Protokoly pro elektronické platební systémy

Vložil/a il_man [1], 11 Květen, 2007 - 16:26

- Security [2]

Malý úvod, potažmo přehled protokolů užívaných při platebních transakcích.

Secure Electronic Transaction (SET)

SET je komplexní protokol pro zabezpečení elektronických transakcí zajišťující důvěrnost informací, integritu plateb a ověření všech komunikujících stran. SET využívá následujících zabezpečovacích mechanismů:

· Šifrování symetrickým klíčem
· Šifrování veřejným klíčem
· Hašovací funkce
· Digitální podpisy
· Certifikace veřejného klíče

Šifrování symetrickým klíčem

Vysílač i přijímač sdílí jeden stejný klíč k šifrování a dešifrování. Nevýhodou je zajištění předání utajeného klíče bezpečnou cestou. Nejznámější symetrické šifrovací mechanismy jsou DES, 3-DES a AES.

Šifrování veřejným klíčem (Asymetrické šifrování)

Používá pro svou funkci 2 klíče - veřejný a soukromý. Při šifrování vysílač šifruje zprávu pomocí veřejného klíče příjemce, ten ji pak dešifruje vlastním soukromým klíčem. K nejznámějším algoritmům pro šifrování veřejným klíčem patří RSA.

Hašovací funkce

Používá se jako doplňkové zabezpečení. Výstupem při použití této metody je haš, neboli digitální otisk dat, což je posloupnost určité délky. Z vypočítaného haše určitých vstupních dat již nelze získat tatáž data zpět. Mezi nejznámější hašovací funkce patří MD5 a SHA1.

Digitální podpis

Slouží k ověření digitálních informací. Implementuje se s použitím asymetrického šifrování a definuje dva algoritmy - jeden pro podepisování a druhý pro ověřování. Digitální podpis se vzhledem k časové náročnosti algoritmů asymetrického šifrování používá zpravidla pouze pro haš zprávy. Princip spočívá v zašifrování haše soukromým klíčem odesílatele. Příjemce z přijaté zprávy vytvoří haš a porovná ho z hašem získaným dešifrováním digitálního podpisu odesílatele. Při jejich shodě je téměř jisté, že zpráva nebyla změněna.

Digitální obálka

Zajišťuje bezpečný přenos a doručení symetrického klíče od vysílače k příjemci. Princip spočívá v

zašifrování vygenerovaného symetrického klíčem K veřejným klíčem příjemce Vk-p. Výsledkem je zašifrovaný klíč E(K)Vk-p, který je odeslán příjemci. Ten ho dešifruje pomocí svého soukromého klíče, čímž získá symetrický klíč, který poté používá při následné komunikaci.

Transakce

Zákazník si na internetu vybere požadované zboží a pošle svůj požadavek obchodníkovi. Obchodník přijme požadavek na nákup zboží a přiřadí mu jedinečné ID, které pošle společně se svým certifikátem a s certifikátem platební brány zákazníkovi. Zákazník ověří přijaté certifikáty a vytvoří zprávu s informací o objednávce OI a o platbě PI a přiřadí jim získané ID. Zákazník zašifruje PI + Dvojitý podpis + OIMD náhodně vygenerovaným symetrickým klíčem K1. Tento klíč je dále zašifrován veřejným klíčem platební brány Vk-pb (digitální obálka). Zašifrovaná zpráva a digitální obálka jsou společně s PIMD, OI, dvojitým podpisem a certifikátem zákazníka odeslány obchodníkovi. Obchodník překontroluje OI pomocí PIMD a dvojitého podpisu a předá zašifrovanou část zprávy obsahující informace o platbě PI, dvojitý podpis a OIMD společně s digitální obálkou platební bráně která, je součástí banky obchodníka. Platební brána po přijetí a přečtení zprávy vyšle do finanční sítě dotaz, zda jsou na účtu zákazníka potřebné prostředky. Finanční síť odpoví zda je/není objednávka krytá
prostředky z účtu zákazníka. Platební brána pošle oprávnění/zamítnutí platby obchodníkovi a ten uzavře/neuzavře objednávku a pošle vyrozumění zákazníkovi. Banka obchodníka přijme od banky zákazníka platbu za sjednané zboží s obchodníkem.

Secure Sockets Layer (SSL)

SSL je protokol, resp. vrstva vložená mezi vrstvu transportní a aplikační, která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran. Použití protokolu SSL však nese jisté riziko. Během komunikace jsou veškerá data mezi zákazníkem,obchodníkem a bankou posílána ve vytvořeném zabezpečeném kanále. Každý z účastníků tedy může číst zprávy třetí strany, tzn. i ty, které mu nenáleží, což je nežádoucí.

Princip

SSL spojení funguje na principu asymetrické šifry, kdy každá z komunikujících stran má dvojici šifrovacích klíčů - veřejný a soukromý. Veřejný klíč je možné zveřejnit a pokud tímto klíčem kdokoliv zašifruje nějakou zprávu, je zajištěno, že ji bude moci rozšifrovat jen majitel použitého veřejného klíče svým soukromým klíčem. Pro výměnu klíčů se používají kryptografické algoritmy RSA, Diffie-Hellman, DSA
nebo Fortezza, pro symetrickou šifru: RC2, RC4, IDEA, DES, 3DES nebo AES a pro jednocestné hašovací funkce: MD5 nebo SHA.

Transakce

· Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi.
· Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací a certifikát serveru.
· Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru.
· Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude kódovat následná komunikace. Ten zakóduje veřejným klíčem serveru a pošle mu ho.
· Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče. Z tohoto základu vygenerují jak server, tak klient hlavní šifrovací klíč.
· Klient a server si navzájem potvrdí, že od teď bude jejich komunikace šifrovaná tímto klíčem. Fáze handshake tímto končí.
· Je ustaveno zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem.
· Aplikace od teď dál komunikují přes šifrované spojení.

Open Financial Exchange (OFX)

OFX specifikuje standard pro elektronickou výměnu finančních dat přes internet. Umožňuje finančním institucím se spojit se svými zákazníky přímo bez prostředníka. Open Financial Exchange používá SGML ke strukturování a formátování informací posílaných mezi aplikacemi. Ačkoliv bylo OFX vytvořeno jako nezávislý standard na různých komunikačních protokolech, ve verzi 1.0.2 již používá Hypertext Transport Protocol (HTTP) k přenosu dat a od verze 2 je celá specifikace postavena již na XML. Vše funguje na bázi požadavku a odpovědi (request-response systém), jež jsou uloženy v obyčejných textových souborech a formátovány pomocí XML. OFX aplikace zasílá požadavek jiné OFX aplikaci, která ji vrací odpověď. Požadavek, který je aplikací zasílán je ve formě HTTP POST příkazu. OFX server, který přijímá POST příkaz, dále data zpracuje a pošle zpět odpověď s požadovanými daty. V OFX se používá hesla k zjištění identity klienta a certifikáty dovolují klientovi autentizovat server. Jakmile je v OFX již jednou zpráva vytvořena, nemůže být změněna tak, aby se to nezjistilo. K tomuto se používají různé hashe. OFX podporuje Secure Sockets Layer (SSL), což je kryptografický protokol běžně užívaný na internetu. SSL šifruje zprávy a zajišťuje jejich integritu a autentizaci.

Visa 3-D Secure

Visa 3-D Secure je tří-doménový zabezpečený protokol. VISA 3D Secure protokol následuje centralizovaný autentizační přístup, kdy se z obchodníkovy komponenty směrují všechny autentizační požadavky do VISA adresáře, který udržuje informace o všech uživatelích a směruje dále požadavek na příslušného uživatele. Vydavatel karty je v komunikaci s držitelem karty díky jeho prohlížeči, kde se sbírají autentizační detaily. Vydavatel je následně zvaliduje a pošle zpět obchodníkovi jako autentizační odpověď. 3-D Secure je mechanismus autentizace držitele karty. Každá karta zadaná do platební brány je kontrolována příslušnou asociací MasterCard nebo VISA. Kontroluje se, zda je pro kartu požadována autentizace držitele karty, či nikoliv. V případě požadavku autentizace je držitel přesměrován na systém vydavatelské banky, kde potvrdí svoji identitu (heslo, e-PIN, nebo jinou tajnou informaci, sdílenou s vydavatelem karty). Výsledek autentizace je předán zpět do platební brány.

Transakce

· Jestliže si držitel VISA karty vybral obchodníka a zboží na jeho webu a rozhodl se jej zaplatit pomocí 3-D Secure, musí mu nejprve poslat číslo své kreditní karty.
· Obchodníkův plug-in se dotáže VISA adresáře na registrační status zákazníka
· Jestliže je číslo kreditní karty v určitém karetním rozsahu (definuje VISA), VISA adresář se dotazuje na příslušný ACS, zdali je číslo karty řádně registrováno.
· Access control server odpoví adresáři VISA a zašle mu údaje o zákazníkovi
· VISA adresář přepošle tuto odpověď do obchodníkova plug-inu
· Obchodníkův plug-in pošle požadavek na autentizaci plátce k ACS pomocí prohlížeče zákazníka
· ACS obdrží požadavek na autentizaci
· ACS autentizuje nakupujícího pomocí znalosti jeho hesla, potom formátuje autentizační odpověď s příslušnými hodnotami a podepíše ji
· ACS vrátí autentizační odpověď obchodníkovu plug-inu pomocí uživatelova prohlížeče. ACS pošle vybraná data na server autentizační historie (Authentication History Server) pro účely logování
· Obchodníkův plug-in obdrží autentizační odpověď
· Obchodníkův plug-in zkontroluje podpis na této odpovědi
· Obchodník pokračuje s autorizací k platbě u své banky
· Banka obchodníka (nabyvatel) autorizuje tento požadavek bance zákazníka (vydavatel) pomocí VisaNetu.

The Bank Internet Payment System (BIPS)

BIPS umožňuje plátcům přístup k těmto bankovním platebním mechanismům ve volně přístupné síti. Plátci mohou posílat zabezpečené platební instrukce přes Internet na BIPS server u své banky, kde

se žádost převede do tradičních bankovních platebních transakcí.
Plátce posílá BIPS platební instrukce na platební server ve své bance a to buď pomocí e-mailu nebo webového rozhraní. BIPS platební server interpretuje a překládá instrukce do bankovních platebních transakcí a posílá je k příslušnému bankovnímu platebnímu systému pomocí tradičních finančních sítí. BIPS schéma spoléhá na existenci infrastruktury veřejných klíčů (PKI), kde každý účastník BIPS má X.509 certifikát, který se používá jak k vytváření podpisů, tak k šifrování citlivých materiálů. Každá instrukční zpráva je digitálně podepsána odesílatelem a zahrnuje odesílatelům certifikát a unikátní transakční identifikátor. Je definováno několik algoritmů pro implementaci digitálních podpisů např. RSA s MD5 pečetí. Podpisy jsou kódovány jako ASCII znaky používající Base64 kódování, v kterém je každý znak reprezentován 6 bity. Na vyšší úrovni je platební instrukce podobná elektronickému šeku v tom, že je digitálně podepsána plátcem, ale v tomto případě je přímo poslána do jeho banky místo příjemci.

Network payment protocol (NPP)

NPP je platební protokol postavený na BIPS. Každá NPP zpráva se skládá z několika atributů jako je typ platby, detaily o plátci a příjemci a množství platby. Ke skrytí částí NPP zpráv je možno použít symetrické šifrování. DES v ECB módu. UCAF/SPA UCAF je univerzální metoda pro předávání autentizačních dat uživatele mezi bankami a obchodníky. Skládá ze dvou komponent:

· UCAF Data Infrastructure - série několika tajných skrytých polí
· UCAF Authentication Data Field - specifické 32- znakové pole v rámci celé UCAF. SPA je bezpečnostní řešení vyvinuté k autentizaci zákazníků při on-line platbách.

Transakce

· Uživatel nakupuje na stránkách obchodníka a na konci jde k pokladně. V tomto momentě, el. peněženka detekuje SPA platební stránku obchodníka.
· El. peněženka, jenž je nainstalována u klienta (PC), čte informace o transakci
· Peněženka požaduje autentizační informace (např. uživatelovo ID a heslo) např. ve formě vyskakujícího pop-up okna.q
· V tomto kroku peněženka posílá autentizační informace a informace o transakci na SPA server do banky zákazníka.
· Server banky zákazníka zkontroluje autentizační informace o zákazníkovi s informacemi, které má uloženy ve své databázi a po úspěšné validaci vygeneruje unikátní transakčně závislý autorizační token (AAV) a pošle jej peněžence na PC zákazníka.
· Peněženka předá tento AAV serveru obchodníka, který jej dále generuje do všech dalších pokladních stránek dané transakce. Uživatel již také nemusí vyplňovat další informace ohledně dopravy, adresy doručení atd.
· Obchodník odešle autorizační požadavek spolu s AAV do své banky.
· Banka obchodníka posílá autorizační požadavek a AAV do banky zákazníka pomocí MasterCard peněžní sítě Banknet.
· Banka zákazníka zkontroluje AAV oproti svým záznamům v databázi a pošle autorizační odpověď bance obchodníka.
· Banka obchodníka pošle autorizační odpověď obchodníkovi.
· Obchodník potvrdí transakci a dodá číslo objednávky či bankovní doklad zákazníkovi.

Homebanking computer interface (HBCI)

HBCI je specifikace pro komunikaci mezi inteligentními systémy uživatele a korespondujícími výpočetními centry pro výměnu homebankingových transakcí. Přenos dat je prováděn pomocí síťového rozhraní a je založen na přizpůsobivé ohraničující syntaxi. HBCI zpráva se skládá z hlavičky, podpisové hlavičky, jednoho či více obchodních segmentů, podpisového traileru a traileru samotné zprávy. Volitelná šifrovací hlavička dovoluje, aby každá zpráva mohla být zabezpečena pomocí příslušných šifrovacích algoritmů. Zpracování zpráv může být prováděno synchronně či asynchronně. Pro verifikaci a šifrování zasílaných zpráv používá RSA. V typické HBCI transakci je použito heslo k

autorizaci uživatele pro přístup do bankovního systému. Každý uživatel má svůj elektronický podpis vytvořený RSA algoritmem. Na rozdíl od symetrických algoritmů (DES, 3DES) u asymetrických algoritmů (RSA) se pracuje se dvěma klíči: soukromým a veřejným. Soukromý klíč zůstává bezpečně uložen na uživatelově PC. Banka pak používá veřejný klíč uživatele k jeho autentizaci a kontrole jeho podpisu.

Zdroje

· http://cs.wikipedia.org [3]
· http://en.wikipedia.org [4]
· http://www.globalpaymentsinc.com [5]
· http://www.fstc.org [6]

URL článku:
https://security-portal.cz/clanky/protokoly-pro-elektronick%C3%A9-platebn%C3%AD-syst%C3%A9my

Odkazy:
[1] https://security-portal.cz/users/ilman
[2] https://security-portal.cz/category/tagy/security
[3] http://cs.wikipedia.org
[4] http://en.wikipedia.org
[5] http://www.globalpaymentsinc.com
[6] http://www.fstc.org