

Rozbor bezpečnosti Internet Bankingu

Bezpečnostní koncept Internet bankingu vychází se změn, které v posledních létech přinesl rozvoj Internetu a jeho nástrojů. V neposlední řadě také větší množství uživatelů operačního systému Linux.

Grafické sjednocení www stránek pro oba operační systémy a jejich internetových prohlížečů umožnil především rozvoj kaskadových stylů CSS.

Proto byl stanoven jako jeden z výchozích parametrů - užití obou operačních systémů. Tomu musí být přizpůsoben bezpečnostní koncept a zejména použitá technologie. Technologie musí být implementovatelná pro oba operační systémy a jejich prohlížeče.

V různých implementacích internetbankingů v řadě bank je použita celá škála bezpečnostních nástrojů. Některým s nich se v rozboru budeme věnovat a vysvětlíme proč nejsou v našem případě použity.

Šifrování dat - autentizace spojení

- **Šifrování dat**

Pro šifrování dat byl použit standardní protokol SSLver 3.0 se symetrickou šifrou AES/256, AES/128 a 3DES(168) podle typu prováděné operace.

- **Autentizace spojení**

Vzhledem k tomu, že jednosměrný protokol SSL autentizuje pouze server vůči klientovi, je nutné zajistit druhou polovinu autentizace, tedy autentizovat klienta vůči serveru. Toto je poměrně kritická operace zejména při útoku „**Man-in-the-Middle Phishing Attack – Phishing 2.0**“. Jednou z možností, poměrně často používanou je „**two-factor authentication**“. Tedy dvou složková autentizace. Druhá složka autentizace obsahuje něco speciálního, co má, nebo ví pouze klient. Na první pohled ideální řešení. Problém je v tom, že i tato druhá složka je přenášena přes Internet k serveru a phishingu nezabrání.

Pro úplnost uvádíme tabulku obsahující běžně používané možnosti zajištění dvou složkové autentizace

Bezpečnostní opatření	Jak pracuje	Útok Phishing 2.0
One Time Password Tokens - OTP (včetně HW, SW, kalkulátoru apod.) *1	Klient dostane HW zařízení, papírovou tabulku apod, které mění heslo-kód, tedy druhou složku, pro každé přihlášení (OTP je obvykle platný 30-60 sekund)	OTP je v konečné fázi zapsán do formuláře a přenášen Internetem. Může být zachycen útočníkem a použit pro přihlášení během několikati milisekund. Je také možné (CitiBank - USA) generovat stránky, které jsou podobné přihlašovací masce banky, odchytnout OTP přerušit spojení a následně jej použít.
Označení zařízení-počítače	Server vytvoří profil zařízení, se kterým komunikuje	Profil je přenášen prostřednictvím internetu, je stále stejný, jeho odchytnutí je jednoduché.

	prostřednictvím informací o zařízení získaných s použitím WWW prohlížeče.	
Použití Cookie	Server umístí u klienta cookie, po té co uživatel odpoví na tajné otázky	Cookie nejsou umístěny na klientském počítači stále. Po určité době jsou vymazány. V tom případě je nutné vyzvat uživatele, aby odpověděl na otázky znovu. Útok Man-in-the-Middle lze vést tak, že útočník přiměje uživatele, aby odpověděl na tajné otázky prostřednictvím serveru útočníka. Pak zachycené odpovědi použije pro logování do realné banky. Útočník může odchytnout text zadaný uživatelem. V tomto případě má však pozici stíženou, protože musí udržet spojení s bankou po dobu platnosti obrázku-textu. Poměrně jednoduché-útočník ukrade heslo v okamžiku kdy je zadáno-potvrzeno. (např simulace přihlašovací masky serveru banky)
Obrázek s textem na WWW stránkách	Uživatel přepíše do pole text v obrázku.	
Virtuální klávesnice	Uživatel zadává přihlašovací heslo prostřednictvím grafické klávesnice na WWW stránkách	

Zásadní problém je v tom, že jsou „tajemství“ ve všech případech sdílená.

Tuto vlastnost lze obejít. První způsob je užití oboustranného protokolu SSL. Tedy certifikát má nejen server banky, ale i klient. Jinými slovy důvěryhodný server musí říci klientovi – „ano spojil jsi se se serverem banky“ a bance „ano spojila jsi se s počítačem klienta“. Certifikát musí vydat certifikační autorita (CA) a to nejen pro banku, ale i pro každého klienta zvlášť. Pak by ovšem všichni klienti museli každý rok žádat o certifikát CA např. VeriSign a platit za něj.

Druhý způsob je použití „tajemství“, které není sdíleno, tedy prvků asymetrického šifrování. V tomto případě si certifikáty – veřejné klíče vyměňují banka a klient mezi sebou, druhá část páru – tajný klíč, zůstává známa pouze klientovi a banka ji neověřuje – není přenášena internetem a naopak. Mimochodem, tímto způsobem se vytváří certifikát vydaný CA. Tajný klíč zůstává klientovi, veřejný klíč CA.

V našem případě jsme zvolili pro autentizaci spojení asymetrické šifrování RSA/1024-4096. Tento systém nám pomůže také při autorizaci aktivních operací. Popis distribuce klíčů je uveden dále.

Tím sice máme zajištěnou autentizaci spojení a ochranu proti tomuto útoku, ale vznikl nám nový problém. Musíme bezpečně uložit tajný klíč a chránit ho proti útoku „trojským koněm“ viz dále.

Bezpečné generování dynamických WWW stránek - napojení na databázi

Generování dynamických WWW stránek je podmíněno přístupem na databázový server. Site server i databázový server musí být chráněn proti neautorizovanému přístupu k datům uloženým na SQL serveru. Ochrana se týká autentizovaných i neautentizovaných uživatelů. I klient může být potencionální útočník.

Pro přístup do databáze a operacemi nad ní se obvykle používá nějaký CGI systém.

který tvoří rozšíření site serveru. Buď se jedná o skriptovací systém (PHP, JSP, ASP apod.), nebo binární kód obvykle psaný v Javě (C/C++, Perl, Python atd.). Systém obvykle umožňuje řízení tvorby dynamických stránek, které následně zprostředkuje site server. Vzhledem k tomu, že se jedná vždy o externí program – interpret skriptovacího jazyka, nebo vlastní program, vzniká tím velké bezpečnostní riziko. Riziko spočívá v tom, že se uživatel může dostat k datům, ke kterým nemá autorizovaný přístup.

Poznámka

V předchozí verzi Internetbankingu tento bezpečnostní problém v podstatě nebylo nutno řešit. Site server byl použit pouze pro generování statické, úvodní, stránky obsahující zpuštění Active X. Ten byl předchozí operací instalován a zaregistrován internetovým prohlížečem na straně klienta. Vlastní přenos dat probíhal protokolem definovaným ComTechem a přístup do SQL serveru řídil komunikační server – služba, která byla oddělena od klientské strany.

Provedli jsme analýzu všech standardních skriptovacích systémů a to z následující pohledů

1. Dostupnost z obou operačních systémů
2. Bezpečnost
3. Rychlost – doba odezvy na dotaz (při předpokládaném počtu přístupů na site server)
4. Grafika navrhovaných WWW stránek

Vzhledem k publikovaným chybám skriptovacích interpretů, které splňovaly první podmínku jsme usoudili, že žádný z nich dostatečně nesplňuje druhou podmínku. Žádný z nich nebyl dostatečně bezpečný pro naši aplikaci, přestože u řady z nich existují dodatečné nástroje, které umožňují bezpečnost zvýšit (např. NuSphere Nu-Coder pro PHP). Třetí a čtvrtá podmínka je v těchto systémech snadno realizovatelná.

Druhým možným přístupem je psát binární kód v Javě resp. JSP. Tím bychom splnili první dvě podmínky, ale dostali bychom se do problémů ve třetí a čtvrté podmínce, které spolu úzce souvisí.

V duchu filozofie naší firmy jsme se rozhodli použít vlastní skriptovací CGI systém. Jeho návrh splňuje všechny čtyři podmínky.

● **Framework ComTech**

Framework ComTech vytváří interpret skriptů, který je zaměřen především na bezpečnost. Jsou v něm zahrnuty a řešeny všechny bezpečnostní funkce a operace s nimi spojené. Společně s ovladači v Jave, umožňuje použití externích kryptovacích zařízení typu tokenů, čipových karet apod. Bezpečným způsobem přistupuje k SQL databázím. Umožňuje vytváření dynamických stránek s použitím JavaAppletů. Je rychlejší než kód psaný v Javě. Na druhé straně rozsah vlastních definovaných funkcí skriptu je zatím omezen. Samozřejmě jsou implementovány všechny základní typy příkazů, které jsou nutné pro řízení chodu kódu napsaného v tomto systému. V zásadě však lze použít jakýkoliv základní HTML kód doplněný o JavaScript, uložených v samostatných souborech.

Framework tedy vytváří prostředky pro maximální dostupnou bezpečnost WWW stránek za cenu toho, že si programátor musí celou řadu funkcí (které jsou běžně dostupné v jiných interpretech) vytvořit sám. Jako site server je použit Apache verze 2.2.

● **Autorizace aktivních operací**

K autorizaci aktivních operací se používají zhruba stejné technologie, jako v případě autentizace spojení. V tomto případě je situace v některých případech poněkud

odlišná. Pokud je prostředek autorizace svázaný s parametry aktivní operace (platby), pak v případě napadení může být aktivní operace (platba dekodována), nikoliv však změněna. Tuto skutečnost lze považovat za menší bezpečnostní riziko i když i samostatný údaj má svou informační hodnotu.

Jestliže tedy použijeme pouze One Time Password v jakékoliv podobě - token, tabulka kódů, TAN (Transaction Authentication Number) je útok proti takovému typu autorizace aktivní operace stejný jako v případě autentizace spojení - phishing a nelze se proti němu účinně bránit.

Pokud však vygenerujeme bezpečnostní kód na základě parametrů operace, pak lze zpětně ověřit, že zadáný kód obsahu transakce odpovídá. Takto vygenerovaný kód se ke klientovi musí dostat v reálném čase prostřednictvím jiného média, než je Internet. K tomuto účelu se používá SMS.

Výhodou tohoto systému je, že není nutné chránit klientský počítač proti útoku „trojským koněm“.

Nejbezpečnější způsob autorizace je elektronický podpis. Ten transakci chrání nejen proti útoku Man-in-the-Middle, ale i proti útoku z prostředí banky, nebo klienta. Obrana je zajištěna tím, že není sdíleno „tajemství“. Pouze klient má k dispozici tajný klíč (TK) z páru veřejný/tajný klíč. Banka má k dispozici veřejný klíč (VK) klienta, který ji umožňuje transakce zkontrolovat, nikoliv však vytvořit. Realizuje se tak princip neodmítnutelnosti zodpovědnosti za požadované transakce klientem.

Tento postup je bezpečnější než předchozí - SMS, protože neumožňuje ani zjištění obsahu transakce. Na druhé straně zůstává možnost útoku „trojským koněm“.

● Užití autorizačních prostředků

Jak vyplývá z předchozího rozboru, lze použít dva typy autorizačních prostředků pro autorizaci aktivních operací

- Autorizace prostřednictvím SMS kódů, který musí obsahovat parametry platby
- Použití mechanismu elektronického podpisu s bezpečným uložením TK klienta

Elektronický podpis, resp. autorizační kód transakce musí být proveden nad celou transakcí. Jestliže umožníme klientovi zadávat hromadný příkaz, pak musí být autorizován hromadný příkaz jako celek a ne jeho jednotlivé položky. Aby byl tento požadavek splněn je nutné udržet tyto informace na straně klienta, nepředávat jej přes internet na site server. Tato část WWW stránek musí obsahovat kód v Javě.

● Distribuce autorizačních prostředků

V systému existují dva typy autorizačních prostředků - mechanismus elektronického podpisu a SMS kód. Jak vyplývá z předchozích rozborů jsou prvky elektronického podpisu použity i pro autentizaci spojení. Certifikát klienta - pár VK/TK je tedy nutné vytvořit a zaregistrovat vždy. Jestliže klient použije k autorizaci platby SMS kód, pak musí být bezpečným způsobem předáno i telefonní číslo, na které bude SMS autorizační kód přicházet.

● Vytvoření a obnova elektronického certifikátu klienta

Klient generuje, prostřednictvím Java programu v internetovém prohlížeči, svůj pár VK/TK na svém počítači. TK zůstává uložený u něj a to buď vsouboru (pokud bude používat SMS autorizaci aktivních operací), nebo na USB tokenu. VK klíč je dočasně uložen na serveru banky. Klient ze serveru obdrží informace nutné pro ověření jeho registrace pracovníkem banky:

ID nové registrace - inicializační kód klienta
Kryptografický otisk SHA1 veřejného klíče - registrační kód klienta

Po návštěvě v bance obdrží klient tzv. aktivační kód klienta. Ten je vytvořen kryptografickým otiskem SHA1 z údajů zadaných klientem během návštěvy banky. Jednoznačnost aktivačního kódu je zaručena tím, že do SHA1 je zahrnuto jeho jedinečné číslo účtu.

Po zadání aktivačního kódu klientem do Internetbankingu a jeho následným porovnáním s údaji na serveru je registrace VK dokončena a ten se stává aktivním.

Tento postup je zvolen kvůli bezpečnému přiřazení klienta a jeho VK. Případné proražení této ochrany (např. z prostředí banky) by nemělo žádné fatální následky, protože TK má k dispozici pouze klient a celá operace by se musela pouze zopakovat.

Platnost certifikátu - páru VK/TK je časově omezena a je nutné jej obnovovat. Klient musí vygenerovat nový pár VK/TK a nový veřejný klíč musí podepsat starým dosud platným TK.

Pokud bude chtít tuto operaci provést po ukončení platnosti TK musí vytvořit novou registraci a znovu přijít do banky.

Jinými slovy, pokud klient nemá k dispozici, z jakéhokoliv důvodu, platný TK obnovu nelze provést.

Změnu telefonního čísla pro SMS autorizaci lze provést na pobočce - nejbezpečnější způsob, nebo přes internet. Ale s tím, že proběhne standardní autorizace aktivní operace prostřednictvím SMS. Autorizační SMS kód přijde samozřejmě na staré, dosud aktivní telefonní číslo.

• Úložiště klíčů - USB token kryptografický procesor

Tato část se týká pouze uložení páru VK/TK v případě, že klient nepoužívá pro autorizaci SMS. Z pohledu útoku „trojským koněm“ je tento bod nejdůležitější. Tvoří ochranu proti napadení počítače klienta a získání TK útočníkem.

V zásadě nelze chránit TK proti tomuto útoku, pokud se vyskytne v nezašifrované podobě v operačním systému a to v jakémkoliv jeho části. K tomu musí vždy dojít, klient ho musí v rámci elektronického podpisu použít. Nejjednodušší způsob útoku je samozřejmě odhycení hesla, pomocí kterého uživatel soubor s TK dešifruje, ale lze mapovat i operační paměť.

Tomu lze zabránit pouze jediným způsobem a to tak, že se TK nikdy v klientském počítači neobjeví. Proto se používá USB token, obsahující kryptografický procesor. Veškeré šifrovací operace se provádí přímo v něm. TK ho nikdy neopustí. USB token je na úrovni čipové karty, používají se stejné procesory, pouze „obal“ je jiný, pro nás vhodnější.

Přístup k USB tokenu a předání VK na server banky zajistí ovladače a program v Javě v internetovém prohlížeči. Toto je hlavní limitující faktor pro použití USB tokenů v operačním systému Linux. Dodavatel USB tokenů musí zajistit podporu pro jejich použití v prostředí Java.

Poznámka

Čipové karty a i USB tokeny se vyrábějí v různých variantách. Ty nejnepříjemnější obsahují pouze flash paměť (obdobně jako USB disky). Jediná vlastnost, kterou mají oproti USB disku je v tom, že jsou přímo chráněny PINem, nebo heslem. To však neochrání proti útoku „trojským koněm“, kdy útočník použije k získání TK okamžik elektronického podpisu na

počítači klienta.

Administrátorské nástroje

Pro správu Internet Bankingů jsou vytvořeny dva administrátorské nástroje. Z pohledu bezpečnosti Internet Bankingů slouží především k registraci veřejných klíčů a GSM telefonních čísel pro SMS autorizaci. Oba nástroje provádějí zápisy do tabulek, které udržují záznamy o provedených operacích s údaji klientů a s jejich účty.

Kromě toho umožňují zadávání základních informací o klientovi, jako je jméno, sídlo (bydliště), atd. Lze zadat také základní informace o účtu (číslo, název, stavy, atd.)

GEBAAdmin

GEBAAdmin je hlavní administrátorský nástroj, určený pro ústředí.

Je napojen přímo na databázi prostřednictvím vnitřní sítě. Jedná se o standardní aplikaci se standardními přístupy do databáze. Vstup je chráněn uživatelským jménem a heslem. Kontroluje se zda nové a předchozí heslo není stejné. Umožňuje podrobné sledování stavu Internet Bankingů, nastavení parametrů bankovních operací a především práci s uživateli administrátorských nástrojů, tedy

- Vytvoření nového uživatele
- Nastavení přednastavených hesel
- Blokování uživatele
- Vymazání uživatele

WEBAdmin

WEBAdmin je podřízený administrátorský nástroj, určený pro pobočky

Je napojen prostřednictvím HTTPS protokolu na databázi. K ní přistupuje prostřednictvím PHP 5. K přístupu používá pobočkovou síť.

Umožňuje zadávání nového klienta, jeho registraci, nebo přeregistraci. Dovoluje také editovat stávající účty, ale pouze jejich název a zadávat nové účty.

Vstup je opět chráněn jménem a heslem. Veškeré aktivní operace je nutné potvrzovat druhým pracovníkem a to jeho uživatelským jménem a heslem. Záznamy jsou vedeny nejen o tom, kdo operaci zadal, ale také o tom, kdo ji potvrdil.

Nový uživatel WEBAdminu je nucen změnit přednastavené heslo při prvním přihlášení. V opačném případě se nepřihlásí. Stávající uživatel může měnit vlastní heslo. Je to jediná operace, která mu je povolena. Kontroluje se zda nové a předchozí heslo není stejné. Délka hesla je minimálně 8 znaků a musí použít velká písmena, malá písmena a číslice.