovat použitelný zůstatek, získávat přehled platebních příkazů a zúčtovaných transakcí, zadávat příkazy k úhradě, nebo převodu, získávat výpisy z banky, měnit limity účtu, zjišťovat informace o bance jako např. úrokové míry, zadávat povolení k inkasu, nebo SIPu a podobně. Záleží však na konkrétní nabídce banky. Pro klienta banky je přímé bankovnictví výhodné nejenom tím, že se nemusí přizpůsobovat otvírací době pobočky, ale i tím, že operace prováděné tímto způsobem jsou zpravidla zpoplatněny nižší sazbou (neboť představují pro banku nižší náklady). Podle výkonného ředitele NetBank D. R. Grimese je klasický pobočkový systém příliš drahý. Budovy, lidé a zařízení představují 50 procent provozních nákladů. Právě proto vznikají tzv. on-line banky, které narozdíl od klasických kamenných bank nemají tak rozsáhlou síť poboček (pokud vůbec nějaké pobočky mají). Na základě výzkumu, který provedla agentura Jupiter Communications, přímé bankovnictví již využívá deset procent amerických domácností, které jsou připojeny na Internet. V této souvislosti společnost odhaduje, že se toto procento do roku 2003 zvýší na 39 [3].

Přímé bankovnictví je tedy takové, kdy klient může provádět určité manipulace s účtem kdekoliv a kdykoliv (má-li k tomu však potřebné prostředky) bez toho, aby musel fyzicky navštívit pobočku banky. Obecně můžeme rozdělit druhy přímého bankovnictví do několika skupin, každá skupina je specifická a tudíž je pro ni vhodný odlišný způsob autentizace.

Druhy přímého bankovnictví:

1. Internet banking
2. Home banking
3. GSM banking
4. WAP banking
5. Phone banking
6. Fax a pošta

Pro úplnost je třeba dodat, že banky své tyto služby nazývají vlastními názvy. Můžeme se tedy setkat s názvy Mobil banka, Mobilkonto označující GSM banking, dále Internetbanking 24, Internet banka, Webkonto označující Internet banking. Pro označení homebankingu některé banky zvolily název Homebanking 24, nebo třeba BankKlient, a v případě Phone bankingu se můžeme setkat s pojmy jako Telefon banka, nebo Callkonto.

2. Význam autentizace v přímém bankovnictví

S nabídkou služeb přímého bankovnictví vznikají problémy, jak tyto služby zajistit tak, aby byly bezpečné. Službu považujeme za bezpečnou tehdy, když se chová tak, jak se od ní očekává [2]. To znamená, aby ke svému účtu získal přístup pouze jeho vlastník, případně další osoba, která má k tomuto účtu dispoziční právo. Aby se tedy nemohlo stát, že by cizí osoba mohla prohlížet zůstatky cizích účtů, nebo historii transakcí, případně aby mohla na cizích účtech zadávat příkazy k převodu, úhradě, apod. K řešení těchto problémů se přímo nabízí jeden z nástrojů zajištění bezpečnosti dat, a to autentizace (samozřejmě ve spojení i s jinými nástroji, jako třeba autorizace, žurnálování,…). Pod pojmem autentizace rozumíme ověření totožnosti uživatele dat, tzn. ověření toho, že je uživatel skutečně tím, za kterého se vydává. Metod autentizace je mnoho, můžeme je však rozdělit do tří základních skupin [4]:

1. autentizace znalostní založená na určité znalosti (např. hesla)
2. autentizace biometrická, jenž spočívá v tom, že každý jedinec má určité biologické znaky jedinečné (např. snímání sítnice oka)
3. autentizace prostřednictvím autentizačního předmětu, kdy se identita prokáže vlastnictvím jedinečného předmětu (např. platební karty)

Jednotlivé způsoby mají nejen své přednosti, ale také i své nedostatky. Proto je třeba pečlivě zvážit, jaký způsob je pro danou situaci nejvhodnější. Současným trendem je kombinace více způsobů autentizace, čímž se některé nedostatky eliminují a celková bezpečnost se zvýší. Absolutní bezpečnost však zajistit nikdy nelze. Typickým příkladem jsou debetní karty. Uživatel se musí, aby si mohl z bankomatu vybrat peníze uložené na svém účtu, prokázat nejen autentizačním předmětem (debetní kartou), nýbrž také znalostí příslušného hesla (PINu). Pokud mu je tato karta odcizena, bez znalosti PINu ji nelze zneužít. Dalším příkladem může být placení v obchodech pomocí platební karty. Nestačí pouze vlastnit tuto kartu, ale je také třeba se podepsat stejně, jako na podpisovém vzoru. V tomto případě je autentizace provedena nejenom prostřednictvím autentizačního předmětu, nýbrž také prostřednictvím biometrické autentizace (vlastnoruční podpis).

3. Internet banking

K využívání této služby je zapotřebí jakýkoliv počítač připojený k Internetu vybavený internetovým prohlížečem, který tvoří uživatelské rozhraní pro ovládání účtu. Předností je, že internetový prohlížeč je součástí většiny počítačů, a že na toto rozhraní je uživatel zvyklý i u jiných služeb. Webová rozhraní těchto služeb často obsahují Java aplety, většina prohlížečů je však podporuje [1].

Možností způsobů autentizace, je v tomto případě několik. Jedním z nejjednodušších, ale zároveň však jeden z nejméně bezpečných je využití znalostní autentizace, konkrétně hesel. Přístup k účtu je pak vázán na znalost správného hesla. Výhodou je, že uživatel může ke svému účtu přistupovat z jakéhokoliv počítače připojeného k celosvětové síti Internet. Musí však znát správné heslo, což může být zároveň nevýhodou. Za bezpečná hesla jsou totiž považována taková, která jsou dostatečně dlouhá a dostatečně „nesmyslná“, a to právě může působit problémy. Uživatelé si často tato hesla zapisují a tím bezpečnost svého bankovního účtu snižují, nebo si je mění na taková, která jsou snadno uhádnutelná. Proto je tento způsob

často používán pouze do určitého peněžního limitu, nebo jen pro určité služby (např. zjištění zůstatku na účtu), jejichž zneužití není tak nebezpečné. Pro vyšší limity se používá bezpečnějších a spolehlivých způsobů. Jedním z nich je elektronický klíč v podobě dat uložených na médiu. Banka vydá klientovi disketu s tímto elektronickým klíčem, který je navíc chráněn PINem (to pro případ, že by byl tento klíč byl odcizen). Uživatel si ho v podobě malého souboru může podle svého uvážení nahrát na jakýkoliv počítač, kde ho může potřebovat (i když se to zpravidla nedoporučuje), nebo ho nahraný na přenosném médiu může nosit s sebou. V případě, že má podezření, že byl elektronický klíč odcizen a mohl by být zneužit, může si prostřednictvím webového rozhraní vygenerovat klíč nový, případně si dokonce i změnit svůj PIN. Jiným způsobem je uložení elektronického klíče na čipovou kartu. Tento způsob je poměrně bezpečný, klíč z karty nelze jednoduše překopírovat, avšak je k tomu potřeba čtečka čipových karet. Také je třeba na počítač nainstalovat softwarový ovladač této čtečky.

Současným trendem v autentizaci jsou jednorázová hesla, což jsou hesla pro jednu jedinou relaci. Přestože se útočníkovi podaří takové heslo odchytit při jeho přenosu, je pro něho nepoužitelné, neboť k další relaci je třeba naprosto jiné heslo. Proto mnoho bank zvolilo tento způsob, který implementovaly různými způsoby. Jedním z nich je použití tzv. autentizačního kalkulátoru, který po zadání správného PINu vygeneruje heslo, jenž je stanoveno zároveň s ohledem na aktuální reálný čas. Název získal tento přístroj podle toho, že skutečně jako kalkulačka vypadá. Autentizační kalkulátor však nemusí mít pouze fyzickou podobu, nýbrž se může jednat o software. Další možností, jak využít jednorázové heslo pro autentizaci v internetovém bankovnictví je zaslání tohoto hesla na předem určený mobilní telefon ve formě SMS. Tuto zprávu však lze odchytit, proto se doporučuje kombinace tohoto jednorázového hesla s heslem fixním. Ve všech případech probíhá komunikace s bankou prostřednictvím Internetu zabezpečeným protokolem https.

V následující tabulce je shrnuty způsoby autentizace v Internet bankingu předními bankami působícími na českém trhu [5].

Tabulka 1: Autentizace Internet bankingu českými bankami

Banka	Způsob autentizace
eBanka	Autentizační kalkulátor, nebo generování čísla PIN prostřednictvím SMS, nebo elektronický klíč (software pro generování elektronického podpisu)
Raiffeisenbank	Přístupový certifikát uložený na disketě nebo v počítači
České spořitelna	Autentizační kalkulátor
Živnostenská banka	Přístupový certifikát uložený na disketě nebo v počítači
Komerční banka	Přístupový certifikát uložený na disketě nebo v počítači + heslo
HVB Bank	Autentizační kalkulátor
Citibank	Číslo debetní karty a vstupní kód HPIN
ČSOB	Čipová karta + čtečka čipových karet
GE Capital Bank	Heslo, aktivní operace zabezpečeny elektronickým podpisem

4. Home banking

Narozdíl od Internet bankingu nelze ovládat svůj účet prostřednictvím jakéhokoliv počítače připojeného k síti internet, neboť je třeba na počítač nainstalovat speciální

programové vybavení. Uživatelské rozhraní totiž netvoří internetový prohlížeč, nýbrž aplikace dodávaná bankou. V některých případech tuto aplikaci lze provázat s účetními programy, proto je Home banking často využíván firmamy. Tato aplikace ve spojení se šifrovanou komunikací s bankou a autorizačního certifikátu zajišťuje vůbec nejvyšší úroveň bezpečnosti ze všech forem přímého bankovnictví. Navíc bývá komunikace klienta s bankou šifrována vhodným algoritmem.

5. GSM banking

Transakce je prováděna prostřednictvím SMS s předem definovanou strukturou (např. ZUST_255348*11_052486_93216). Komunikace bývá zpravidla oboustranná, tzn., že i banka se svým klientem komunikuje prostřednictvím těchto strukturovaných zpráv. Většina mobilních telefonů obsahují technologii SIM Toolkit ve které je nahraná bankovní aplikace. Pak stačí postupně zadávat pouze požadované položky v menu, a mobil sestaví zprávu sám. Některé banky nabízejí službu GSM banking výhradně pomocí této technologie.

Autenizace je zajištěna přímo telefonním číslem registrovaného mobilního přístroje v kombinaci s přiděleným PINem, které musí uživatel zadat. Tento PIN je obrana proti zneužití mobilního telefonu třetí osobou. Navíc může být i samotný mobilní telefon chráněn proti zneužití dalším PINem. Při využití technologie SIM Toolkit se veškerá komunikace s bankou vede v zašifrované podobě oproti zasílání strukturovaných SMS, kde je pro zvýšení bezpečnosti často používaná technologie jednorázových hesel s využitím autentizačního kalkulátoru. Pravděpodobnost odchycení zprávy je v případě GSM sítě výrazně nižší, než v případě Internetu.

6. WAP banking

WAP banking je velice podobný Internet bankingu, rozdíl spočívá v tom, že místo webových stránek jsou využívány stránky wapové, založené na protokolu WAP (Wireless Application Protocol), ke kterým se přistupuje pomocí prohlížeče nainstalovaném v mobilním telefonu. Tuto službu v současné době umožňují všechny moderní mobilní telefony. Lze však k ní přistupovat i z jiných zařízení, jako jsou osobní digitální organizéry, pagery nebo palubní počítače automobilů. Komunikace tímto protokolem je šifrovaná, což je důvod, proč není možné využít softwarové emulátory (např. gelon.net). Pro svou nákladovou náročnost pro uživatele není tento způsob přímého bankovnictví v širší míře využíván.

7. Phone banking

K využívání této služby postačí jakýkoliv telefonní přístroj s nastavenou pulsní volbou a s přístupem do veřejné telefonní sítě. Phone banking je vhodný zejména pro ty, kteří nemají zkušenosti s moderní technikou.

Služby poskytované Phone bankingem můžeme rozdělit na:

- pasivní
- aktivní

Pasivní služby jsou takové, kdy informace pouze získáváme. Mohou to být služby, které klienta informují o zůstatku na účtu, které podávají informace banky např. o úrokové míře, apod. většinou prostřednictvím automatu. Aktivní služby na rozdíl od pasivních umožňují zadávat příkazy (příkaz k převodu, inkasu, apod.).

Po vytočení čísla telefonní banky automat požádá o zadání uživatelského čísla a PINu prostřednictvím klávesnice. Protože je zde stejně jako i v jiných případech používáno hesel, je nejslabším článkem samotný klient. Nebezpečí zneužití hesla při jeho prozrazení lze částečně

předejít nastavením limitů pro transakce prováděné po telefonu. Další bezpečnostní riziko přestavuje možnost „odposlechnutí“ zadávaných údajů, které je vyšší v případě použití pevné telefonní linky. Pro případ, že klient své heslo zapomene, může získat přístup k službě pomocí kontrolních otázek a odpovědí, na kterých se s bankou domluvil při zřizování služby. Někdy bývá při použití jiného telefonu, než na kterém se uživatel s bankou domluvil, pro přístup k službě třeba více hesel.

8. Fax a pošta

Fax a pošta jsou klasickým komunikačním prostředkem. V tomto případě jsou, narozdíl od předešlých způsobů, transakce provádeny se zpožděním. Formuláře k těmto příkazům banky zveřejňují na Internetu, jejichž součástí je i pole pro vyplnění klientského čísla (identifikátoru) a jednorázového autentizačního kódu autentizátoru). Tento kód bývá vygenerován autentizačním kalkulátorem (fyzickým, nebo softwarovým), případně může být heslo zasláno e-mailem nebo SMS, čímž se zabrání zneužití autorizačních práv třetí osobou. Jelikož je tento kód generován i na základě typu transakce a zadaných částkách, je zabráněno tomu, aby byl příkaz zneužit pozměněním zadaných údajů při jeho přenosu (integrita). Zpravidla bývá tento způsob z pohledu vyřizování běžných bankovních transakcí považován pouze za doplňkový.

9. Závěr

Autentizace je v přímém bankovnictví jedním z rozhodujících faktorů ovlivňující bezpečnost tohoto systému. Přímé bankovnictví lze zajistit různými komunikačními kanály, pro každý z těchto kanálů je vhodný jiný způsob autentizace. Způsob, jakým je prokázání identity zajištěn, závisí kromě toho také na konkrétních službách, které jsou prostřednictvím přímého bankovnictví poskytovány. Uživatel, který využívá k on-line přístupu ke svému bankovnímu účtu více komunikačních kanálů je v současné době nucen používat i několik naprosto odlišných autentizačních způsobů. To vede k zvýšení nároků na daného uživatele a tím i k snížení bezpečnosti systému. Kromě toho to může vést i k ekonomickým ztrátám, kdy se uživatel rozhodne z důvodu pro něho nepřijatelných komplikací pouze pro jeden komunikační kanál.

Literatura:

[1] BĚLOHUBÝ, J. *Ještě chodíte do banky?* [online].[cit. 12-2-2003]. Dostupné z <http://www.belohuby.cz/clanky/ms8.htm>.

[2] BORLAND, R.: *Bezpečnost UNIXu a Internetu v praxi.* Praha: Computer Press, 1998. 948 s. ISBN 80-7226-082-0

[3] WOODOVÁ, CH. *Bankovní služby bez poboček - Bankovnictví přes Internet - Komunikace* [online]. Poslední revize 5.10.2002 [cit. 25-2-2003]. Dostupné z < http://www.pcworld.cz>.

[4] *Dvoufaktorová autentizace* [online], [cit. 5-1-2003]. Dostupné z <http://system.ccb.cz/site/bezpecnost/cedrus.htm>.

[5] Propagační materiály jednotlivých bank [cit. 27-2-2003].

Kontaktní adresa:

Ing. Miloslav Hub
Ústav systémového inženýrství a informatiky, FES
Univerzita Pardubice
Studentská 84
530 09 Pardubice
E-mail: miloslav.hub@upce.cz

Recenzovala: Ing. Jitka Komárková, Ph.D., Ústav systémového inženýrství a informatiky, FES, Univerzita Pardubice