

2/4 NOVÉ ZPŮSOBY JAK PORAZIT SSL - SSLSTRIP

SSL neboli Secure Socket Layer je protokol, resp. vrstva vložená mezi vrstvu transportní (např. TCP/IP) a aplikační (např. HTTP), která poskytuje zabezpečení komunikace šifrováním a autentizací komunikujících stran. Běžně jej využívá každý, např. v rámci internet bankingu. Ze SSL se stala fráze, která je běžným uživatelům webových služeb opakována tak často, že si začnou myslet, že je to pravda. Konečně, příkladů je více než dost, pro ukázkou vyjádření dvou velmi známých bank v ČR.

„Bezpečnost komunikace s bankou přes internet: Pro základní bezpečnost Vašich příkazů musí být zajištěno, aby příkaz k bankovní operaci nebyl nikým modifikován. K tomuto účelu je použito silné 128bitové šifrování komunikace s bankou po internetu pomocí technologie SSL. Pro navázání šifrované komunikace je navíc použit certifikát serveru banky vydaný důvěryhodnou certifikační autoritou, který zajistí, že

Protokol SSL

SSL v tiskových prohlášeních

skutečně komunikujete s bankou a ne s někým, kdo se za aplikaci internetového bankovníctví pouze vydává.“

*„Pro zajištění bezpečnosti vybudovala banka certifikační autoritu a využila svou infrastrukturu veřejných klíčů (PKI). ... **Veškerá komunikace probíhá v SSL (Secure Socket Layer) a ... Tím jsou uspokojeny veškeré požadavky na bezpečnou komunikaci, tj. identifikaci, autentikaci, autorizaci, důvěrnost, integritu a nepopíratelnost.“***

Podobná vyjádření jsou samozřejmě silným zjednodušením reálné skutečnosti, ale přiznejme si, že je to stále víc, než ví 90 % obyvatel ČR, resp. kteréhokoliv rozvinutého státu na světě.

Bezpečnost není černobílá

Na SSL, tedy obecně na problematiku šifrování komunikace, je potřeba pohlížet z více směrů. V pozitivním slova smyslu je jejím cílem zajistit, aby data putovala v zabezpečeném kanálu, nešla tak čist cizím subjektem, natož provádět nepozorované modifikace. Bezpečnost je ale složitá soustava, kde věci nejsou bílé a černé. Jde třeba o to, jestli šifrovaná data neobsahují něco nebezpečného. Nemyslím teď jen zájem většiny vlád a silových složek čist a odposlouchávat libovolnou komunikaci na světě a vše odůvodňovat hrozbou terorismu. Mnohem častěji jde o nevhodné použití této technologie, zejména včasné ukončení SSL komunikace. Je dost nebezpečné to dělat až na straně aplikačního serveru. Máte IDS? Aplikační firewally? V tuto chvíli jsou vám k ničemu. Tento příklad uvádím pouze proto, aby bylo jasnější, že šifrování je v mnoha případech hezká idea, která bývá nevhodně přenesena do elektronického světa.

V rámci dalšího uvažování o nových hrozbách pomí-
neme ty staré. Tedy např. to, že SSL je jen rámec, který
využívá různé šifrovací algoritmy, různé délky klíčů
atd. Takže lze používat SSL, kde bude využít např.
DES a 40bitový klíč. To určitě není dobře. Ne kvůli
SSL, ale kvůli DES, který je již několik let považován
za „mrtvý“. Útoky, které budeme dále rozebírat, po-
čítají s tím, že si server s klientem pokusí domluvit to
nejlepší dostupné šifrování a nejdelší možný klíč. Dále
pro upřesnění budeme předpokládat, že většinu tech-
nik nelze používat bez kombinace s jinými a že každý
útok musí být zařazen do nějakého prostředí. V našem
případě se tedy zaměříme na útoky, které využívají
MITM - Man In The Middle techniky. Ty nejjedno-
dušší mohou být na LAN síti, zejména ARP spoofing,
případně na WIFI. Ale nelze zcela ztratovat ani kom-
binace, kdy útočník navede svou oběť např. kvůli pře-
klepu URL na svou stránku. Např. paypal.com je le-
gitimní stránka, ale paypall.com nebo paypal.com jen
počítají s tím, že uživatel nezná dobře anglický jazyk
nabo může přehlédnout dvě podobně vypadající pís-
mena.

Nyní krátký exkurz do historie. Protože je SSL tak
často více méně marketingovým způsobem zneuží-
váno, bylo a je terčem zájmu bezpečnostních specia-
listů i hackerů. Příkladů je více, ale blíže probereme
pouze použití programu Ettercap.¹ Jedná se o víceúče-
lový nástroj na sniffing síťového provozu, doplněný
o techniky vybrané techniky MITM, včetně arpspoof.²
Jeho první verze umožňovaly podvrhávat statický cer-
tifikát, který na uživatele asi nepůsobil moc důvěry-
hodně. Vše bylo statické - jméno certifikační autority,

**Podmínky
realizace dále
popisovaných
útoků**

**První verze
MITM proti SSL -
statická forma**

¹ Autoři Alberto Ormighi a Marco Valleri.

² Vlastní technika je blíže popsána v kapitole o hackingu.

jméno webové stránky, divný čas atd. I na něj ale mnoho lidí kliklo.



Druhá verze MITM proti SSL - dynamická forma

V dalších verzích Ettercap se tato funkcionality o dost změnila. Výsledkem byla „celkem slušná kopie“, kdy se „on the fly“, tedy průběžně, zkopíroval původní certifikát, ale místo „hrátek“ s MD5 kolizí se jen zfalšoval tzv. fingerprint. Výsledek byl velmi elegantní a výrazně se zvětšilo procento uživatelů, kteří nakonec klikli na „ano“ a dodanému certifikátu začali důvěřovat. Originál se samozřejmě liší, ale podvržený certifikát má v pořádku jméno organizace, certifikační autoritu, platnost. Jen na začátku je uvedeno „Certifikát nemohl být z neznámeného důvodu ověřen“, místo „Tento certifikát byl ověřen pro následující použití“. Použitý mechanismus je blíže popsán v manuálu programu Ettercap.

Rozdíl v certifikátech pouze v poli „Otisky“



Prohlížeč certifikátů: "www.ingkonto.cz"

Obecně | Detaily

Certifikát nemohl být z neznámého důvodu ověřen.

Vydáno pro

Obecné jméno (CN)	www.ingkonto.cz
Organizace (O)	ING Bank N.V., organizační složka
Jednotka organizace (OU)	.
Sériové číslo	5A:46:E1:A3:0B:81:28:FC:55:19:C9:C0:27:6D:B4:96

Vydal

Obecné jméno (CN)	<není součástí certifikátu>
Organizace (O)	VeriSign Trust Network
Jednotka organizace (OU)	VeriSign, Inc.

Platnost

Vydáno dne	26.3.2008
Platný do	3.4.2011

Otisky

Otisk SHA1	80:C4:EA:D9:6E:A6:C7:9B:DD:DC:11:46:FF:55:1D:42:45:8C:ED:87
Otisk MD5	D2:7F:41:DE:01:6A:69:3F:95:71:A2:6F:F7:E0:69:EA

Prohlížeč certifikátů: "www.ingkonto.cz"

Obecně | Detaily

Tento certifikát byl ověřen pro následující použití:

Certifikát SSL serveru
Server SSL s krokováním

Vydáno pro

Obecné jméno (CN)	www.ingkonto.cz
Organizace (O)	ING Bank N.V., organizační složka
Jednotka organizace (OU)	.
Sériové číslo	5A:46:E1:A3:0B:81:28:FC:55:19:C9:C0:27:6D:B4:96

Vydal

Obecné jméno (CN)	<není součástí certifikátu>
Organizace (O)	VeriSign Trust Network
Jednotka organizace (OU)	VeriSign, Inc.

Platnost

Vydáno dne	26.3.2008
Platný do	3.4.2011

Otisky

Otisk SHA1	32:3D:2B:09:85:50:C3:D1:AA:E3:7C:04:52:C5:99:15:4C:B1:70:F4
Otisk MD5	48:35:C5:CF:F1:02:FD:BF:9F:69:F5:39:13:EE:B1:F1

díl 4, Nové způsoby jak porazit SSL - SSLSTRIP

V případě, že uživatel neodolal a kliknul - vždyť on(a) se skutečně potřebuje přihlásit do banky, hacker už mohl v klidu sledovat, jak mu oběť sděluje své jméno a heslo.



Viditelná hesla v případě MITM proti SSL v programu Ettercap

ettermcap NG-0.7.3

Start Targets Hosts View Mitm Filters Logging Plugins Help

Targets Connections

	Host	Port	-	Host	Port	Proto	State	Bytes
	192.168.1.136	2899	-	195.39.69.111	80	T	closed	56273
	192.168.1.136	2900	-	195.39.69.111	80	T	closed	8271
	192.168.1.136	2901	-	195.39.69.111	80	T	closed	9268
	192.168.1.136	2902	-	195.39.69.111	80	T	closed	5589
	192.168.1.136	2903	-	195.39.69.111	80	T	closed	10445
	192.168.1.136	2904	-	195.39.69.111	80	T	closed	5085
	192.168.1.136	2840	-	74.125.43.102	80	T	closed	2224
	192.168.1.136	7210	-	217.66.161.4	5060	U	idle	2214
	192.168.1.136	2905	-	192.168.1.1	53	U	idle	430
	192.168.1.136	51848	-	192.168.1.1	53	U	idle	158
M	192.168.1.136	2906	-	193.33.126.71	443	T	opening	0
M	192.168.1.136	2907	-	193.33.126.71	443	T	opening	0
M	192.168.1.136	2908	-	193.33.126.71	443	T	opening	0
M	192.168.1.136	2909	-	193.33.126.71	443	T	opening	0
M	192.168.1.136	2910	-	193.33.126.71	443	T	idle	42734
M	192.168.1.136	2911	-	193.33.126.71	443	T	idle	16400
M	192.168.1.136	2912	-	193.33.126.71	443	T	idle	6494
*	192.168.1.136	2913	-	193.33.126.71	443	T	idle	14838

View Details Kill Connection

ARP poisoning victims:

GROUP 1 : 192.168.1.136 00:13:20:85:25:51

GROUP 2 : 192.168.1.1 00:1B:FC:57:AE:DE

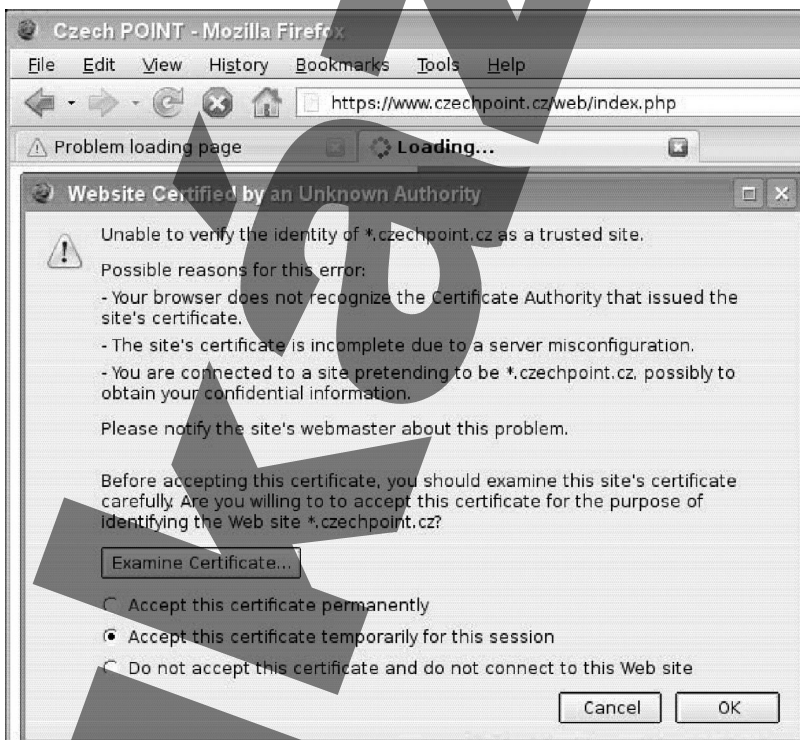
HTTP : 193.33.126.71:443 -> USER: 1111 PASS: 1111 INFO: https://www.ingkonto.cz/ib4/welcome.do

Demonstrovaný útok fungoval téměř ideálně, dokud se nezačalo pomalu měnit zabezpečení webových prohlížečů. Boj se zlozvyky je vcelku složitý, ale zde stačilo poměrně málo - změnit pozitivní model vyhodnocení SSL certifikátu za negativní. V čem je hlavní rozdíl? Je téměř jisté, že i když uživatel vidí výjimku, je zvyklý klikat na „OK“ nebo „Ano“.

**Změna
pozitivního
modelu
za negativní -
webové prohlížeče**

Je to rozdíl mezi Firefox 2 a Firefox 3 nebo IE6 a IE7. Pro lepší názornost je uveden příklad státní instituce, která má bezpečnou komunikaci téměř v popisu práce.

Neznámý certifikát a pozitivní model



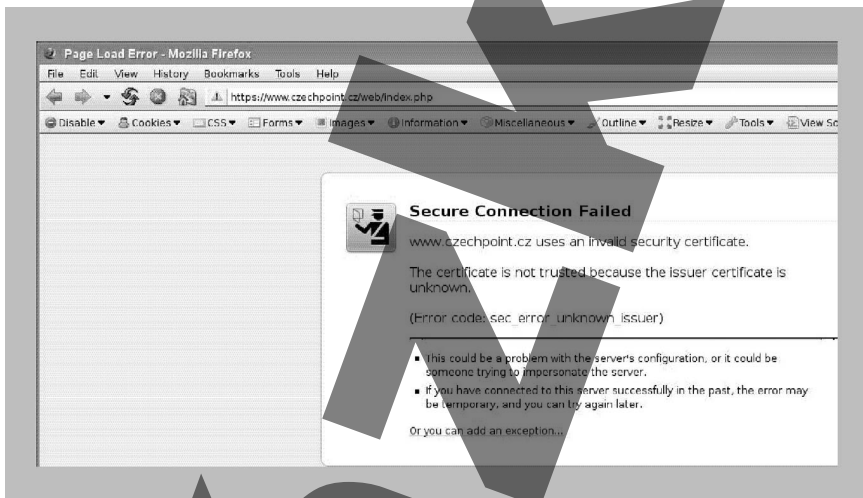
díl 4, *Nové způsoby jak porazit SSL - SSLSTRIP*

Reakce na certifikát podepsaný neznámou certifikační autoritou. Kdo by neznal PostSignum Public CA. Potvrdit výše uvedené ve FF2 šlo velmi snadno.



Reakce FF3 na stejnou stránku je naprosto rozdílná.

Neznámý certifikát a negativní model



Velmi se to podobá známému „na stránce vznikla chyba, prosím, obraťte se na svého administrátora“. Při používání pozitivního modelu byl uživatel sice varován, ale potřeboval přesně jeden klik, aby problém „vyřešil“. V případě negativního modelu potřebuje pokračovat v dalších krocích:

- 1) Kliknout na odkaz „Or you can add an exception“ nebo jeho jazykový ekvivalent.
- 2) Znovu kliknout na tlačítko „Add Exception“ (a možná si přečíst ještě jednou varování, co se vlastně děje).
- 3) Kliknout na další tlačítko „Get Certificate“ (stále není konec).
- 4) Teprve teď, když přeskočí možnost prohlédnout certifikát v detailu, může akceptovat výjimku (trvale nebo dočasně).

4 kliknutí navíc

4 je více než 1. Jednoduchá logika a z pohledu bezpečnosti vcelku účinná, i když to někteří uživatelé nemusí chápat.



Secure Connection Failed

www.czechpoint.cz uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.

(Error code: sec_error_unknown_issuer)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

You should not add an exception if you are using an internet connection that you do not trust completely or if you are not used to seeing a warning for this server.

[Get me out of here!](#)

[Add Exception...](#)



Neznámý certifikát a negativní model - pokračování



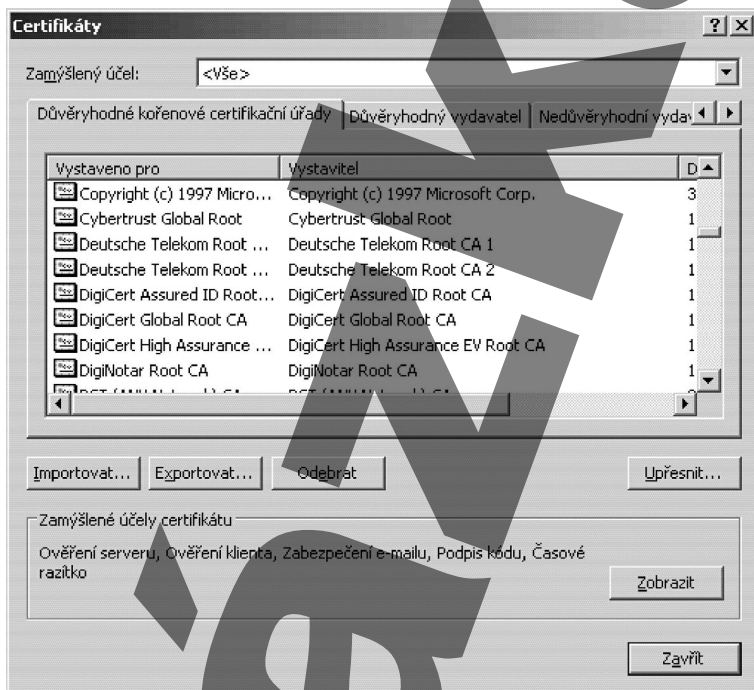
Způsob, jakým se přidávají výjimky do seznamu důvěryhodných certifikátů, není jediným způsobem, jakým se snaží výrobci prohlížečů upozorňovat uživatele, zda-li jsou nebo nejsou na zabezpečené stránce, např. žluté (Mozilla Firefox 2) nebo červené (Internet Explorer 7) zbarvení URL cesty; nebo také bílé (Mozilla Firefox 3 už zase barevný není).

Konečně se dostáváme k avizované novince, tedy dalšímu, způsobu, jak vyzrát nad SSL. Dosavadní starý svět důvěry v bezpečnost a použití SSL „skončil“ zhruba v únoru 2009, kdy na BlackHat DC 2009 prezentoval Moxie Marlinspike svůj v podstatě jednoduchý nápad. Proč bojovat s HTTPS, když to jde i bez něj.

Studoval hlouběji používání SSL certifikátů a jejich řetězení. Běžnou odpovědí na otázku „proč a kdy považuje internetový prohlížeč SSL certifikát za důvěryhodný?“ je, že se snaží vyhodnotit vybrané prvky certifikátu, jako např. název organizace a domény. Dále kontroluje pravost podpisu a platnost certifikátu. Nakonec ověřuje skutečnost, jestli zná certifikační autoritu, která certifikát vydala. Když ji má v interním seznamu, ověření končí, protože důvěryhodnost certifikátu serveru se rovná důvěryhodnosti certifikátu CA. Když nemá, jde po řetězci jednotlivých CA tak dlouho, dokud nenajde „kořen“. Jedna zajímavá věc, která ale nemá s tímto útokem nic společného - už jste se někdy dívali na seznam CA, která vám dodává výrobce prohlížeče a kterým tedy „musíte“ důvěřovat? Jsou jich desítky, možná stovky, závisí na použitém prohlížeči.

Podstata techniky SSLSTRIP

Kdy je vlastně certifikát důvěryhodný?

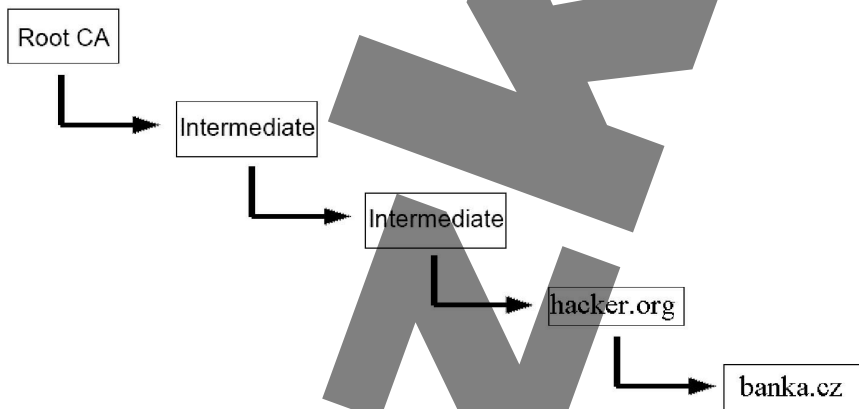


Kdo rozhoduje za nás?

Nemám nic proti Deutsche Telekom, ale Telefonice O2 nebo jiným operátorům také nedůvěřuji, tak proč za mě Microsoft rozhodl, že zrovna tento ano?

V čem je tedy uvedený příklad ověřování platnosti, resp. důvěryhodnosti špatný? Zaměřuje se jen na ověření podpisu a podmínkou je, aby byl „řetěz ověřování“ kompletní. Je to jeden z příkladů, jak špatně může dopadnout implementace matematicky velmi silného PKI do reálného světa. Co se stane, když se řetěz pro ověřování malinko prodlouží?

Řetězení certifikátů - naivní model pro ověření důvěryhodnosti

S

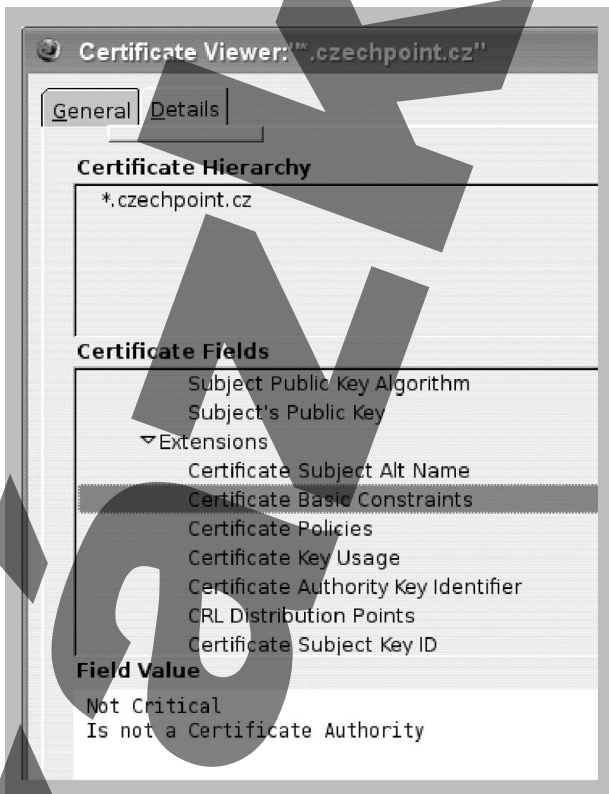
Nestane se vůbec nic. Vždyť přece platí, že:

- 1) všechny podpisy jsou platné,
- 2) certifikát není expirovaný,
- 3) posloupnost řetězce je netknutá,
- 4) kořenová CA je v seznamu nainportovaných certifikátů prohlížeče.

Jenže rozdíl je, že hacker.org právě vytvořil platný certifikát pro banka.cz - přitom není banka.cz. Kde se stala chyba? Většina autorit neřeší nastavování příznaku „basicConstraints: CA=FALSE“, resp. v grafickém zázornění.



Co dokáže jedno „bezvýznamné“ pole v X.509 certifikátu



Totéž platí pro většinu prohlížečů. IE, Firefox, Opera, Konqueror a další toto pole a jeho hodnotu prostě neřeší. Každý tak může vytvořit certifikát pro libovolnou další doménu.

Sázka na lidské chování

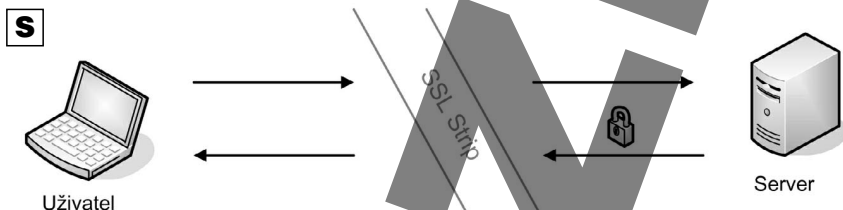
Výše uvedený autor tedy přišel s nástrojem, který je známý jako SSLSTRIP, aby uvedenou zranitelnost demonstroval. Při jeho použití se navíc vychází z jedné mnohokrát ověřené pravdy. Kdy jste naposledy napsali

přímo do URL? Většina uživatelů internetu prostě jde na správnou doménu, která je implicitně publikována pomocí HTTP (tedy nešifrovaná) a odtud teprve pomocí tlačítka nebo odkazu „bezpečný vstup na účet“ nebo podobně přechází na zabezpečenou verzi. Případně počítá s tím, že dojde k automatickému přesměrování (známé HTTP kód 302). Většina stránek je napsána tak, že najetím na tlačítko není vidět správný odkaz na URL. Kód může být v AJAX nebo jiném rozšíření, které je dnes běžné. Uživatel tedy nemůže vědět, resp. vidět, kam jde. Na druhou stranu, i když je odkaz zobrazován, je to téměř nepodstatné, protože jej většina uživatelů stejně nesleduje.



Jak SSLSTRIP pracuje?

Jak SSLSTRIP funguje? Jedná se o transparentní HTTP proxy. V případě, že zachytí pokus o HTTPS komunikaci, nahradí směrem k uživateli HTTPS za HTTP, ale se serverem dále komunikuje pomocí HTTPS - tam to ani jinak nejde. Výsledkem je, že server nemůže rozpoznat rozdíl a uživatel pouze nevidí v URL cestě jedno písmenko.



Jak to vypadá ve skutečnosti? Konfigurace je jednoduchá - manuál k programu to shrnuje ve 4 bodech (návod je jen pro Linux):

- 1) Povolte forwarding:


```
echo „1“ > /proc/sys/net/ipv4/ip_forward
```
- 2) Nastavte si pravidla na iptables firewallu - všechny HTTP provoz bude přesměrován na zvolený port (default TCP/10000):


```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port <yourListen-Port>
```
- 3) Spustíte SSLSTRIP s možnostmi, jaké chcete:
- 4) Začnete provádět MITM - arpspoof:


```
arpspoof -i <yourNetworkDevice> -t <yourTarget> <theRoutersIpAddress>
```


Za příklad jsem vybral SERVIS24 České spořitelny, ale nezáleží na tom - SSL si nevybírám. Je to jako hádanka pro děti, s tím rozdílem, že není 5, ale jen jeden rozdíl.

Když chybí jedno písmenko

Příklad jedné z českých bank - správně

PŘIHLÁŠENÍ SERVIS 24 English version

HEBLEM KLIENŤSKÝM CERTIFIKÁTEM KALKULÁTOREM

Klientské číslo

Heslo

ODESLAT

V přihlašovacím dialogu vyplíte, prosím, své klientské číslo služby SERVIS 24 a heslo internetového bankovníctví (případně aktuální heslo pro službu Telebanking). Po řádném zadání přihlasovacích údajů klikněte na tlačítko **Odeslat** pro vstup do aplikace internetového bankovníctví. K prvnímu přihlášení potřebujete znát také **bezpečnostní kód**. Bez tohoto čísla by Vaše první přihlášení nebylo úspěšné.

Bezpečnostní upozornění

Rádi bychom Vás upozornili na rizika spojená s používáním nezabezpečeného počítače k přístupu do aplikace SERVIS 24 Internetbanking. Věnujte prosím pozornost následujícím radám.

- Používejte legální a aktualizovaný operační systém, aktuální antivirový program, antispyware a personální firewall.
- Věnujte zabezpečení Internetbankingu alespoň takovou pozornost, jako věnujete zabezpečení svého bydlení, auta a jiného majetku.
- Neotvírejte e-mailové zprávy od odesílatelů, které neznáte nebo zprávy s podezřelým názvem či obsahem.
- Nesdílujte osobní údaje, hesla či kódy PIN formou e-mailu. Česká spořitelna od klientů nebude nikdy údaje touto formou požadovat! Nikdy nezasiíláme nevyžádané e-maily s odkazy na internetové adresy.

Máte problémy s přihlášením?
 Použití čipové karty
 Bezpečnostní zásady klienta

[Přihlášení do správce certifikátů](#)
[Stránky České spořitelny](#)
[Informace o službě SERVIS 24](#)
[Dáma verze služby SERVIS 24 Internetbanking](#)

Hotovo www.servis24.cz

díl 4, Nové způsoby jak porazit SSL - SSLSTRIP

Příklad jedné z českých bank - špatně

SERVIS 24 Internetbanking - České spořitelna - Přihlášení - Mozilla Firefox

http://www.servis24.cz/jobankling-24/jdspatcher?aid=19991999

Česká spořitelna - Nejověřivější banka... -24 SERVIS 24 Internetbanking - Čes...

LINKA SERVIS 24 844 11 11 44

726 11 11 44 (Telefonická OZ)
605 66 11 44 (T-Mobile)
776 99 11 44 (Vodafone)

SERVIS 24
INTERNETBANKING

ČESKÁ SPOŘITELNA

PŘIHLÁŠENÍ SERVIS 24 English version

HESLEM KLIENSKÝM CERTIFIKÁTEM KALKULÁTOREM

Klientské číslo
Heslo

ODESLAT

1 2 3 4 5 6 7 8 9 0 - = << >>
q w e r t y u i o p | | \
Lock a s d f g h j k l ; ' /
Shift z x c v b n m , . / Shift

[Máte problémy s přihlášením?](#)
[Použití čipové karty](#)
[Bezpečnostní zásady klienta](#)

» [Přihlášení do správy certifikátu](#)
» [Stránky České spořitelny](#)
» [Informace o službě SERVIS 24](#)
» [Demo verze služby SERVIS 24 Internetbanking](#)

Hotovo

V přihlašovacím dialogu vyplňte, prosím, své **klientské číslo** služby SERVIS 24 a **heslo** internetového bankovníctví (případně aktuální heslo pro službu Telebanking). Po řádném zadání přihlašovacích údajů klikněte na tlačítko **Odeslat** pro vstup do aplikace internetového bankovníctví. K prvnímu přihlášení potřebujete znát také **bezpečnostní kód**. Bez tohoto čísla by Vaše první přihlášení nemlo úspěšné.

Bezpečnostní upozornění

Rádi bychom Vás upozornili na rizika spojená s používáním nezabezpečeného počítače k přístupu do aplikace SERVIS 24 Internetbanking. Věnujte prosím pozornost následujícím radám.

- Používejte legální a aktualizovaný operační systém, aktuální antivirový program, antispyware a personální firewall.
- Věnujte zabezpečení Internetbankingu alespoň takovou pozornost, jako věnujete zabezpečení svého bydlení, auta a jiného majetku.
- Neotvírejte e-mailové zprávy od odesílateřů, které neznáte nebo zprávy s podezřelým názvem či obsahem.
- **Nesdělte** osobní údaje, hesla či kódy PIN formou e-mailu. Česká spořitelna od klientů **nebu**de nikdy údaje touto formou požadovat! Nikdy nezasílame nevyžádané e-maily s odkazy na internetové adresy.

V logu proxy je pak zaznamenáno vše potřebné. SSLSTRIP je na začátku, není napsán jako dokonalý nástroj. Je dost věcí, které by v něm šly zlepšit. Dnešní stránky jsou plné složitého kódu, používají cookie a další metody, takže všechny stránky nemusí se současnou verzí tohoto nástroje fungovat správně. Ale

princip a možné dopady jsou naprosto zřejmé. Autor nástroje v rámci konference provedl pár testů. Za 24 hodin byly zachyceny desítky hesel k platebním bránám, jako je paypal, desítky čísel kreditních karet a stovky dalších hesel k „zabezpečeným“ službám. Dále demonstroval možnosti, jak tento útok provádět i bez arspooft, tedy MITM na jiné úrovni.

Pro všechny, kteří si chtějí útok vyzkoušet, je zde URL, ze které je možné si potřebný nástroj a know-how stáhnout: <http://www.thoughtcrime.org/software/sslstrip/>.

Doporučení pro běžné uživatele není v danou chvíli snadné. Snad jen ostražitost a zase ostražitost. Také není na škodu znát některé klíčové stránky a psát jejich URL přímo, včetně specifikace protokolu, nebo si stránky v tomto tvaru dát do záložek (bookmark).

V kombinaci s technikami založenými na MD5 kolizích, popsanych také v těchto aktualitách, můžeme doufat, že internet banking a jiné citlivé služby, kde se na bezpečnost klade důraz, nebude pouze adrenalínovým sportem pro běžné uživatele. Je totiž hezké, že vás každá banka varuje, kolik máte věnovat zabezpečení svého počítače a kolik toho musíte znát. Diskuse na téma „přenesení odpovědnosti“ velmi přesahuje rozsah této aktuality. Otázkou spíše je, jsou-li toho běžní uživatelé schopni.

**Kde program
SSLSTRIP
stáhnout?**

**Doporučení pro
koncové uživatele**

BUKÁNKO