Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Bezpečnost internetového bankovnictví

Filip Kubec

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Akademický rok 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Filip Kubec

obor Informatika

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 16 určuje tuto bakalářskou práci.

Název práce: **Bezpečnost internetového bankovnictví**

Osnova bakalářské práce:

1. Úvod
2. Cíl práce a metodika
3. Systémy zabezpečení internetových finančních transakcí
4. Kontrola identity uživatele
5. Porovnání systémů zabezpečení
6. Závěr
7. Seznam použitých zdrojů
8. Přílohy

Rozsah hlavní textové části: 30 - 40 stran

Doporučené zdroje:

ANDERSON, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. 2. vyd. Indianapolis: Wiley, 2008.ISBN 978-0-470-06852-6

PŘIBYL, Jiří. Informační bezpečnost a utajování zpráv. 1. vyd. Praha: Vydavatelství ČVUT, 2004. ISBN 80-01-02863-1

SINGH, Simon. Kniha kódů a šifer : tajná komunikace od starého Egypta po kvantovou kryptografii. 2. vyd. Praha: Argo, 2009. ISBN 978-80-7363-268-7

Handbook of Applied Cryptography [online]. Dostupné z URL: http://www.cacr.math.uwaterloo.ca/hac/

Vedoucí bakalářské práce: **Ing. Marek Pícka**

Termín odevzdání bakalářské práce: březen 2011

.....
Vedoucí katedry

.....
Děkan

V Praze dne: 28. 2. 2011

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Bezpečnost internetového bankovnictví" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31.3.2011 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Marku Píckovi, za vedení při psaní bakalářské práce a za velmi cenné konzultování daného tématu. Dále neméně děkuji celé své rodině a bývalé přítelkyni za podporu a pomoc v průběhu mého studia a také Martinu Sitárovi, CISA, za zodpovězení otázek ohledně zabezpečení služby Mojebanka Komerční banky a několik dalších dobrých rad.

Bezpečnost internetového bankovnictví

Security of Internet Banking

Souhrn

Práce se věnuje tématu bezpečnosti internetového bankovnictví. Cílem práce je porovnání zabezpečení internetového bankovnictví jednotlivých finančních institucí v České republice. Tato služba se na finančním trhu začala objevovat v průběhu osmdesátých let dvacátého století a dodnes se poměrně rychle vyvíjí. Původně šlo o přístup přes terminály, což byly jedny z prvních informačních systémů pro domácí použití, dnes je tato služba zajištěna softwarově, za pomoci aplikací internetového bankovnictví. V první části práce jsou vysvětleny základy zabezpečování internetové komunikace. Následuje popis různých modelů kontroly identity uživatele. Na konci práce je popsáno a porovnáno několik modelů, které využívají naše banky.

Summary

This work focuses on the topic known as security of internet banking. The aim of the thesis is comparison of security solutions of various financial institutions in Czech Republic. This service appeared to a financial market during 1980's and is still quite rapidly developing. Firstly it was realized by terminals, which was kind of first information systems for end-users, today the service is provided by software means, using internet banking applications. First part of this work covers basics of securing the internet communication. The next part follows definition of several models of user authentication. The thesis is concluded with description and comparison of some models used at our banks.

Klíčová slova: banka, bezpečnost, certifikát, identita, internet, SSH, SSL, TLS

Keywords: bank, certificate, identity, internet, security, SSH, SSL, TLS

Obsah:

1. Úvod

Internet je komunikační síť propojující navzájem počítačové sítě po celém světě. Počítače v těchto sítích mezi sebou komunikují pomocí sady protokolů TCP/IP. Nejznámějšími a zřejmě i nejpoužívanějšími službami, které dnes internet poskytuje, jsou WWW (World Wide Web) a e-mail.

Za prvního předchůdce internetu lze považovat počítačovou síť, která byla roku 1968 instalována v Národní výzkumné laboratoři ve Velké Británii. Tato síť však fungovala jen v této jedné budově. První rozsáhlejší sítí byl až ARPANET, vytvořený americkou vládní agenturou ARPA (Advanced Research Projects Agency, agetura pro pokročilé výzkumné projekty), financované ministerstvem obrany USA. Jak je tedy zřejmé, tato síť sloužila hlavně pro vládní a vojenské účely.

První webové stránky spustil 6. června 1991 švýcarský institut pro jaderný výzkum CERN na adrese http://info.cern.ch/. Tyto stránky byly uloženy na jejich serveru, který byl v roce 1989 největším internetovým serverem v Evropě. V letošním roce tento web oslaví dvacet let své existence a tím i dvacet let fungování služby World Wide Web.

Od poloviny roku 1994 existuje WWW Consorcium (W3C), zahrnující několik členských organizací, které společně s veřejností stanovují a schvalují webové standardy a tím dohlížejí na rozvoj služby WWW. Tuto komunitu řídí Tim Berners-Lee, otec myšlenky a zakladatel služby WWW a Jeffrey Jaffe, který zastává funkci výkonného ředitele.

Než přišlo na řadu internetové bankovnictví, existovalo několik jiných způsobů bezhotovostního platebního styku. Například šek zaručuje svému držiteli (příjemci), že mu banka vydá uvedenou částku z účtu vystavitele šeku. Nejrozšířenějším prostředkem pro bezhotovostní platební styk však byly již od poloviny minulého století platební karty. V roce 1969 byla vydána první karta s magnetickým proužkem, který v sobě nesl statická data o klientovi a přepisovatelná data o zůstatku na klientově účtu. První platební karta s čipem se objevila v roce 1974. U nás byla průkopníkem v oblasti platebních karet Živnostenská banka, která začala roku 1988 vydávat tyto karty k tuzexovému účtu. V roce 1991 pak vydala první Visa kartu u nás.

Přímým předchůdcem moderního domácího online bankovnictví byl v roce 1981 přístup k bankovním službám čtyř hlavních New Yorských bank (Citibank, Chase Manhattan, Chemical a Manufacturers Hanover) za pomoci systému videotex, což byla jedna z prvních realizací informačního systému pro koncového uživatele. V roce 1983 je následovala Bank of Scotland se systémem Prestel. V roce 1994 pak přišla Stanford Federal Credit Union (Palo Alto, Calofornia) s prvním online internetovým bankovnictvím, které mohli využívat všichni její klienti.

2. Cíl práce a metodika

Cílem této práce je porovnání způsobů zabezpečení aplikací internetového bankovnictví a přístupu k nim a zabezpečení internetových finančních transakcí u různých bankovních institucí v České republice. Z tohoto porovnání by měly být zřejmé klady i zápory jednotlivých řešení.

Nejprve se tedy pokusím seznámit čtenáře s problematikou bezpečnosti na internetu, konkrétně pak s bezpečností internetového bankovnictví. Podrobněji budu rozebírat jednotlivé způsoby zabezpečení internetových datových toků, uvedu, které z těchto jsou nejlepší a nejčastěji používané právě pro zabezpečení komunikace klienta se serverem banky a dále pak budu popisovat několik způsobů ověření identity uživatele při přístupu k aplikacím internetového bankovnictví.

Mezi používané technologie zabezpečení datových toků se řadí SSH (Secure Shell), SSL (Secure Sockets Layer) a TLS (Transport Layer Security). Ze způsobů ověření identity uživatele jsou to certifikáty, čipové karty, bezpečnostní klíče v podobě kalkulačky pro generování jednorázových hesel a samozřejmě hesla samotná, která si v případě využívání certifikátu nebo čipové karty uživatel sám vytvoří, nebo jsou mu vygenerována bankou, pro mnohonásobné použití k přístupu do aplikace internetového bankovnictví, nebo od banky obdrží sadu hesel jednorázových.

Pro stručný přehled práce uvedu obsah následujících kapitol. V kapitole třetí popisuji jednotlivé systémy zabezpečení internetových finančních transakcí. V kapitole čtvrté popisuji způsoby kontroly identity uživatele. Kapitola pátá popisuje zabezpečení jednotlivých služeb internetového bankovnictví u několika bank na základě informací, získaných z krátkého dotazníku a demoverzí jejich aplikací internetového bankovnictví.

3. Systémy zabezpečení internetových finančních transakcí

V dnešní době velká část finančních transakcí probíhá přes internet, a to nejen formou platebních příkazů v aplikacích internetového bankovnictví. Už jen samotný výběr z bankomatu cizí banky znamená, že vaše banka, tedy ta, u které máte svůj běžný účet, musí vybrané peníze uhradit bance, z jejíhož bankomatu jste je vybrali, a to právě formou internetové transakce. Podobně pokud svůj nákup zaplatíte platební kartou, vaše banka musí nákup uhradit na účet banky, u které má obchodník svůj účet. Pokud máme porozumět zabezpečení těchto finančních toků, měli bychom začít od úplného základu. Tím základem je šifrování.

3.1 Informační bezpečnost

K porozumění šifrování je nezbytné pochopit záležitosti spojené s informační bezpečností v obecném smyslu. Informační bezpečnost se v závislosti na situaci a požadavcích projevuje různými způsoby. Bez ohledu na to, kdo je do předávání dat zapojen, všichni účastníci musí mít jistotu, že budou plněny určité bezpečnostní předpoklady. Některé z nich jsou uvedeny níže (viz Tabulka 1).

soukromí/utajení	**povolit přístup k informacím pouze těm, kteří jsou k tomu**
integrita dat	**zajištění proti neoprávněné změně**
ověření/identifikace subjektu	**potvrzení totožnosti**
ověření zprávy (MAC)	**potvrzení zdroje informace/ověření původu informace (message authentication code)**
podpis	**prostředek k propojení informace a subjektu**
certifikace	**schválení pravosti informace důvěrným subjektem**
časová razítka	**zaznamenání časového údaje o vzniku nebo existenci**
Non-repudiation (nezamítnutelnost)	**prevence proti zamítnutí/popření předchozích závazků nebo akcí**
odvolání	**odvolání osvědčení (certifikace) nebo povolení**

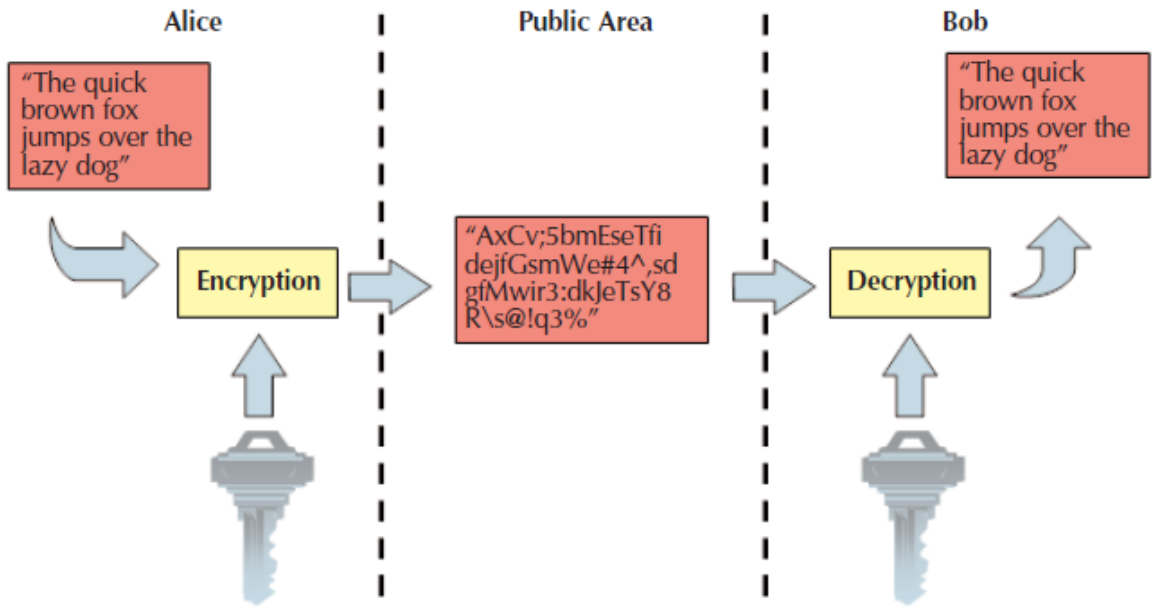
Tabulka 1 - Bezpečnostní předpoklady síťové komunikace[1]

Podpis je tedy jedním ze základních nástrojů, používaných v informační bezpečnosti. Je to základní kámen mnoha dalších služeb, jako je ověření původu dat nebo identifikace.[1]

[1] MENEZES, A. J., VAN OORSCHOT, P. C., VANSTONE, S. A., Handbook of Applied Cryptography, s. 3

3.2 Šifrování

Šifrování je postaveno na dvou základních procesech: zašifrování a dešifrování (viz Obrázek 1). Zašifrování přemění holý text na šifru, kterou je možné opačným postupem, dešifrováním, přeměnit zpět na holý text.

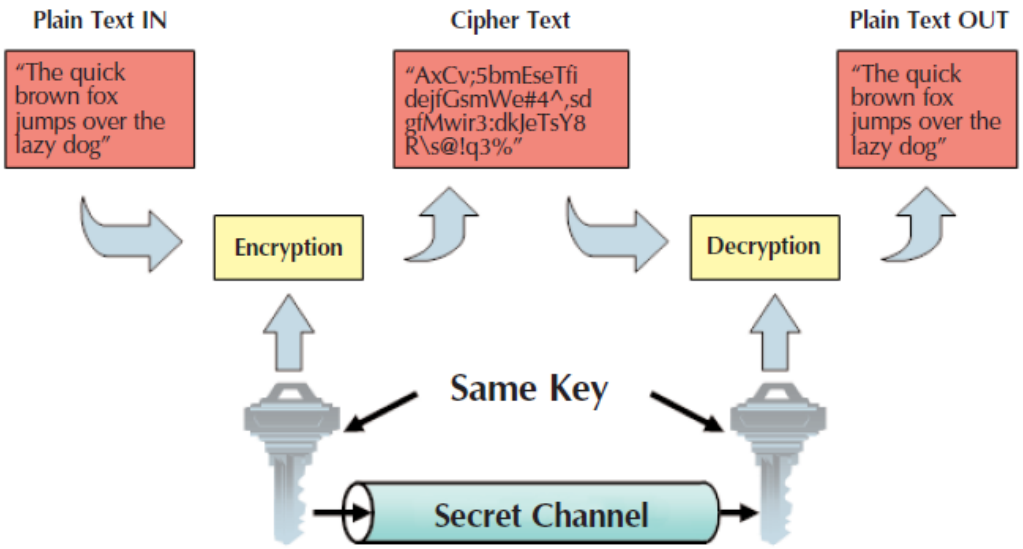


Obrázek 1 – Šifrování[2]

V dnešní době jsou oba dva základní šifrovací modely jsou odvozeny z matematických funkcí. Jsou to symetrické šifry a asymetrické šifry. Ve spojení s nimi se navíc používají hash functions (hashovaní funkce, hašovací funkce) jako dodatečný bezpečnostní prvek.[2]

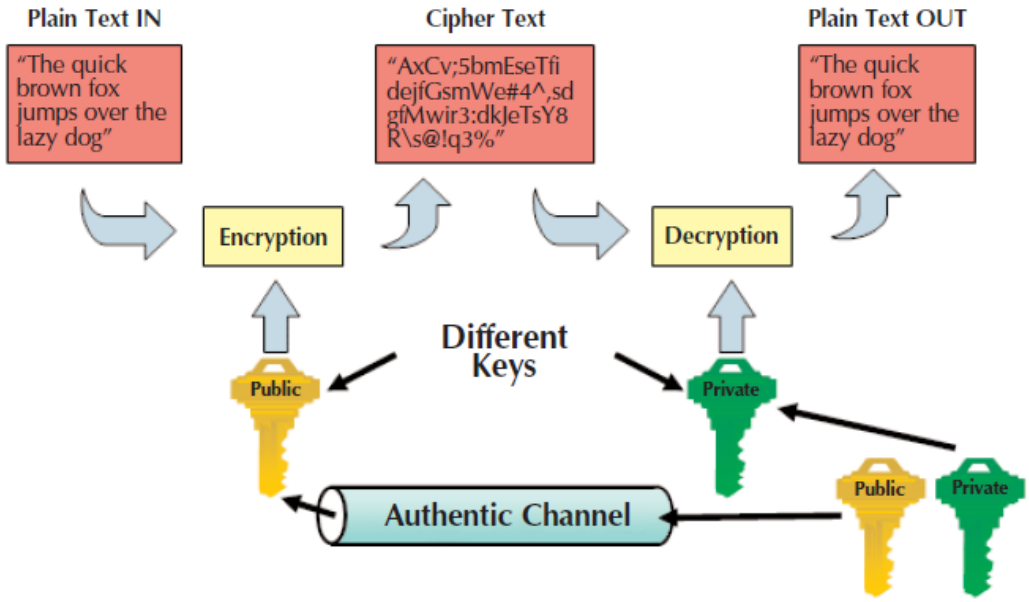
- *Symetrické šifry* (viz Obrázek 2) používají k zašifrování i dešifrování stejný klíč. Využívají matematické funkce transpozice a substituce. Transpozice znamená, že znaky z šifrovaného textu jsou umístěna na jinou pozici v šifře. Například slovo „šifra“ zašifruje jako „ifraš“. Substituce nahrazuje znaky jinými znaky. Například slovo „heslo“ zašifruje jako „nudfe“ nahrazením písmen „k“ za „n“, „e“ za „u“, „s“ za „d“, „l“ za „f“ a „o“ za „e“.

[2] DE CLERCQ, J., Understanding and Leveraging SSL-TLS for Secure Communications, s. 3



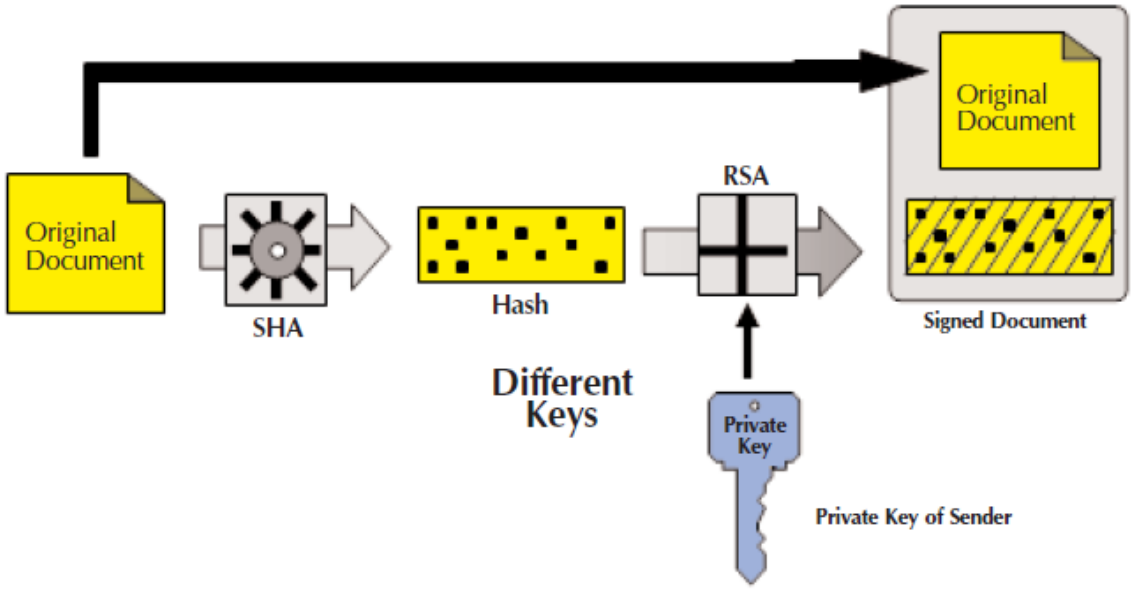
Obrázek 2 - Symetrická šifra

- *Asymetrické šifry* (viz Obrázek 3) používají pro zašifrování a dešifrování odlišné klíče. Jsou odvozeny ze složitějších matematických problémů, jako jsou faktorizace, diskrétní logaritmus nebo teorie eliptické křivky.



Obrázek 3 - Asymetrická šifra

- *Hash functions* (viz Obrázek 4) jsou postaveny na jednocestných matematických funkcích. Nejčastěji se používají pro poskytnutí služeb integrity, utajení a ověření pravosti. Vstupní data mohou mít libovolnou délku, ale jsou redukována na řetězec fixní velikosti. Výstupem je digitální otisk (hash). Pokud je originální zpráva během přenosu změněna, příjemce to zjistí, protože zpráva a otisk do sebe „nezapadnou“.



Obrázek 4 - Hash function[3]

Tyto tři výše uvedené modely mají různé charakteristiky, a tedy slouží různým cílům. Většina bezpečnostních řešení je kombinací těchto tří základních a jsou nazývána hybridní kryptografická řešení, kterými se bude tato práce zabývat později.

U mnoha šifrovacích řešení je znám algoritmus, na kterém jsou postavena, což na jednu stranu umožňuje jejich analýzu a rozvoj efektivnějších implementací, avšak potřebujeme něco dalšího, co by zajistilo utajení. A tím je šifrovací klíč, který má funkci tajného vstupního parametru šifrovacího procesu.[3]

[3] DE CLERCQ, J., Understanding and Leveraging SSL-TLS for Secure Communications, s. 9

3.3 Hybridní kryptografická řešení

Jak už je uvedeno výše, hybridní systémy jsou kombinací základních šifrovacích modelů. Používají symetrický klíč a algoritmus k zakódování zprávy, poté použijí veřejný klíč příjemce k zakódování symetrického klíče do tzv. schránky (lockbox), kterou pak lze společně se zakódovanou informací odeslat příjemci v podobě tzv. digitální obálky. Příjemce poté použije soukromý klíč k dešifrování schránky a získaný symetrický klíč k dešifrování zprávy. Je tedy použit rychlejší symetrický klíč na zprávu a zároveň jsou využity výhody bezpečnější metody zašifrování šifrovacího klíče asymetrickou šifrou. Příkladem hybridních kryptografických řešení jsou protokoly SSL/TLS, SSH a standard S/MIME, používaný k zabezpečení emailové komunikace.[4]

[4] DE CLERCQ, J., Understanding and Leveraging SSL-TLS for Secure Communications, s. 10

3.4 SSH

Protokol SSH (viz Obrázek 5) byl vyvinut v roce 1995 Tatu Ylönenem na Helsinské Technické Universitě ve Finsku a nahradil dříve používaný nezabezpečený telnet. Tatu začátkem toho roku zaznamenal útok na universitní síť s cílem získat přístupová hesla, a proto vyvinul toto bezpečnostní řešení. Původně mělo sloužit pouze pro zabezpečení universitní sítě, ale brzy si uvědomil, že jeho produkt by mohl mít širší využití. Uvolnil tedy SSH1 jako open source produkt (produkt s volně přístupným a upravitelným zdrojovým kódem) založený na protokolu SSH-1 pro všechny uživatele pracující s operačními systémy založenými na Unixu.

Hned z počátku, s tím, jak software nabýval na popularitě, začalo se objevovat mnoho chyb a problémů, které nebylo možné opravit tak, aby nebyla ztracena zpětná kompatibilita. Proto byla již v roce 1996 představená nová verze protokolu, SSH-2.

Až v roce 1998 byl však pro nový protokol vyvinut softwarový produkt SSH2. Ten ale nedosáhl předpokládaného úspěchu. Za prvé proto, že mu oproti SSH1 chybí několik užitečných a praktických možností konfigurace, za druhé proto, že jde o komerční produkt, a tedy není volně dostupný.

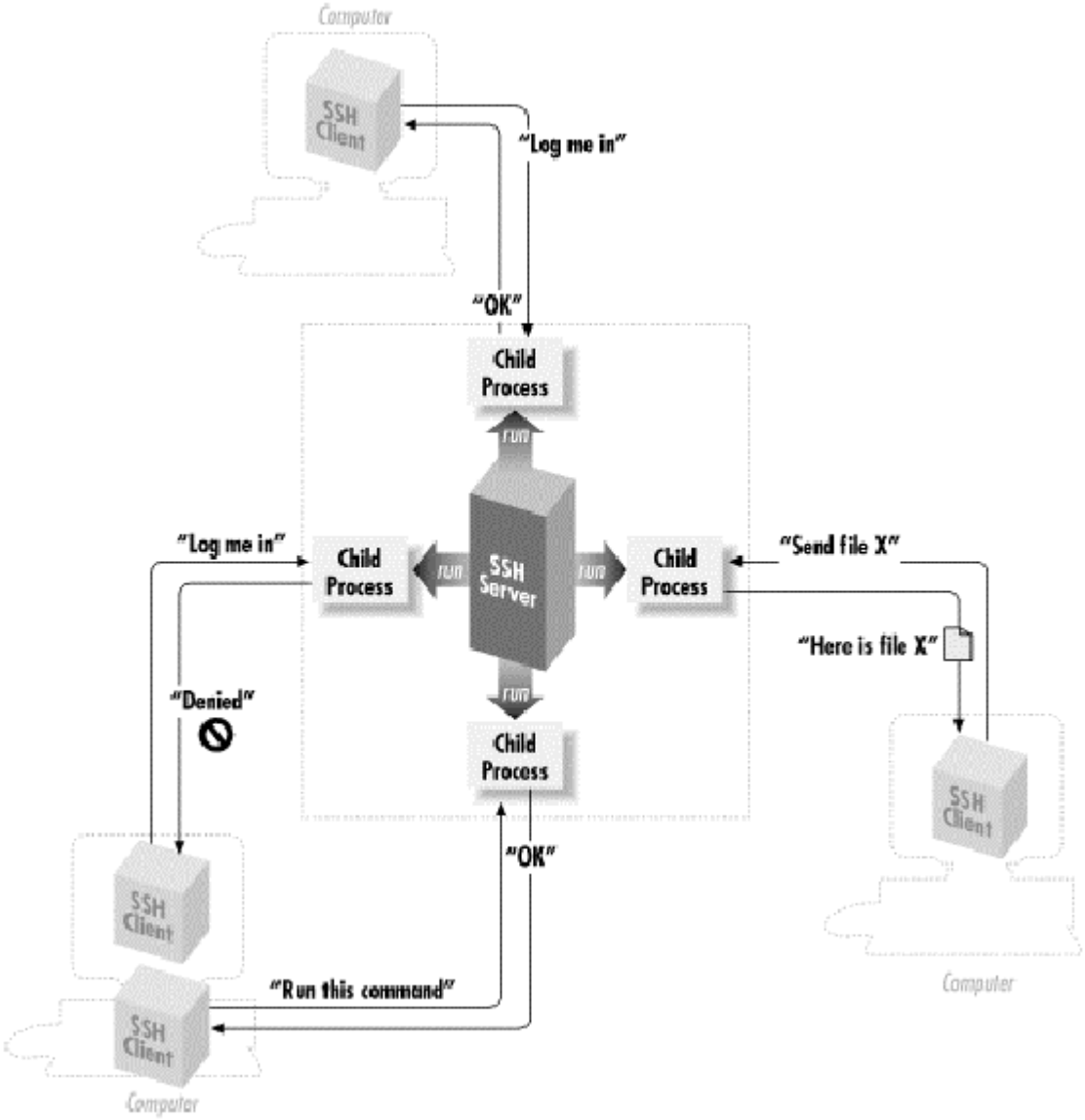
Zjednodušeně původní protokol SSH sloužil jako zabezpečená alternativa k příkazům pro přístup k souborům v jiném počítači (r-commands): rsh (vzdálený shell, remote shell), rlogin (vzdálené přihlášení, remote login) a rcp (vzdálené kopírování, remote copy).[5]

Práce protokolu SSH-1 spočívá ve 4 hlavních krocích:

- Než spolu klient a server začnou komunikovat, je třeba navázat bezpečné spojení, aby mohli sdílet šifrovací klíče, hesla a všechna další data. To proběhne jednoduše tak, že klient kontaktuje server, dohodnou se na verzi SSH protokolu, který oba podporují, poté přepnou na paketový protokol, server poskytne klientovi parametry spojení, klient pošle serveru svůj tajný klíč, zakódovaný pomocí přijatých parametrů a na základně tohoto klíče jsou následně zašifrována veškerá přenášená data.

[5] BARRET, D. J., SILVERMAN, R., SSH, The Secure Shell: The Definitive Guide, s. 1

- V dalším kroku klient prokáže svojí totožnost jednou z možných metod (heslo, veřejný klíč, …).



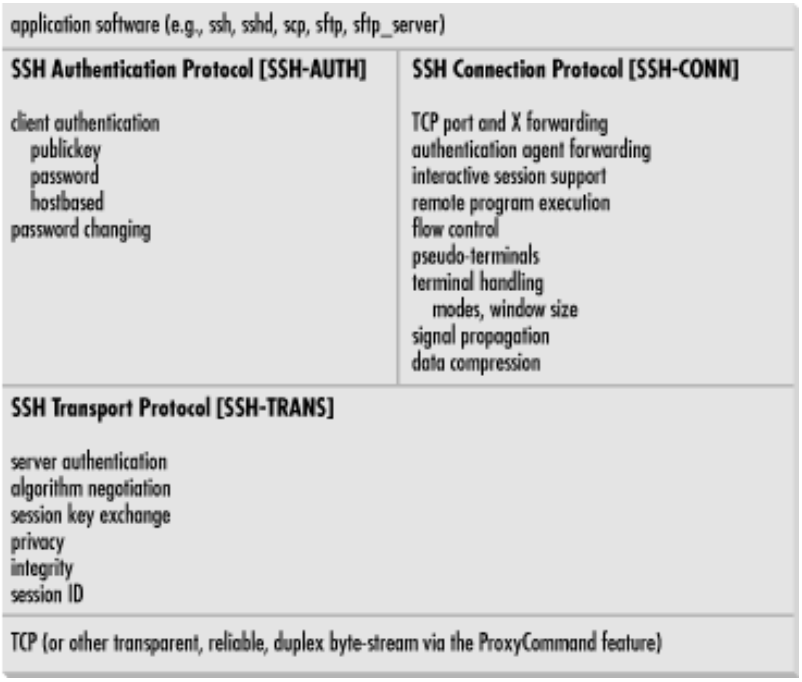
Obrázek 5 – Architektura SSH[6]

- Kontrola integrity dat byla jednou z největších slabin protokolu SSH-1, proto je v protokolu SSH-2 použita novější metoda.

- Posledním krokem je komprese dat, ke které protokol SSH-1 používá službu zip operačního systému GNU.[6]

[6] BARRET, D. J., SILVERMAN, R., SSH, The Secure Shell: The Definitive Guide, s. 2

Na rozdíl od SSH-1, který zahrnuje několik funkcí do jednoho protokolu, je SSH-2 rozdělen na několik modulů a skládá se ze tří spolupracujících protokolů (viz Obrázek 6), čímž se jeho architektura podobá protokolu SSL: [7]



Obrázek 6 - SSH-2 protokoly[7]

- SSH Transport Layer Protocol je základní stavební blok, který zajišťuje počáteční spojení, paketový protokol, ověření identity serveru, základní šifrování a integritu přenášených dat.
- SSH Authentication Protocol zasílá serveru ověření identity klienta buď metodou veřejného klíče, nebo metodou „hostbased“, nebo pomocí hesla.
- SSH Connection Protocol zprostředkovává komunikaci aplikační vrstvy se sítí a může vytvořit několik komunikačních kanálů skrze jedno připojení.

[7] BARRET, D. J., SILVERMAN, R., SSH, The Secure Shell: The Definitive Guide, s. 58

Mezi hlavní vylepšení u SSH-2 patří:

- Rozšíření nabídky šifrovacích algoritmů mezi klientem a serverem, kterými jsou například „host key“ nebo „hash function“.
- Silnější kontrola integrity dat za pomoci MAC (Message Authentication Code).
- „Session rekeying“, což znamená, že pokud jsou šifrovány velké objemy dat, periodicky se mění šifrovací klíč.

Obrázek 7 shrnuje některé důležité rozdíly mezi SSH-1 a SSH-2. [8]

SSH-2	SSH-1
Separate transport, authentication, and connection protocols.	One monolithic protocol.
Strong cryptographic integrity check.	Weak CRC-32 integrity check.
Supports password changing.	N/A
Any number of session channels per connection (including none).	Exactly one session channel per connection (requires issuing a remote command even when you don't want one).
Full negotiation of modular cryptographic and compression algorithms, including bulk encryption, MAC, and public-key.	Negotiates only the bulk cipher; all others are fixed.
Encryption, MAC, and compression are negotiated separately for each direction, with independent keys.	The same algorithms and keys are used in both directions (although RC4 uses separate keys, since the algorithm's design demands that keys not be reused).
Extensible algorithm/protocol naming scheme allows local extensions while preserving interoperability.	Fixed encoding precludes interoperable additions.

Obrázek 7 - Porovnání SSH-1 a SSH-2[8]

[8] BARRET, D. J., SILVERMAN, R., SSH, The Secure Shell: The Definitive Guide, s. 62

3.5 SSL

Protokol SSL (Secure Sockets Layer) začala vyvíjet firma Netscape Communications na počátku 90. let 20. století. Vyvíjel se ve třech verzích (SSL 1.0, SSL 2.0, SSL 3.0) a v dnešní době je nahrazen novějším protokolem TLS (Transport Layer Security). Je určen pro komunikaci mezi klientem a serverem a zajišťuje následující základní bezpečnostní služby:

- ověření pravosti (ten, s kým komunikuji, je opravdu tím, za koho se vydává)
- důvěrnost spojení (nikdo cizí nemůže vidět obsah komunikace)
- integrita spojení (nikdo cizí nemůže změnit obsah komunikace)

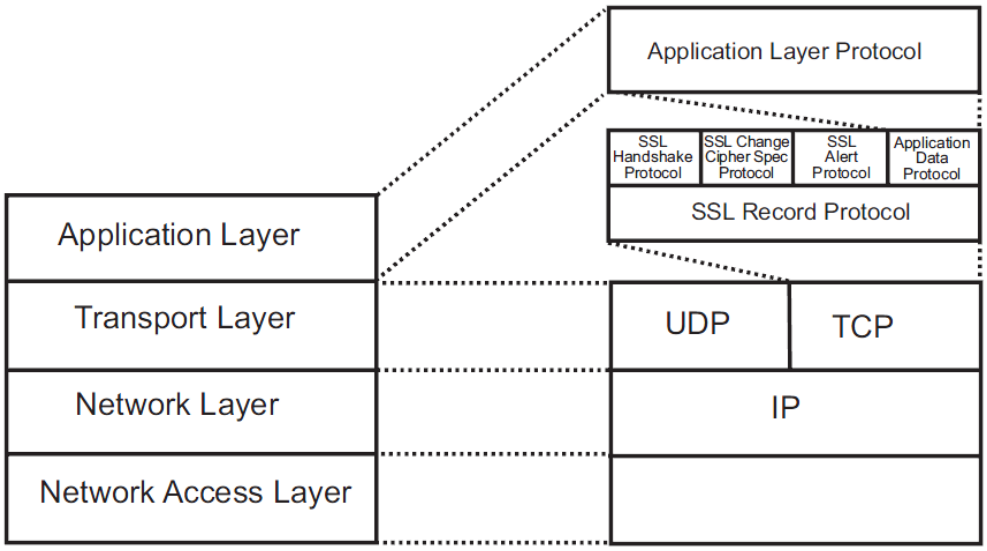
Jak je zřejmé z názvu, protokol SSL je orientovaný na sockety, to znamená, že všechna, nebo žádná z dat zaslaných nebo přijatých ze socketu jsou zašifrována úplně stejně. Není tedy možné přidat například digitální podpis pouze k jedné části dat.

Zjednodušeně jde o vrstvu, ležící mezi přenosovou (komunikační) vrstvou a aplikační vrstvou. Rozsah jejích funkcí je dvojí: [9]

- Za prvé zavádí bezpečné spojení mezi komunikujícími stranami.
- Za druhé používá toto spojení k bezpečnému přenosu dat vyšší vrstvy (aplikační) od odesilatele k příjemci. Rozdělí tedy data na přenositelné části (tzv. fragmenty) a zpracovává každý zvlášť. Konkrétně každý fragment může být komprimován, označen pomocí MAC (Message Authentication Code), zašifrován a rozšířen o záhlaví, poté je odeslán. Každý takový fragment se označuje jako SSL záznam. Ten je na straně příjemce dešifrován, ověřen podle MAC, dekomprimován a spojen s ostatními fragmenty, aby mohla být data odeslána příslušné vyšší vrstvě.

Obrázek 8 znázorňuje umístění SSL vrstvy. Skládá se ze dvou podvrstev a několika podprotokolů:

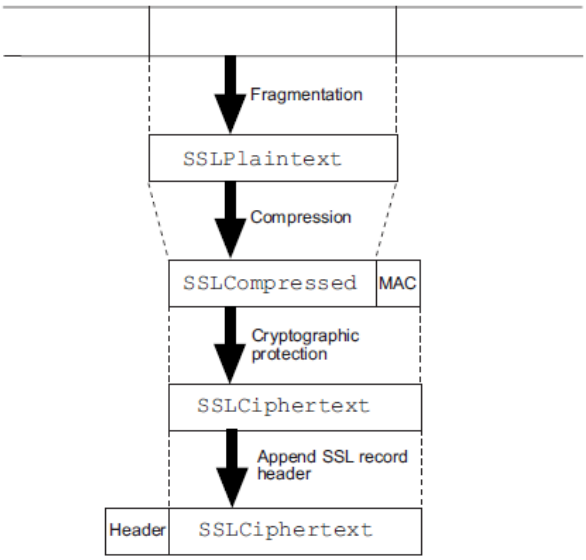
[9] OPPLIGER, R., SSL and TLS: Theory and Practice, s. 75



Obrázek 8 - Vrstva SSL a její podvrstvy a podprotokoly v kontextu[10]

- Spodní vrstva leží na některé z možných vrstev zajišťujících spojení a přenos dat, může to být například protokol TCP/IP. Tato vrstva obsahuje SSL Recor Protocol (SSL záznamový protokol, viz Obrázek 9) a zajišťuje výše zmíněnou druhou funkci (práce s daty): [10]

    - Fragmentace je první krok práce s daty v SSL Record Protocol. Data z vyšší vrstvy jsou rozdělena do bloků velikosti 2^{14} bytů nebo menších.



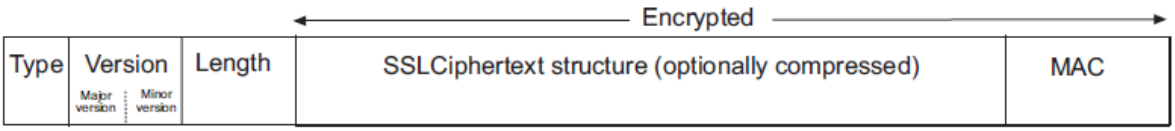
Obrázek 9 - SSL Record Protocol[10]

[10] OPPLIGER, R., SSL and TLS: Theory and Practice, s. 88

- Dalším krokem je komprese (komprimace), která je volitelná a obvykle se nepoužívá.

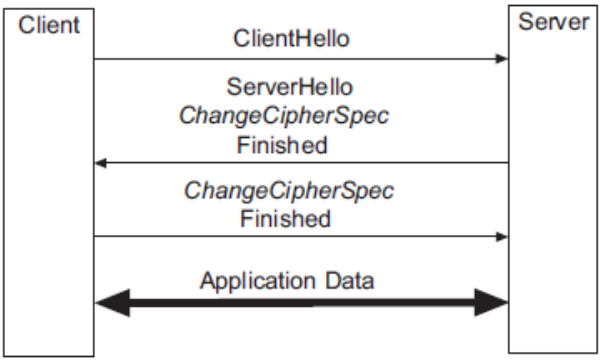
- Následuje šifrování, které zahrnuje šifrování dat a ověření identity zprávy (přidělení MAC). To lze provést třemi způsoby. Zaprvé ověřením zprávy a zašifrováním zprávy společně s MAC; tento způsob používají například protokoly SSL/TLS. Zadruhé zašifrováním zprávy a ověřením šifry; tento způsob používá například protokol IPsec. Zatřetí zašifrováním zprávy a ověřením zprávy; tento způsob používá například protokol SSH.

- Nakonec je k výslednému balíčku přidána hlavička (SSL Record Header). Konečný výstup z SSL Record Protocol znázorňuje Obrázek 10.



Obrázek 10 - SSL record[11]

- Vrchní vrstva leží navrch SSL záznamového protokolu a obsahuje čtyři protokoly:[11]
  - SSL Handshake Protocol (viz Obrázek 11) umožňuje vzájemné ověření identity mezi komunikujícími stranami a dohodu o použité šifrovací sadě a kompresní metodě použité pro komunikaci.



Obrázek 11 - SSL Handshake Protocol (zjednodušený)[11]

[11] OPPLIGER, R., SSL and TLS: Theory and Practice, s. 94

- SSL Change Cipher Spec Protocol umožňuje komunikujícím stranám oznámit změnu šifrování, umístit bezpečnostní parametry na správné místo a zajistit jejich účinnost.
- SSL Alert Protocol umožňuje komunikujícím stranám oznámení a výměnu výstražných zpráv.
- SSL Application Data Protocol je nejpodstatnější částí SSL. Přenáší data z vyšší – nejčastěji aplikační – vrstvy do SSL záznamového protokolu, kde jsou šifrována a odtud bezpečně přenesena.

Jednou z velkých výhod SSL protokolu je jeho nezávislost na protokolu aplikační vrstvy. To znamená, že na SSL vrstvu může být položena jakákoliv aplikační vrstva založená na TCP.

Cílem SSL protokolu je tedy bezpečný přenos aplikačních dat mezi komunikujícími stranami. Za tímto účelem SSL protokol vytváří a používá SSL connections (SSL připojení) a SSL sessions:

- SSL připojení je použito pro přenos dat mezi dvěma komunikujícími stranami, např. mezi klientem a serverem ve formě zašifrovaného, případně navíc komprimovaného balíčku. Avšak k těmto datům se pojí některé šifrovací a jiné parametry, které nejsou s těmito z bezpečnostních důvodů přenášena. Za tímto účelem je ke každému jednomu nebo více SSL připojením přiřazeno SSL session.
- SSL session je propojení dvou komunikujících stran vytvořené SSL Handshake protokolem. SSL session vymezuje sadu šifrovacích a dalších parametrů použitých k zabezpečení a případné komprimaci přenášených dat. Proto může být SSL session sdílena několika SSL připojeními.

Mezi dvěma entitami tedy může být několik SSL připojení zároveň. Teoreticky mezi nimi může existovat v jednu chvíli i několik SSL sessions, ale tato možnost se využívá jen zřídka.

Podobně jako u procesů běžících na procesoru, i SSL připojení a SSL sessions nabývají v průběhu své existence různých stavů. Tyto stavy zavádí na obou stranách komunikačního kanálu SSL Handshake Protocol, který je zároveň koordinuje a synchronizuje. Celkem existují čtyři stavy: probíhá čtení, probíhá zápis, čekající na čtení a čekající na zápis.

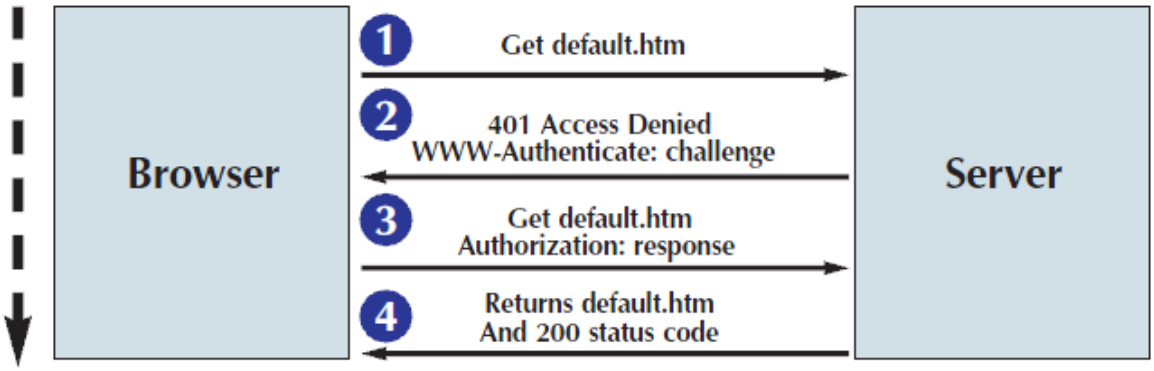
SSL je tedy šifrovací protokol, to znamená, že používá různé šifrovací techniky. Konkrétně pro šifrování dat a ověření pravosti zprávy používá šifrovací metodu skrytého klíče, pro ověření identity uživatele a ustanovení šifrovacího klíče používá šifrovací metodu veřejného klíče. Existují tři základní algoritmy pro výměnu šifrovacího klíče: RSA, Diffie-Hellman a FORTEZZA.[12]

[12] OPPLIGER, R., SSL and TLS: Theory and Practice, s. 81

3.6 SSL v porovnání s dalšími protokoly ověření identity klienta

V protokolu SSL probíhá ověření identity klienta na základě certifikátu, existují ale i další možnosti, z nichž nejznámější jsou základní ověření (basic authentication) a výběrové ověření (digest authentication). Nejprve ale vysvětlím HTTP ověření, z kterého se tyto dvě možnosti ověřování odvíjejí.

Toto nejjednodušší ověřování, které se odehrává mezi webovým serverem a prohlížečem, probíhá ve čtyřech krocích (viz Obrázek 12). V prvním kroku prohlížeč odešle serveru požadavek na data. Pokud server požaduje po klientovi ověření jeho identity, pošle jako odpověď chybovou zprávu 401 (neautorizovaný přístup) a společně s ní seznam ověřovacích protokolů a výzvu k potvrzení identity. Webový prohlížeč si vybere jeden z nabídnutých ověřovacích protokolů a na základně přijaté výzvy a přístupových práv uživatele (uživatelské jméno, heslo, …) vytvoří odpověď, kterou odešle serveru. Pokud server na základně této odpovědi usoudí, že je vše v pořádku, pošle uživateli požadovaná data a stavový kód 200 (tzv. „no errors“ zpráva).[13]

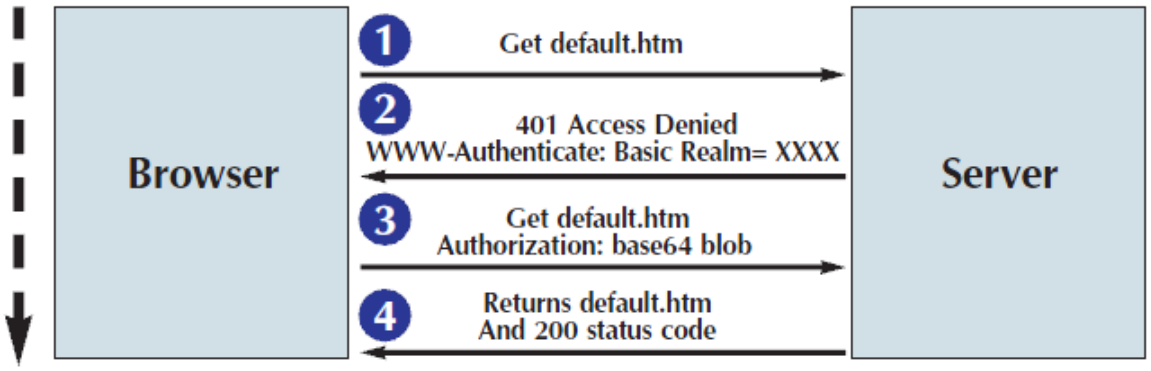


Obrázek 12 - HTTP ověření[13]

Protokol základního ověření je součástí specifikace protokolu HTTP/1.0, takže funguje s jakýmkoliv webovým prohlížečem. Pomocí jednoduchého mechanismu přenáší přihlašovací údaje uživatele na webový server. Oproti výše uvedenému způsobu se liší ve druhém a třetím kroku (viz Obrázek 13). V tomto případě server ve druhém kroku odešle prohlížeči navíc jméno základní ověřovací oblasti (basic authentication realm) a prohlížeč

[13] DE CLERCQ, J., Understanding and Leveraging SSL-TLS for Secure Communications, s. 59

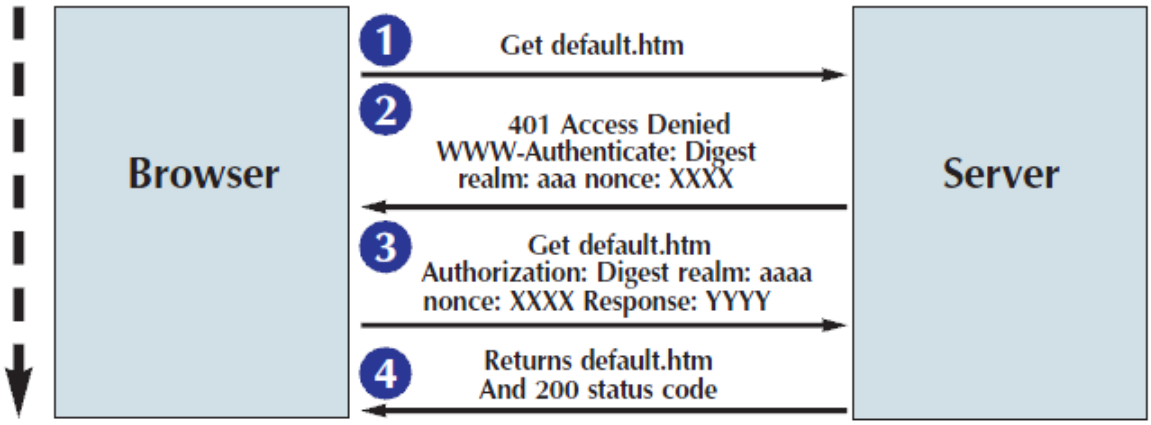
ve třetím kroku zakóduje uživatelské jméno, heslo a jméno základní ověřovací oblasti pomocí base64 šifrování a tento balíček zašle zpět serveru. V případě základního ověřování lze navíc zahrnout uživatelské jméno a heslo přímo do URL v tomto formátu: http://username:password@website.com, není to však příliš bezpečné z důvodu použití jednoduchého base64 šifrování.



Obrázek 13 - Základní ověření (basic authentication)[14]

Protokol výběrového ověření byl původně uveden již ve specifikaci protokolu HTTP/1.0, jeho rozšířená a dnes používaná verze je však uvedena až ve specifikaci protokolu HTTP/1.1. Výběrové ověření je opět založeno na předchozích dvou způsobech a opět nabízí důležité vylepšení, kterým je lepší kódování přístupových údajů uživatele. Oproti výše uvedeným se liší ve druhém, třetím (viz Obrázek 14) a čtvrtém kroku. Ve druhém kroku server odešle prohlížeči kromě chybové zprávy 401 navíc klíčové slovo „digest“ a seznam výběrových ověřovacích oblastí (digest authentication realm), do kterých webová stránka patří. Nejdůležitější část zprávy pro prohlížeč je výběrová výzva (digest challenge), obvykle označovaná jako „nonce“ (only once, pouze jednou; unikátní kód). Následně prohlížeč použije uživatelovo heslo k vytvoření hashe k výzvě a ten společně s výzvou a ověřovací oblastí odešle zpět serveru. Ten porovná přijatý hash s tím, který si sám vypočítal (podle uživatelova hesla, ke kterému má přístup) a pokud je vše v pořádku, odešle prohlížeči požadovaná data.[14]

[14] DE CLERCQ, J., Understanding and Leveraging SSL-TLS for Secure Communications, s. 39



Obrázek 14 - Výběrové ověření (Digest authentication)[15]

Z následujícího porovnání (viz Obrázek 15) výše uvedených způsobů ověřování identity uživatele s ověřováním pomocí certifikátu, které používá SSL, jsou zřejmé výhody i nevýhody každého z nich.[15]

	Basic Authentication	Digest Authentication	SSL Client Certificate-Based Authentication
Protocol based on open standard	Yes	Yes	Yes
Browser support	Internet Explorer Netscape Navigator Mozilla Firefox	Internet Explorer	Internet Explorer Netscape Navigator Mozilla Firefox
Communication security strength	Weak—base64 encoded, requires SSL	Stronger—because based on a challenge-response mechanism	Strong—because based on asymmetric cryptographic mechanism
Requires SSL	Yes	No	Yes
Supports authentication through firewalls and proxies	Yes	Yes	Yes
Authentication strength	Low—because based on the use of a user ID password	Low—because based on the use of a user ID password	High—because based on the use of private keys and certificates

Obrázek 15 – Porovnání metod ověřování[15]

[15] DE CLERCQ, J., Understanding and Leveraging SSL-TLS for Secure Communications, s. 40

3.7 TLS

Protokol TLS je strukturně identický s protokolem SSL. Má však oproti němu mnoho nových možností a postupů. Například je možné rozšíření o nové typy záznamů (record types), které budou dodatečně definovány pro TLS záznamový protokol (TLS Record Protocol).

Nejzřetelnějším rozdílem mezi SSL a TLS je způsob, kterým generují šifrovací materiál. Oba protokoly používají pro vytváření šifrovacích parametrů generátor s jedinečnou konstrukcí, TLS je však specifické tím, že tato konstrukce je založena na skupině pseudonáhodných funkcí (pseudo random function family, PRF). Ta u TLS 1.0 a TLS 1.1 kombinuje dvě hašovací funkce – MD5 a SHA-1 – k vytvoření digitálního podpisu, u TLS 1.2 už je použita pouze jedna z nich.

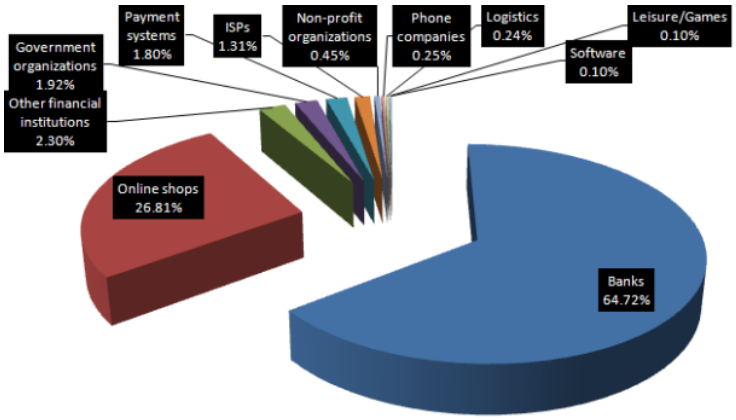
Dnes existují tři verze TLS protokolu. Protokol TLS 1.0 je velmi podobný a zpětně kompatibilní s SSL 3.0, dříve se tedy o něm mluvilo spíš jako o SSL 3.1. Protokol TLS 1.1 je také zpětně kompatibilní s SSL 3.0 i TLS 1.0, zejména co se šifrovacích sad týče. Ale při vytváření spojení už TLS 1.1 nesmí používat staré šifrovací sady, používané SSL 3.0 a TLS 1.0. Konečně TLS 1.2 používá zcela nové šifrovací sady. [16]

[16] OPPLIGER, R., SSL and TLS: Theory and Practice, s. 133

4. Kontrola identity uživatele

Ačkoli již internet existuje několik desetiletí a bezpečnostní opatření na této celosvětové síti se vysokým tempem vyvíjí, téměř stejně rychle se zdokonalují i pokusy tato opatření prolomit. V dnešní době většina dat, která mají nějakou hodnotu, jsou chráněna především přístupovými právy. Proto pokud chce někdo tato data neprávem získat, je nejjednodušší získat nejprve přístupová práva k nim.

V dnešní době stále roste počet případů zneužití online identity. Nejběžnějšími jsou phishing, což jsou v principu podvodné e-maily, požadující po uživateli zadání jeho přístupových údajů do formuláře na falešné stránce, man-in-the-middle, kdy jde o odposlouchávání komunikace a malware, což může být v tomto případě podvodný software typu keylogger. Pro příklad v roce 2007 byly finanční instituce terčem 92.6 % všech online phishingových útoků. Obrázek 16 znázorňuje cílení phishingových útoků v roce 2010 (banky znázorněny modrou barvou). [17]



Obrázek 16 - Cíle phishingových útoků[17]

Jádrem provádění internetových finančních transakcí je potřeba vzájemně rozpoznatelných identit. Uživatel potřebuje mít jistotu, že své peníze posílá té správné organizaci, stejně tak organizace musí důvěřovat identitě uživatele. Dříve k tomuto účelu postačovalo uživatelské jméno a heslo. Dnes se však ukazuje, že s rostoucím počtem útoků s cílem tyto údaje získat, není již déle bezpečné použití hesla jako jediného identifikačního prvku.

[17] http://www.racknine.com/blog/software/phishing-attacks-on-the-rise/

4.1 Požadavky na metody ověřování identity

Proto bylo vyvinuto mnoho nových metod ověřování identity. Aby jakýkoliv nový způsob ověření identity byl využitelný v praxi, nesmí být příliš pracný a jeho zavedení nesmí být přehnaně finančně náročné, zvlášť pro koncového uživatele. To by ho totiž odrazovalo od jeho využití. Existují tedy čtyři základní kritéria pro hodnocení efektivity technik ověřování identity: [18]

- *Silné zabezpečení* znamená poskytnutí nějakého dodatečného faktoru pro ověření identity, který zmírní nedostatky využití samotného hesla.

- *Flexibilita a odhad nebezpečí* nám říká, že hloubka, do jaké je ověřována identita entity, má být pouze taková, jakou vyžaduje odhadnutá hrozba. To znamená, že pro přístup k účtu z domova je odhadnuté nebezpeční nižší, než pro převod mezi dvěma bankami, prováděný ze zahraničí.

- *Jednoduchost použití* je významný prvek ve vztahu k uživateli. Pokud je přístup příliš těžkopádný nebo matoucí, uživatel raději zvolí jinou možnost.

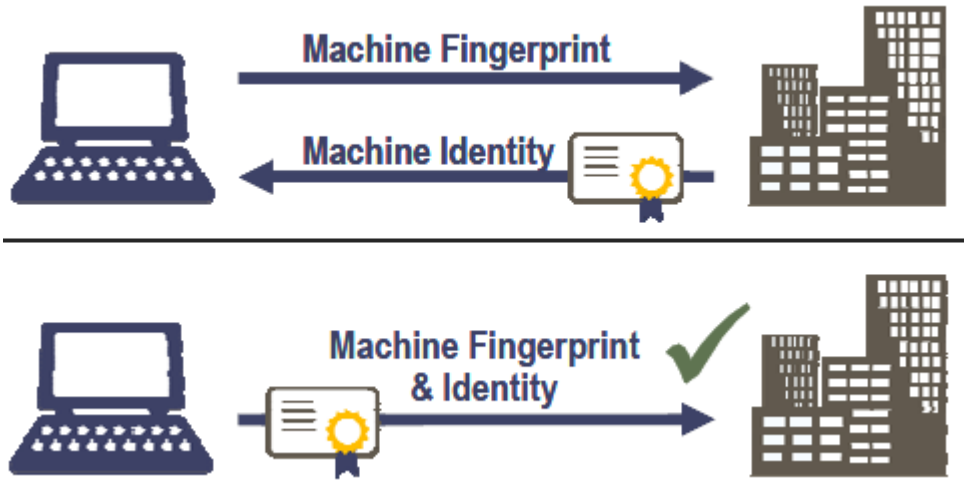
- *Jednoduché a levné nasazení* je zvlášť v dobách finanční krize velice podstatným kritériem. Při vývoji nové metody ověřování identity je tedy třeba myslet na to, že bude třeba ji poskytnout milionům zákazníků. Měla by také zapadnout do existující infrastruktury.

4.2 Úrovňové ověřování identity

K uživatelskému heslu je tedy přidána další úroveň zabezpečení. Heslo je první úrovní, je to něco, co uživatel zná. Další úrovní je něco, co uživatel má, nějaký fyzický faktor. Proto v případě, kdy někdo odcizí uživateli jeho heslo, kvůli absenci zmíněného fyzického faktoru mu přesto bude zabráněno v přístupu k účtu. Těmi fyzickými faktory mohou být:

[18] ENTRUST, Securing What's at Risk: A Common Sense Approach to Protecting Users Online; s. 5

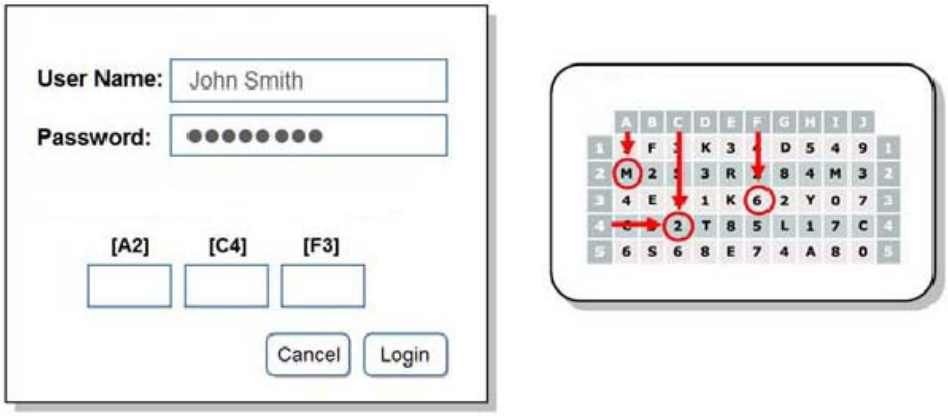
- *Stroj*, například počítač, který uživatel používá pro přístup ke svému účtu. K vytvoření identity uživatelova počítače vede jednoduchý postup. Nejprve je vytvořen otisk počítače, který je založen na jeho parametrech, jako jsou rozlišení obrazovky, rychlost procesoru, velikost operační paměti nebo třeba internetový prohlížeč, který uživatel nejčastěji používá. Tento otisk je bezpečně uložen. Na základě otisku je pak vytvořena identita počítače. Počítač je při každém přístupu ověřován na základě přidělené identity a otisku, který je porovnán s tím uloženým (viz Obrázek 17).[19]



Obrázek 17 - Ověření identity počítače[19]

- *Mřížka* v podobě souřadnicové sítě s náhodně vsazenými znaky může být dalším faktorem pro dodatečnou identifikaci. Každý uživatel dostane unikátní tabulku vytisknutou na kartě. Tyto tabulky je navíc možné periodicky vyměňovat, čímž se zamezí tomu, aby někdo, kdo odposlouchává komunikaci klienta s bankou, nezískal postupně všechny znaky v tabulce. V jednotlivých buňkách mohou být buď pouze číslice, pouze písmena, nebo kombinace obojího. Při přihlašování je pak uživatel kromě svého uživatelského jména a hesla dotazován navíc na znaky podle souřadnic (viz Obrázek 18). Například pokud budou požadovány souřadnice A2, C4 a F3, odpověď bude vypadat následovně:

[19] ENTRUST, Securing What's at Risk: A Common Sense Approach to Protecting Users Online; s. 6



Obrázek 18 - Ověření identity pomocí tabulky znaků[20]

- *Mobilní telefon* nebo podobný komunikační přístroj lze také použít pro dodatečné ověření identity. Je to velice efektivní prostředek zejména proti man-in-the-middle útokům. Nejčastěji jde o SMS s krátkým přehledem zadané transakce a náhodně generovaným potvrzovacím kódem.[20]

Další možností dodatečného ověření identity uživatele je přidělení certifikátu. Certifikáty bývají časově omezené a je žádoucí je uchovávat na externím paměťovém médiu, popřípadě na čipové kartě. Druhá možnost však pro koncového uživatele znamená dodatečný poplatek za vydání karty a pronájem čtečky čipových karet.

Obrázek 19 - PIN kalkulátor[20]

[20] ENTRUST, Securing What's at Risk: A Common Sense Approach to Protecting Users Online; s. 8

Poslední z běžně užívaných metod jsou PIN kalkulátory (viz Obrázek 19), které na základě nějakého algoritmu náhodně generují číselný kód, který uživatel zadá společně s uživatelským jménem a heslem.

Kromě přístupu do aplikací internetového bankovnictví je běžným prvkem ochrany také dodatečná autorizace transakcí. Běžně se používá ten samý postup, jako při vstupu do aplikace, tedy například ověření transakce certifikátem a uživatelským heslem. Navíc je možné využít jednorázový kód, který banka vygeneruje a zašle uživateli např. SMS zprávou. Tento kód má ve většině případů omezenou časovou platnost. Další možností je sada jednorázových autorizačních kódů (např. 50 kódu najednou), které uživatel zadává buď postupně, nebo je při autorizaci platby dotazován na kód s daným pořadovým číslem. Tuto sadu kódů uživatel nejčastěji dostane přímo na pobočce své banky.[21]

4.3 Ověřování identity u nás

V českých finančních institucích je internetové bankovnictví poměrně nový pojem, i přesto je ale úroveň jeho zabezpečení srovnatelná s úrovní zabezpečení v zemích s mnohem delší historií těchto služeb.

Nejběžnějším řešením ověřování identity uživatele při přihlášení do aplikace internetového bankovnictví je kombinace uživatelského certifikátu a uživatelského hesla. Tento způsob má velice dobrý poměr bezpečnosti a jednoduchosti použití. Zároveň není finančně náročný ani pro banky, ani pro jejich klienty.

Méně běžným, ale stále bohužel ještě používaným řešením je ne zcela bezpečná kombinace pouze uživatelského jména (čísla) a uživatelského hesla. Dnes bývá tento způsob přihlašování k aplikaci internetového bankovnictví doplněn ještě o SMS kód, což už je poměrně těžko překonatelná překážka v neautorizovaném přístupu.

Málo používané je i řešení kombinací klientského certifikátu na čipové kartě, který je chráněn přístupovým PIN kódem a uživatelského hesla. Je to způsobeno zřejmě tím, že čipové karty a často ani čtečky těchto karet, nejsou vydávány klientům zdarma. Tento způsob je však velmi bezpečný.

[21] KRHOVJÁK, J., LORENC, V., MATYÁŠ, V., Autentizace a autorizace finančních transakcí

Poslední dvě řešení jsou kombinací PIN kalkulátoru, respektive TAN kódu, s některým z předchozích způsobů ověřování. PIN kalkulátor je generátor hesel, který na základě atributů transakce vypočte autorizační kód. TAN kódy jsou jednorázové kódy. Klient si je může vyzvednout na pobočce, nebo jsou mu zaslány poštou. Jsou vydávány v sadách, nejčastěji po 50 nebo 100 kódech a po jejich vypotřebování klient obdrží kódy nové.

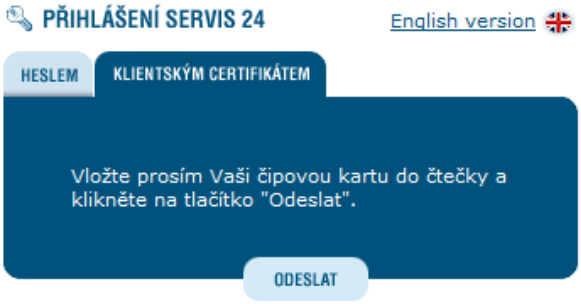
5. Porovnání systémů zabezpečení

V této kapitole uvedu vždy několik informací o bance samotné a následně popíšu příslušnou aplikaci internetového bankovnictví a její zabezpečení proti neoprávněnému přístupu.

5.1 Česká spořitelna

Česká spořitelná má přes 5 milionů klientů a je tedy největší bankou na českém trhu. Její služby internetového bankovnictví mají název SERVIS 24 (pro fyzické osoby) a BUSINESS 24 (pro právnické osoby) a ke dni 30. 9. 2010 měly 1 296 595 aktivních klientů.

V základním nastavení je přístup k internetovému bankovnictví České spořitelny zabezpečen pouze klientským číslem a heslem, která lze však zadat pomocí grafické klávesnice (viz Obrázek 21), což znesnadňuje odposlech. Tento způsob zabezpečení je přesto velmi slabý. Proto Česká spořitelna nabízí identifikaci pomocí klientského certifikátu (viz Obrázek 20). Toto řešení je však považováno za nadstandardní a je tedy zpoplatněno. Navíc jsou certifikáty vydávány pouze na čipových kartách, takže klient si musí od banky půjčit čtečku těchto karet.



Obrázek 21 - Česká spořitelna, přihlášení klientským certifikátem

Obrázek 20 - Česká spořitelna, přihlášení klientským číslem a heslem

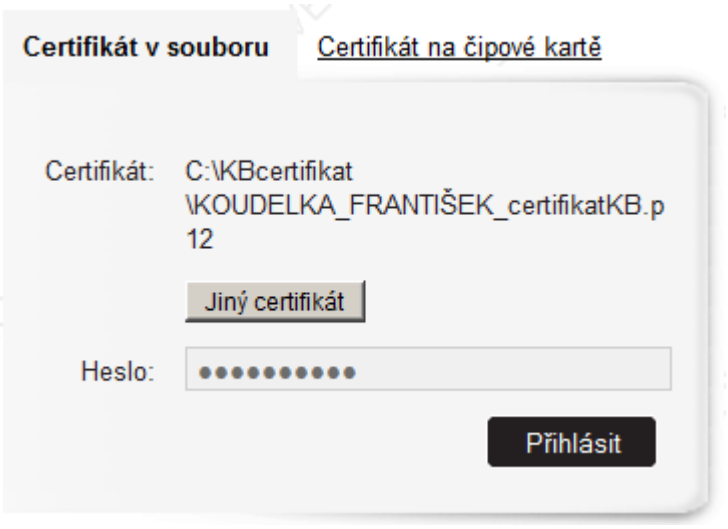
Aktivní transakce jsou však dodatečně autorizovány pomocí autorizačního SMS kódu nebo opět pomocí klientského certifikátu. Pokud tedy klient využívá pouze základní zabezpečení, hrozí sice, že se nějaká třetí osoba neoprávněně dostane k údajům na jeho účtu, je však velice nízká pravděpodobnost, že by mohl provést jakoukoliv aktivní transakci v případě, že nevlastní i klientův mobilní telefon.

Komunikace klienta s bankou je zabezpečena dnes běžným 128 bitovým šifrováním a hashovacím algoritmem SHA-1 pomocí protokolu TLS 1.0. Identita banky je navíc zaručena certifikátem serveru banky (ověřovatel VeriSign, Inc.), klientské certifikáty vydává První certifikační autorita a.s.

5.2 Komerční banka

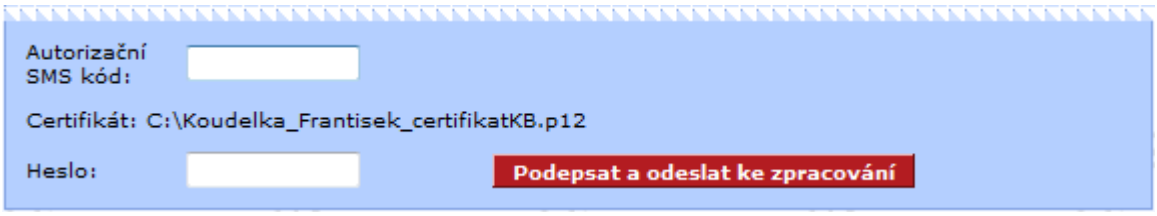
Komerční banka má necelé 2 miliony klientů a řadí se tedy mezi největší banky v České republice. Její služby internetového bankovnictví se jmenují Mojebanka (zejména pro fyzické osoby) a Profibanka (pro právnické osoby).

Komerční banka nabízí již v základním balíčku přihlášení pomocí uživatelského certifikátu. Ten si uživatel může zdarma stáhnout do svého počítače jako tzv. „certifikát v souboru“ (viz Obrázek 22), nebo za příplatek dostane čipovou kartu a půjčí si od banky čtečku (přihlašovací okno pak vypadá podobně, jako u České spořitelny).



Obrázek 22 - Komerční banka, přihlášení certifikátem v souboru

Aktivní transakce jsou v případě Komerční banky podepisovány digitálním podpisem, tj. za pomoci uživatelského certifikátu a hesla, dodatečný povinný autorizační prvek pro první aktivní transakci během jednoho přihlášení v aplikaci Mojebanka tvoří autorizační SMS kód (viz Obrázek 23).



Obrázek 23 - Komerční banka, autorizace platby

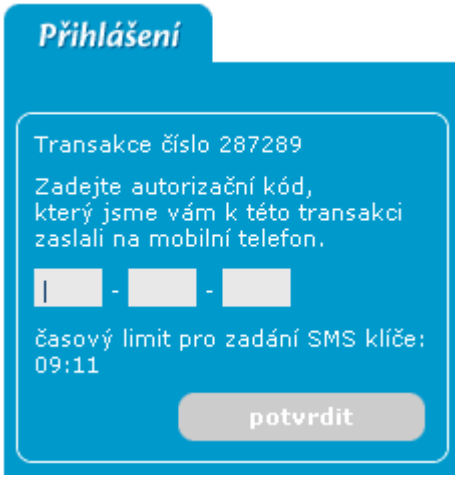
Komunikace klienta s bankou je zabezpečena silným 168 bitovým šifrováním a hashovacím algoritmem SHA-1 pomocí protokolu TLS 1.1. Identitu serveru banky zaručuje jeho certifikát (ověřovatel VeriSign, Inc.), klientské certifikáty vydává vlastní certifikační autorita Komerční banky.

5.3 ČSOB

Tato instituce patří se svými 3 miliony klientů mezi největší banky u nás. Její služby internetového bankovnictví InternetBanking 24 (primárně pro fyzické osoby) a BusinessBanking 24 (pro právnické osoby) a ostatní služby přímého bankovnictví využívá přes 2 miliony uživatelů.

ČSOB nabízí tři způsoby přihlášení do aplikace internetového bankovnictví. V případě prvního způsobu zadá klient své uživatelské číslo a heslo (podobně jako u České spořitelny), druhý způsob se liší pouze dodatečnou autorizační SMS s tzv. kódem transakce. Tento kód má časově omezenou platnost (viz Obrázek 24). Třetím způsobem přihlášení je opět čipová karta, která je stejně jako v předchozích případech za příplatek a klient si opět musí pronajmout čtečku těchto karet.

Aktivní transakce jsou opět autorizovaný SMS kódem, respektive digitálním podpisem pomocí certifikátu.



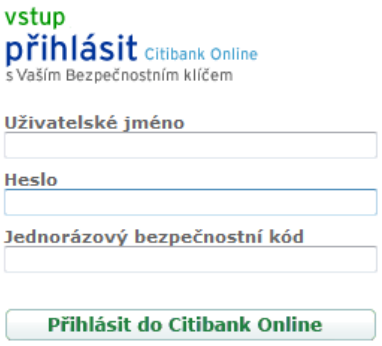
Obrázek 24 - ČSOB, "kód transakce" pro přihlášení

Komunikaci klienta s bankou chrání 128 bitové šifrování a hashovací algoritmus SHA-1 protokolu TLS 1.0. Identita serveru banky je potvrzena certifikátem (ověřovatel GlobalSign), klientské certifikáty vydává První certifikační autorita a.s.

5.4 Citibank

Citibank je součástí finanční skupiny City, která patří mezi největší svého druhu na světě. Její službu internetového bankovnictví Citibank Online údajně využívají všichni její klienti.

K ověření identity klienta používá Citibank uživatelské jméno, heslo a jednorázový bezpečnostní kód (viz Obrázek 25). Ten je generován tzv. Bezpečnostním klíčem, což je



Obrázek 25 - Citibank, jednorázový bezpečnostní kód pro přihlášení

autentizační kalkulátor. Jiný způsob ověření identity Citibank nepodporuje. Aktivní transakce je třeba autorizovat bezpečnostním kódem, který lze zadat pomocí grafické klávesnice.

Komunikace klienta s bankou je zakódována 128 bitovým šifrováním a hashovacím algoritmem SHA-1 podle protokolu TLS 1.0. Identitu banky ověřuje certifikát (ověřovatel VeriSign, Inc.).

5.5 eBanka

Tento peněžní ústav byl na českém trhu jedním z prvních, když v roce 1998 zavedl pro své klienty služby homebankingu. Původním záměrem bylo vybudování především elektronické banky, tento plán však nepřinesl očekávaný úspěch a banka byla v roce 2006 prodána skupině Raiffeisen. Název aplikace internetového bankovnictví eKonto však zůstal zachován.

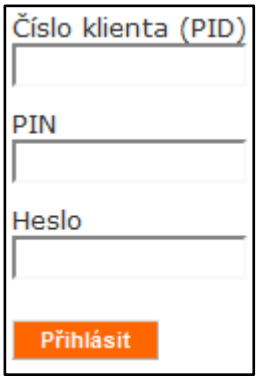
eKonto nabízí tři způsoby ověření identity klienta. První se jmenuje „Mobilní klíč“ a spočívá v autentizaci pomocí klientského čísla a tzv. „certifikačního kódu“ zaslaného prostřednictvím SMS. I přesto, že jde jen o dva prvky ochrany, je to bezpečné řešení díky SIM Toolkitu, který umožňuje přijímání šifrovaných SMS. Druhý způsob s názvem „Osobní klíč“ kombinuje klientské číslo s tzv. „osobním elektronickým klíčem“, což je kalkulátor autorizačních kódů. Tento kód je navíc vygenerován až po zadání PIN. Třetí způsob, nazvaný „Internetový klíč“, kombinuje klientské číslo s osobním certifikátem a heslem. Použitím tří ochranných prvků jde o nejbezpečnější řešení, Raiffeisenbank však již novým klientům osobní certifikáty nevydává. Autorizace plateb probíhá pomocí autorizačního SMS kódu.

Komunikační kanál mezi klientem a bankou zabezpečuje 256 bitové šifrování a hashovaní algoritmus SHA-1 protokolu TLS 1.1. Server banky je ověřen certifikátem (ověřovatel VeriSign, Inc.).

5.6 ING Bank

Nejznámějším produktem skupiny ING je na našem území ING Konto. Není to klasický běžný účet, jde o účet spořící. Přesto jsem ho do tohoto porovnání zařadil, protože nabízí zajímavé řešení zabezpečení.

Pro přístup do ING Konta je vyžadována znalost tří parametrů (viz Obrázek 26). Jsou to klientské číslo, PIN a heslo. Toto řešení nenabízí nijak nadprůměrné zabezpečení přístupu k účtu, avšak transakce jsou povoleny pouze na další účty v rámci ING (např. fondy, pojištění) a na předem definované, ve smlouvě uvedené transakční účty jiných bank.



Obrázek 26 - ING Konto, přihlášení

Data, přenášená mezi klientem a bankou, jsou zašifrována podle 168 bitového klíče a SHA-1 hashovacího algoritmu pomocí protokolu TLS 1.0. Server banky má udělený certifikát od ověřovatele VeriSign, Inc.

5.7 mBank

Tato banka přišla na český trh koncem roku 2007 z Polska. Jde o čistě internetovou banku, která patří v této oblasti mezi největší na světě. I přes rostoucí konkurenci stále zůstává leaderem v oblasti internetového bankovnictví.

Při přihlašování do aplikace mKonto je po uživateli požadováno pouze identifikační číslo klienta a heslo, čímž se tato služba řadí vedle SERVIS 24 České spořitelny mezi méně bezpečné. Stejně jako SERVIS 24 i mKonto používá pro autorizaci plateb autorizační SMS kód.

Přenos dat je opět šifrován 168 bitovým klíčem a SHA-1 hashovacím algoritmem protokolu TLS 1.0. Identita banky je ověřena od VeriSign, Inc.

5.8 Přehled

Pro snazší porovnání výše uvedených řešení ověřování identity uživatelů internetového bankovnictví (viz Tabulka 2) a způsobů autorizace plateb (viz Tabulka 3) uvádím stručný přehled v následujících tabulkách.

OVĚŘENÍ IDENTITY KLIENTA					
	Uživatelské jméno a heslo	Certifikát	Certifikát na čipové kartě	SMS kód	PIN kalkulátor
5.1 Česká spořitelna	●	—	●*	—	—
5.2 Komerční banka	—	●	●*	—	—
5.3 ČSOB	●	—	●*	●	—
5.4 Citibank	●	—	—	—	●*
5.5 eBanka	●	●*	—	●*	●*
5.6 ING Bank	●	—	—	—	—
5.7 mBank	●	—	—	—	—
* zpoplatněno					

Tabulka 2 - Ověření identity klienta, porovnání

AUTORIZACE TRANSAKCÍ				
	SMS kód	Certifikát	Certifikát na čipové kartě	PIN kalkulátor
5.1 Česká spořitelna	●	—	●*	—
5.2 Komerční banka	●	●	●*	—
5.3 ČSOB	●	—	●*	—
5.4 Citibank	—	—	—	●*
5.5 eBanka	●	●*	—	●*
5.6 ING Bank	—	—	—	—
5.7 mBank	●	—	—	—
* zpoplatněno				

Tabulka 3 - Autorizace transakcí, porovnání

6. Závěr

Vzhledem k neochotě několika bankovních institucí, zejména jejich pracovníků, bylo velice obtížné dohledat potřebné informace o zabezpečení některých aplikací internetového bankovnictví, abych je pak mohl porovnat a tím splnit cíl mé práce. Světlou výjimku tvoří Komerční banka, jejíž ředitel bezpečnosti mi zprostředkoval kontakt na jednoho z pracovníků jeho oddělení, který mi na osobní schůzce nejen zodpověděl mé otázky (viz 8.1 Dotazník), ale dostalo se mi od něj i mnoha užitečných rad.

Z předchozí kapitoly by měly být zřejmé klady i zápory jednotlivých u nás používaných modelů zabezpečení aplikací internetového bankovnictví proti zneužití třetí osobou. Dle mého nejslabší zabezpečení má mBank, jejíž použití pouze klientského čísla a hesla jako zabezpečovacích prvků by mi přišlo naprosto nedostačující a bylo by zřejmě zásadním argumentem pro vyhledání služeb jiné banky. Naopak nejsilnější mi přijde zabezpečení použitím klientského certifikátu uloženého na čipové kartě, respektive použití PIN kalkulátoru. Jejich vydání je však všemi výše zmíněnými bankami zpoplatněno, což je pro mě, jakožto studenta bez stálého příjmu, nepřípustné řešení. Osobně používám internetové bankovnictví Komerční banky, jíž jsem klientem. Můj názor ohledně zabezpečení její aplikace internetového bankovnictví tedy může být považován za silně subjektivní. Použití tzv. „certifikátu v souboru“, který banka vydává zdarma, v kombinaci s heslem mi však přijde naprosto dostačující. Pokud bych navíc dbal doporučení banky a měl certifikát uložený pouze na externím paměťovém médiu, věřím, že pravděpodobnost napadení mého účtu by se blížila nule.

Při pokusu objektivně vybrat nejlépe zabezpečenou aplikaci internetového bankovnictví mi přišlo celkem logické zvolit aplikaci eBanky, která má dle mého názoru u nás nejdelší zkušenost v této oblasti. A pokud je klient ochotný si za bezpečí svých peněz připlatit, jsou veškeré informace o jeho účtu téměř nedotknutelné.

7. Seznam použitých zdrojů

BARRET, Daniel J., SILVERMAN, Richard. SSH, The Secure Shell: The Definitive Guide. 1. vydání. O'Reilley, 2001. 558 s. ISBN 0-596-00011-1

MENEZES, Alfred J., VAN OORSCHOT, Paul C., VANSTONE, Scott A.. Handbook of Applied Cryptography. 5. vydání. CRC Press, 2001. 816 s. ISBN 0-8493-8523-7

OPPLIGER, Rolf. SSL and TLS: Theory and Practice. 1. vydání. Artech House, 2009. 284 s. ISBN 978-1-59693-447-4

Internetové zdroje:

DE CLERCQ, Jan. Understanding and Leveraging SSL-TLS for Secure Communications [online]. [cit. 2011-03-25]. Dostupný z WWW: <http://www.windowsitpro.com/resource/understanding-and-leveraging-ssltls-for-secure-communications.aspx >

ENTRUST. Securing What's at Risk: A Common Sense Approach to Protecting Users Online [on-line]. [cit. 2011-03-25]. Dostupný z WWW: <http://entrust.com/resources/download.cfm/22313/>

KRHOVÁK, Jan, LORENC, Václav, MATYÁŠ, Václav. Autentizace a autorizace finančních transakcí [on-line]. Brno: Zpravodaj ÚVT MU, 2007 [cit. 2011-03-25]. Dostupný z WWW: <http://ics.muni.cz/zpravodaj/articles/561.html>

Phishing Attacs on the rise [on-line]. 2010 [cit. 2011-03-25]. Dostupný z WWW: <http://www.racknine.com/blog/software/phishing-attacks-on-the-rise/>

8. Přílohy

8.1 Dotazník

Ověření identity banky

SSL/TLS? Verze:

Certifikační autorita:

Šifrování dat

Délka šifrovacího klíče:

Webový prohlížeč

Doporučený webový prohlížeč:

Autentizace klienta

Uživatelské jméno a heslo: ANO/NE

Certifikát: ANO/NE

Čipová karta: ANO/NE

SMS kód: ANO/NE

PIN kalkulátor: ANO/NE

Minimální délka hesla:

Autorizace platby

Certifikát: ANO/NE

Čipová karta: ANO/NE

SMS kód: ANO/NE

PIN kalkulátor: ANO/NE

Nadstandardní zabezpečení:

8.2 Seznam obrázků

8.3 Seznam tabulek