Otázka 22
Zadání

***Předmět:* A7B32KBE**

Aplikovaná kryptografie a bezpečnost. Adresáře veřejných klíčů. Revokace klíče a revokační certifikáty. Vztahy důvěry. Autentizace uțivatele v systému, autentizace stanice v síti. LDAP, Kerberos. Šifrované síťové protokoly. Bezpečnost ukládání dat. (A7B32KBE)

Aplikovaná kryptografie a bezpečnost

Počítačová bezpečnost je obor informatiky, který se zabývá zabezpečením informací v počítačích, tedy odhalováním, analýzou a zmenšováním rizik spojených s používáním počítačů. Počítačová bezpečnost zahrnuje tyto úkoly:

- ochranu před neoprávněnou manipulací se zařízeními počítačového systému
- ochranu před neoprávněnou manipulací s daty
- ochranu informací před krádeží (nelegální tvorbou kopií dat) nebo poškozením
- zabezpečení komunikací a přenosu dat (pomocí kryptografie)
- zabezpečení uložených dat před neoprávněným přístupem
- zajištění celistvosti a nepodvrhnutelnosti dat (integrity)

Počítačová ochrana je často více zaměřená na techniku a matematiku, než některé jiné počítačové oblasti. Z hlediska managementu spočívá ve třech krocích:

- prevence – ochrana před hrozbami
- detekce – odhalení neoprávněných (skrytých, nezamýšlených) činností a slabých míst v systému
- náprava – odstranění slabého místa v systému

Z hlediska technického provedení může zahrnovat následující kroky:

- omezení fyzického přístupu k počítači pouze pro oprávněné uživatele, kteří budou dodržovat bezpečnost při práci s počítačem a daty
- použití hardwarových zařízení, která vynucují bezpečnostní opatření, což snižuje závislost počítačové bezpečnosti na software (počítačových programech)
- využití mechanismů operačního systému, která vynucují pravidla chování programů, aby byl omezen rozsah programů, kterým je nutné důvěřovat
- nasazení doplňujících přídavných softwarových systémů podporujících bezpečnost
- využití záznamů o činnosti počítačového systému (logování) pro možnost zpětného dohledání informací o událostech během bezpečnostního incidentu
- využití záznamů o změnách v programech (verzování), které je možné využít pro sledování jejich vývoje

Při realizaci kroků vedoucích k lepší počítačové bezpečnosti nesmíme opomíjet bezpečnostní projekt a plánování.

Pro realizaci těchto kroků se z valné míry užívá bezpečnostích softwarových systémů, které buď nějakým způsobem užívají kryptografických principů a algoritmů nebo jsou na nich zcela založeny.

Adresáře veřejných klíčů

Asymetrická kryptografie se od své starší, symetrické kolegyně liší jednou významnou vlastností. Pro utajování komunikace používá dva různé klíče, z nichž jeden slouží pouze pro šifrování a druhý pouze pro dešifrování. Tyto dva klíče na sobě závisí, nelze však bez dodatečných informací pomocí jednoho klíče získat klíč druhý. Uživatel, který chce utajovat svou komunikaci s kolegy, zveřejní klíč určený pro šifrování. Vystaví jej například na své webové stránce, zapíše na specializovaný server veřejných klíčů, připojuje jej ke svým e-mailům, zkrátka snaží se o jeho co nejširší rozšíření. Tento klíč se stává veřejným klíčem. Druhý, soukromý klíč si uživatel ponechá v tajnosti. Kdokoliv pak může pomocí veřejného klíče zašifrovat zprávu, kterou je však schopen rozšifrovat pouze držitel odpovídajícího soukromého klíče, tj. příjemce zprávy.

Tohoto modelu lze s výhodou použít pro vytváření elektronických podpisů. Elektronický podpis zprávy je blok dat logicky spojený se zprávou a vytvořený použitím soukromého klíče autora. Pomocí autorova veřejného klíče lze pak kdykoliv ověřit, že podpis byl skutečně vytvořen použitím odpovídajícího soukromého klíče. Díky vlastnostem asymetrických algoritmů lze takto získat spolehlivou informaci o původu zprávy. Stačí získat veřejný klíč uživatele, jehož podpisy chci ověřovat.

S touto elegancí asymetrických systémů je ovšem spojena jejich velká slabina, a tou je získání správného veřejného klíče. Pokud si uživatelé vymění své veřejné klíče osobně, mohou si být jisti, kdo je vlastníkem klíče. Pokud však uživatel získal cizí veřejný klíč z nějakého nespolehlivého zdroje (např. ze serveru veřejných klíčů), nemá žádnou jistotu, že tento klíč skutečně patří osobě, jejíž klíč hledal. U každého veřejného klíče je sice uvedena identifikace jeho vlastníka, ale může se jednat o klíč patřící osobě se stejným jménem nebo v horším případě o klíč podvržený útočníkem, který se snaží vydávat za někoho jiného.

Pro bezpečné používání asymetrických šifer je tedy nutné zavést nějaký mechanismus, který poskytne potřebnou jistotu o původu veřejného klíče. Takovou jistotu může poskytnout například potvrzení klíče důvěryhodnou stranou, které důvěřují všichni účastníci komunikace. Potvrzením je elektronický podpis, který ověřovatel připojí k veřejnému klíči uživatele a vytvoří tak certifikát veřejného klíče. Ověřovatel veřejného klíče se nazývá certifikační autorita (CA). Celý systém založený na asymetrické kryptografii a certifikačních autoritách se nazývá systém PKI (Public Key Infrastructure - překládáno systém správy veřejných klíčů).

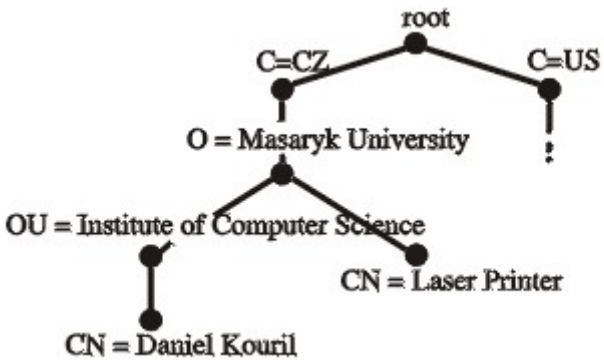
Certifikáty se mohou šířit zcela volně, každý uživatel, který zná veřejný klíč CA, může ověřit podpis na certifikátu. CA je široký pojem, může jím být úzce specializovaná, často komerční organizace nebo jen řadový uživatel. Vždy však platí, že veškerá důvěra v certifikát je úměrná důvěře v autora elektronického podpisu na certifikátu. CA svým podpisem potvrzuje původ klíče. CA proto často podmiňují vydání certifikátu předložením osobních dokladů. Certifikát podepsaný neznámou, neověřitelnou entitou nemá o mnoho větší význam, než samotný nepodepsaný veřejný klíč.

Certifikát veřejného klíče obsahuje minimálně tři části:

- Podepisovaný veřejný klíč.
- Certifikační informace: identifikátor vlastníka veřejného klíče (vlastníkem nemusí být jen fyzický uživatel, veřejný klíč může být spojen s funkcí v organizaci, s hardwarovým nebo softwarovým produktem, s právnickou osobou apod.), doba platnosti certifikátu, jméno CA.
- Jeden nebo více elektronický podpisů CA. Podpis je zpravidla aplikován na všechny výše uvedené položky.

Uživatel, který chce získat certifikát, nejprve vytvoří dvojici veřejného a soukromého klíče. Veřejný klíč spolehlivým způsobem (např. na osobně) doručí CA, která po ověření totožnosti uživatele vydá certifikát. Soukromý klíč zůstává stále utajen a ani CA nezná soukromý klíč uživatele.

Pro ukládání certifikátů s veřejnými klíči a manipulaci s nimi slouží standard ITU-T X.509, jenž je částí série doporučení X.500, která definuje adresářové služby. Adresářem ve smyslu těchto norem je databáze údajů o uživatelích a zdrojích v systému, odkud lze např. získat e-mailovou adresu kolegů nebo seznam dostupných tiskáren. Adresář lze také použít pro ukládání certifikátů. Norma X.500 doporučuje, aby záznamy byly uspořádány do stromu, který odráží organizační strukturu systému. Každá organizačně samostatná jednotka (OU) v rámci stromu může spravovat svou část záznamů. V tomto modelu definuje X.500 jednoznačné identifikátory záznamů v adresáři (Distinguished names, DN), které odpovídají pozici uživatele nebo jiné entity v organizaci. Toto pojmenování je odvozeno od pozice záznamu ve stromu. Například jméno {C=CZ, O=Masaryk University, CN=Laser Printer} identifikuje záznam pro tiskárnu Masarykovy univerzity v ČR. Názvy položek ve jméně jsou zkratkami anglických výrazů Country, Organization, Organization Unit, Common Name. X.500 definuje mnoho dalších identifikačních položek, např. pro adresu nebo telefonní číslo.



Struktura záznamů v X.509

Uložené certifikáty ve formátu dle X.509 obsahují následující položky:

- verze: upřesňuje formát certifikátu
- sériové číslo: jednoznačně identifikující číslo přidělené od CA. Každý certifikát vydaný CA má jiné sériové číslo
- identifikátor algoritmu: algoritmus, spolu s dalšími údaji použitými při vytváření podpisu certifikátu
- CA: identifikátor CA, která vytvořila a podepsala certifikát
- coba platnosti: obsahuje dva časové údaje: časový okamžik, před kterým certifikát ještě neplatí, a časový okamžik, po kterém již neplatí
- subjekt: uživatel, kterému patří certifikovaný veřejný klíč
- veřejný klíč: podepisovaný veřejný klíč, spolu s identifikátory algoritmů, pro které je určen
- podpis CA: je funkcí všech položek certifikátu

Revokace klíče a revokační certifikáty

I když zpravidla certifikát obsahuje dobu platnosti, mohou nastat případy, kdy je nutné veřejný klíč zrušit okamžitě. Může například dojít k prozrazení soukromého klíče nebo skončení zaměstnaneckého poměru uživatele držícího zaměstnanecký certifikát. Proces zneplatnění veřejného klíče se nazývá revokace. Cílem je, aby se všichni uživatele veřejného klíče dověděli o jeho neplatnosti. Vzhledem k nekontrolovanému šíření certifikátů je revokace relativně obtížný problém.

K zneplatňování vydaných certifikátů slouží revokační seznam CRL (certificate revocation list), Je to seznam revokovaných (zneplatněných) digitálních certifikátů. Certifikáty jsou zneplatňovány pomocí jejich sériových čísel. CRL vždy vydává CA, která vydala odvolávaný certifikát. CRL je generován a zveřejňován pravidelně, často v daném intervalu. Může být také zveřejněn bezprostředně po tom, co byl certifikát zrušen. Všechny CRL mají nastavenu omezenou platnost (24 hodin nebo méně). Během doby platnosti může aplikace konzultovat obsah CRL a ověřit podle něj platnost kontrolovaného certifikátu. Pro zabránění spoofingu (zneužití) na vydavatele CRL jsou obvykle CRL seznamy elektronicky podepsány certifikátem CA, který lze ověřit pomocí certifikátu CA.

Existují dva různé stavy revokace definované v RFC 3280:

Zrušení (Revoked): Certifikát je nevratně zrušen. Používá se v případě, že certifikační autorita (CA) vydala nesprávné osvědčení, nebo pokud by soukromý klíč mohl byt ohrožen. Certifikáty mohou byt rovněž zrušeny kvůli zjištění nedostatků v bezpečnostních požadavcích (například falšování dokumentů pro vydání certifikátu), chybného chování softwaru nebo porušení jakékoli jiné bezpečnostní podmínky stanovené provozovatelem CA nebo jejich zákazníků. Nejčastějším důvodem pro zrušení je, že uživatel již není jediným držitelem soukromého klíče (např. soukromý klíč byl ztracen, ukraden, zkopírován).

Držení (Hold): Tento vratný stav může být použit k nastavení dočasné neplatnosti certifikátu (např. pokud si uživatel není jistý že byl soukromý klíč ohrožen, případně zapomene heslovou frázi). Pokud se v tomto případě zjistí, že ke klíči nikdo neměl přístup, může být obnoven. Certifikát je znovu zplatněn a odstraní se z CRL.

Vztahy důvěry

Jak již bylo popsáno výše, důvěryhodnost veřejného klíče je zabezpečena (nebo alespoň zvýšena) jeho podepsáním nějakou certifikační autoritou. Dochází tedy k přenosu důvěry z certifikační autority na samotný veřejný klíč.

Hodnota digitálního certifikátu je úměrná míře důvěry, kterou máme k údajům v něm uvedených. Proto je pro certifikační autoritu nejdůležitější důvěra, kterou vůči svému okolí vzbuzuje (tj. že nevydá digitální certifikát s nepravdivými údaji). Certifikační autorita proto musí adekvátním způsobem pečovat o svoji důvěryhodnost, jinak by nebylo možné využít principu přenosu důvěry. Důvěryhodnost certifikační autority můžeme posoudit podle jejích webových stránek, použitého mechanismu ověření údajů, které žadatel o digitální certifikát předkládá a dalších znaků (články v tisku a a elektronických médiích, kótované akcie a podobně). Cena vydaného certifikátu (resp. oblíbenosti certifikační autority) pak obvykle odpovídá této těžko exaktně definovatelné míře důvěry.

Placené certifikační autority získávají od svých klientů peníze, které používají jednak na zajištění vlastní činnosti, ale hlavně na platbu za zařazení vlastních kořenových certifikátů do software, který využívá přenosu důvěry. Certifikační autority tak například platí za distribuci svých kořenových certifikátů v Microsoft Windows, webových prohlížečích jako Internet Explorer, Firefox a dalších programech.

Přenos důvěry se běžně využívá i v reálném světě. Čteme časopisy, noviny, hovoříme s lidmi, sledujeme televizi. Pokud se dozvíme něco nového, přikládáme informaci váhu podle důvěryhodnosti zdroje informací. Přenášíme tak důvěryhodnost zdroje informací na jím poskytovanou informaci. Věříme více svým blízkým přátelům nebo autoritám (seriózní noviny, učitel ve škole, kvalitní kniha, odborný pořad v televizi). Naopak s rezervou obvykle přistupujeme k informacím „jedna paní povídala" nebo k reklamě. Nevěříme řádně odsouzenému člověku nebo prokázanému falzifikátu.

Stejným způsobem se uplatňuje přenos důvěry u certifikační autority. Je-li certifikační autorita důvěryhodná, můžeme věřit informacím uvedených v digitálních certifikátech, které vydala (resp. digitálně podepsala). Věříme, že by certifikační autorita nevytvořila digitální certifikát s nepravdivými údaji.

V počítači jsou šifrovací klíče uloženy v úložišti certifikátů nebo v klíčence (tokenu). Při ověřování autentičnosti veřejného klíče můžeme využít toho, že klíč je digitálně podepsán důvěryhodnou certifikační autoritou (jinou osobou atp.). Pokud je digitální podpis certifikátu platný a důvěřujeme certifikační autoritě, která klíč podepsala, přeneseme důvěru a věříme v důvěryhodnost neznámého veřejného klíče.

Jak jsme již bylo zmíněno výše, pro usnadnění přenosu důvěry jsou v počítači obvykle předem přítomny kořenové klíče certifikačních autorit, které jsou distribuovány buď přímo s operačním systémem (Microsoft Windows) nebo s příslušnou aplikací (Firefox, Opera, Thunderbird atd.). Do úložiště je možné přidávat další certifikáty a následně důvěřovat certifikátům, které jsou jimi ověřitelné.

Autentizace uživatele v systému, autentizace stanice v síti, LDAP, Kerberos

V souvislosti s ověřováním uživatelských a strojových identit je často zmiňován systém, či princip AAA (triple A). Znamená Authentication, Authorization, Accounting (autentizace, autorizace, účtování). Obzvláště mezi pojmy autentizace a autorizace je třeba důsledně rozlišovat.

Autentizace je proces ověření proklamované identity subjektu. To se zpravidla děje pomocí uživatelského jména a hesla, předložením certifikátů nebo ověřením biometrických údajů. Cílem je tedy ověřit, že uživatel je skutečně tím, za koho se vydává.

Autorizaceoprávnění je oproti tomu schválení přístupu a přidělení práv uživateli na základě předchozí autentizace.

Účtování je proces záznamu (logování) činnosti uživatele, která následuje po autentizaci a autorizaci.

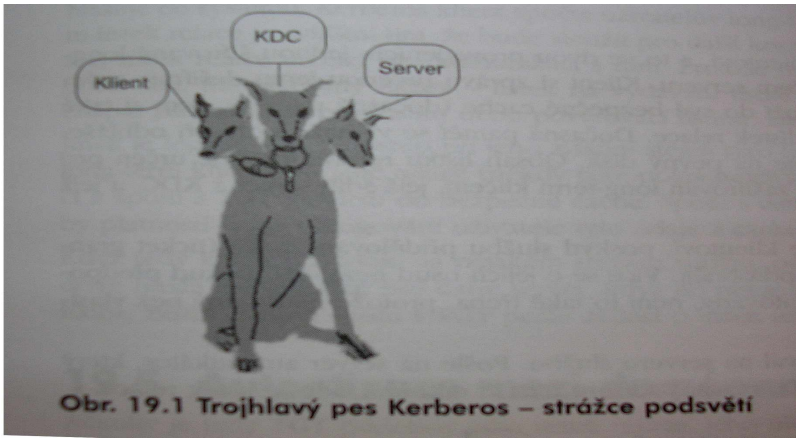
LDAP (Lightweight Directory Access Protocol) je definovaný protokol pro ukládání a přístup k datům na adresářovém serveru. Podle tohoto protokolu jsou jednotlivé položky na serveru ukládány formou záznamů a uspořádány do stromové struktury (jako ve skutečné adresářové architektuře). Je vhodný pro udržování adresářů a práci s informacemi o uživatelích (např. pro vyhledávání adres konkrétních uživatelů v příslušných adresářích, resp. databázích). Protokol LDAP je založen na doporučení X.500, které bylo vyvinuto ve světě ISO/OSI, ale do praxe se ne zcela prosadilo, zejména pro svou „velikost" a následnou „těžkopádnost".

Protokol LDAP již ve svém názvu zdůrazňuje fakt, že je „odlehčenou" (lightweight) verzí, odvozenou od X.500 (X.500 - Mezinárodní standard, vyvinutý spolkem International Consultative Commitee of Telephony and Telegraphy, pro formátování elektronických zpráv přenášených přes sítě nebo mezi počítačovými sítěmi).

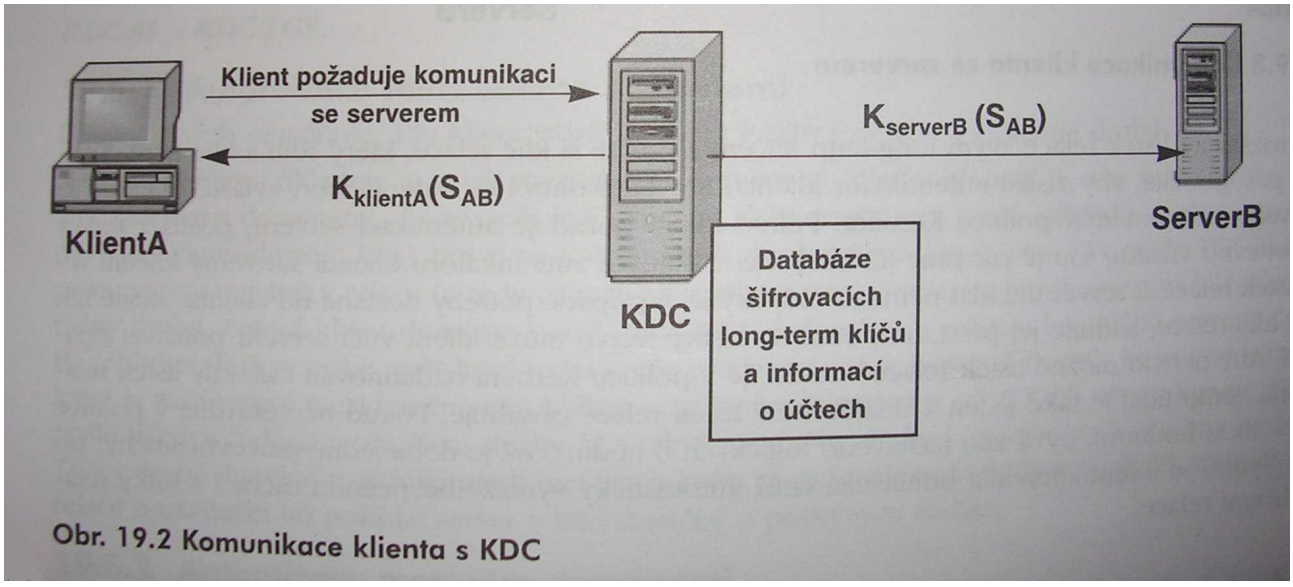
Aplikace funguje na bázi klient-server. Protože LDAP umožňuje i ukládání certifikátů a hesel, podporuje tak funkci autentizace klienta. Též může uchovávat informace o uživatelových právech a tím podporuje správnou autorizaci.

Kerberos je síťový autentizační protokol umožňující komukoli komunikujícímu v nezabezpečené síti prokázat bezpečně svoji identitu někomu dalšímu. Kerberos zabraňuje odposlechnutí nebo zopakování takovéto komunikace a zaručuje integritu dat. Jeho smyslem je podporovat centrální autentizaci uživatelů. To je velmi užitečné, protože v například v jedné firmě můžou ne jen desítky až stovky uživatelů, ale i desítky serverů, na které je třeba, aby přistupovali. Bez podobného autentizačního systému, jako je třeba Kerberos by bylo třeba, aby si každý ze serverů uchovával svou databázi uživatelů a aby na každém z nich byla zvlášť nakonfigurována softwarová podpora autentizace a autotizace. To je problém, protože množství sdílených klíčů potom roste geometrickou řadou, což představuje problém jak výkonostní, tak potenciální bezpečnostní riziko. Kerberos umožňuje, aby veškeré údaje uživatelích a jejich právech byly uloženy na jednom centrálním úložišti a zároveň poskytuje prostředek, pomocí kterého si mohou jeho clienti (v tomhle případě jsou jimi samotné servery), tyto údaje ověřit. Byl tedy vytvořen primárně pro model klient-server a poskytuje dokonce vzájemnou autentizaci – identitu své protistrany si mohou ověřit klient i server.

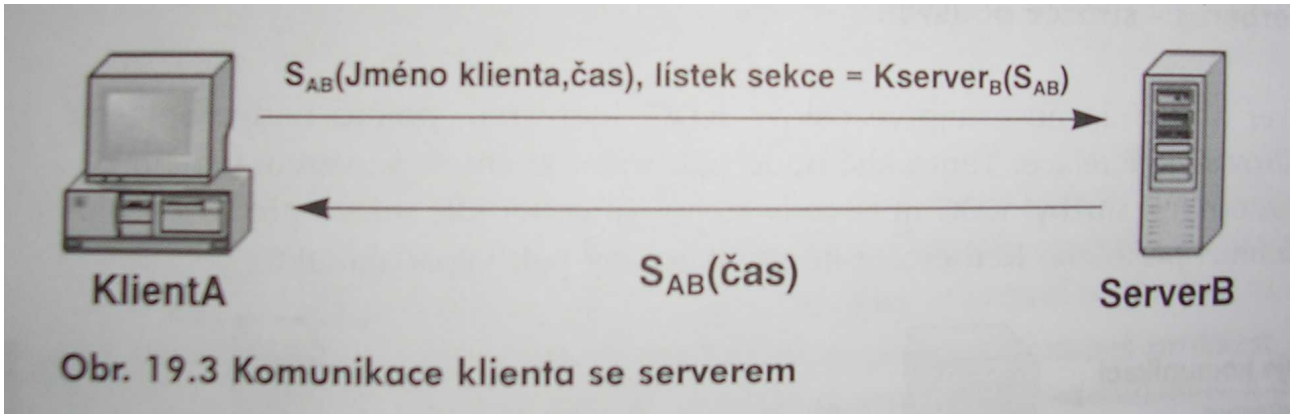
Kerberos je založen na Needham-Schroeder Symmetric Key Protocol. Používá důvěryhodné třetí strany nazývané též Key Distribution Center (KDC) sestávající ze dvou logicky oddělených částí: Autentikačního serveru (AS) a Ticket-Granting Serveru (TGS). Kerberos pracuje na principu tiketů sloužících k ověření identity uživatelů. KDC si udržuje databázi tajných klíčů; každá entita v síti, ať už klient nebo server, vlastní svůj tajný klíč známý pouze jí a KDC. Znalost tohoto klíče slouží k prokázání identity dané entity. Pro komunikaci mezi entitami KDC vygeneruje „session key", kterým obě protistrany zabezpečí vzájemnou komunikaci. Bezpečnost tohoto protokolu významně závisí na vzájemné synchronizaci času protistran a krátké životnosti tiketů. Na základě přiděleného tiketu jsou uživateli též přidělovány autorizační práva.



Obr. 19.1 Trojhlavý pes Kerberos – strážce podsvětí



Obr. 19.2 Komunikace klienta s KDC



Obr. 19.3 Komunikace klienta se serverem

Šifrované síťové protokoly

SSL, Secure Sockets Layer je protokol, jenž se snaží řešit bezpečnost rodiny protokolů TCP/IP na transportní úrovni. Je to vrstva vložená mezi vrstvu transportní (tj. TCP a aplikační (např. HTTP), která umožňuje zabezpečení komunikace šifrováním a autentizací komunikujících stran. Cílem je poskytnout bezpečný komunikační kanál mezi dvěma stanicemi sítě na úrovni spojení TCP/IP a umožnit bezpečnou implementaci všech běžných protokolů jako TELNET, FTP, HTTP.
Protokol je navržen tak, aby zajišťoval vysokou míru bezpečnosti. Používá kombinaci kryptografie s veřejným klíčem s kryptografií tajným klíčem.

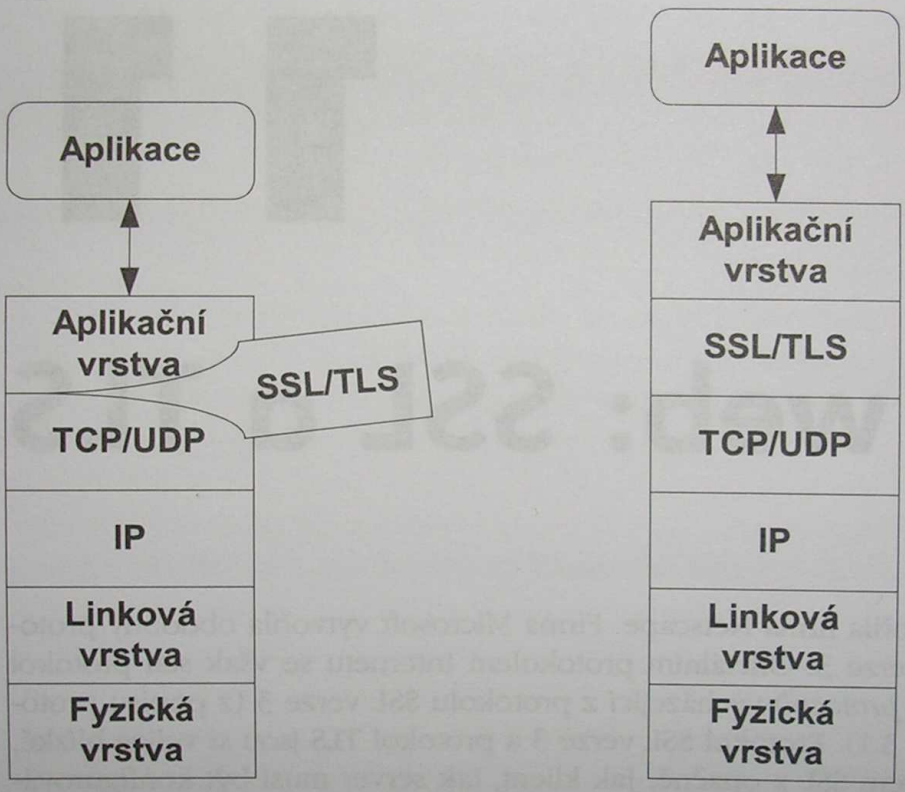
Ustavení SSL spojení funguje na principu asymetrické šifry a používá pro ustavení klíčů relace. Těmito klíči relace je pak zabezpečena samotná komunikace pomocí některého blokového nebo proudového symetrického kryptografického algoritmu. Protokol také zajišťuje vzájemnou kryptografickou autentizaci obou komunikujících stran. Při návrhu SSL byla jako jeden z cílů brána v úvahu i interoperabilita a snadnost rozšiřování protokolu o nové kryptografické algoritmy. Proto pro ustanovení klíče relace může SSL použít nejrůznější algoritmy s veřejným klíčem. Po ustanovení klíče relace je další komunikace zabezpečena zašifrováním některým z mnoha volitelných symetrických algoritmů s tajným klíčem.
Asi nejznámějším protokolem, který byl implementován pomocí SSL, je protokol HTTPS, což je zabezpečená verze protokolu HTTP. Ten se nejčastěji využívá pro bezpečnou komunikaci s internetovými servery. Po vytvoření SSL spojení (session) je komunikace mezi serverem a klientem šifrovaná, a tedy zabezpečená.
Následovníkem SSL je protokol Transport Layer Security (TLS).

Ustavení SSL spojení (SSL handshake, tedy „potřásání rukou") pak probíhá následovně:

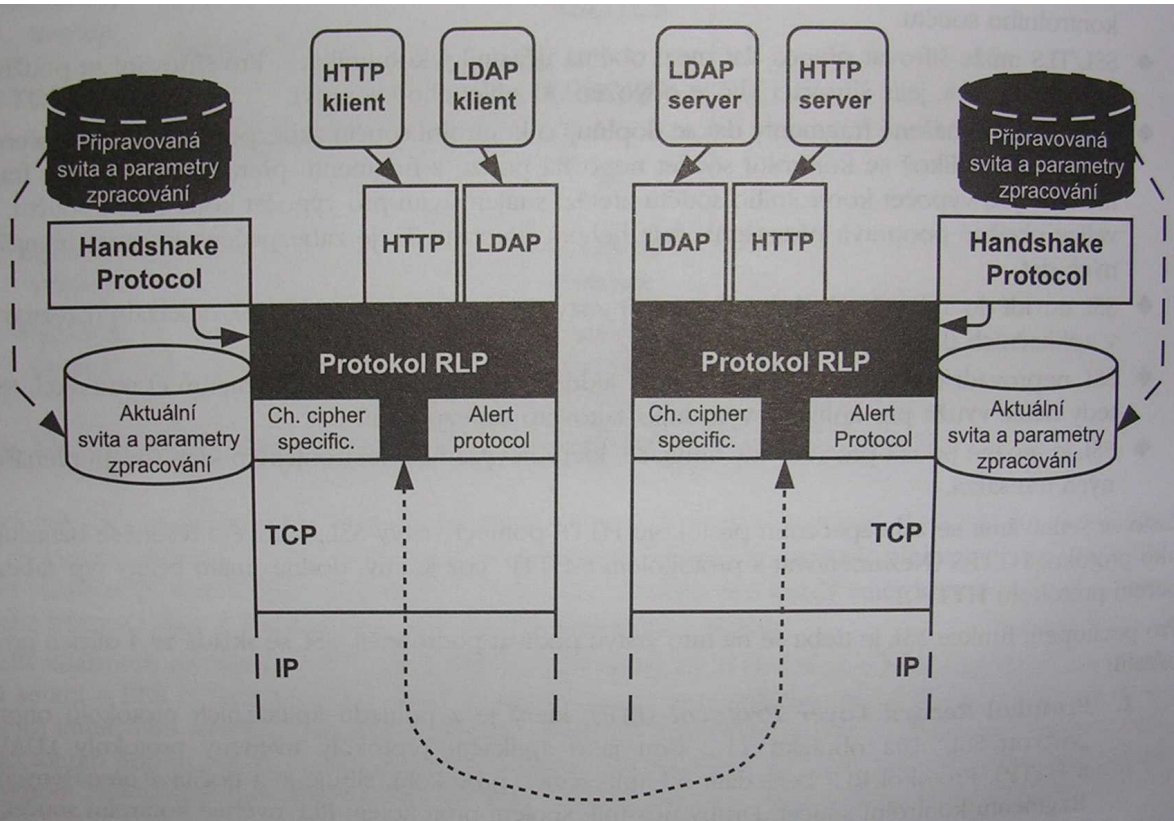
- Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.).
- Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací a hlavně certifikát serveru.
- Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru.
- Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude šifrovat následná komunikace. Ten zašifruje 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 symetrickým šifrovacím algoritmem a vygenerovaným šifrovacím klíčem.
- Aplikace od teď dál komunikují přes šifrované spojení.

Během první fáze ustanovení bezpečného spojení si klient a server dohodnou kryptografické algoritmy, které budou použity. V dnešní implementaci jsou následující volby:

- pro výměnu klíčů: RSA, Diffie-Hellman, DSA nebo Fortezza
- pro symetrickou šifru: RC2, RC4, IDEA, DES, 3DES nebo AES
- pro jednocestné hašovací funkce: MD5 nebo SHA



Obr. 11-1 Vrstva SSL (resp. TLS) se vkládá mezi aplikační vrstvu a protokol TCP



Obr. 11-2 Soustava protokolů SSL (resp. TLS)

SSH (Secure Shell) je v informatice označení pro program a zároveň zabezpečený komunikační protokol v počítačových sítích, které používají TCP/IP. SSH byl navržen jako náhrada za TELNET a další nezabezpečené vzdálené shelly (rlogin, rsh apod.), které posílají heslo i veškerou další komunikaci v nezabezpečené formě a umožňují tak jejich odposlechnutí při přenosu pomocí počítačové sítě. Šifrování přenášených dat, které SSH poskytuje, slouží k zabezpečení dat při přenosu přes nedůvěryhodnou síť, jako je například Internet.
SSH umožňuje bezpečnou komunikaci mezi dvěma počítači, které se využívá pro zprostředkování přístupu k příkazovému řádku vzdáleného systému, kopírování souborů a též jakýkoliv obecný přenos dat (s využitím síťového tunelování). Zabezpečuje autentizaci obou účastníků komunikace, transparentní šifrování přenášených dat, zajištění jejich integrity a volitelnou bezeztrátovou kompresi. Server standardně naslouchá na portu TCP 22.
Aktuálním internetový standardem je od roku 2006 protokol SSH v2.

PGP, Pretty Good Privacy (dost dobré soukromí) je počítačový program a protokol, který umožňuje šifrování a podepisování. To je založeno jednak na algoritmu RSA pro asymetrickou kryptografii a druhak symetrické šifře IDEA. Kromě IDEA bývají použity ale i jiné algoritmy. První verze PGP byla uvolněna Philem Zimmermannem v roce 1991. Další verze byly vyvíjeny Philem Zimmermannem i jinými subjekty. Existuje komerční implementace PGP i volně šiřitelná open-source verze GPG (GNU Privacy Guard).

PGP mělo takový vliv, že bylo standardizováno, aby byla umožněna spolupráce mezi různými verzemi PGP a podobného software. PGP bylo přijato jako internetový standard pod názvem OpenPGP. Nyní se jedná o otevřený standard dodržovaný PGP, GnuPG (GNU Privacy Guard nebo také GPG), Hushmail, Veridis, Authora a jinými.

Nejčastěji se setkáváme s použitím při šifrování e-mailů. Pro tento účel existuje mnoho pluginů, které umožní práci s PGP většině e-mailových klientů.

IPsec (IP security) je bezpečnostní rozšíření IP protokolu založené na autentizaci a šifrování každého IP datagramu. V architektuře OSI se jedná o zabezpečení již na síťové vrstvě, poskytuje proto transparentně bezpečnost jakémukoliv přenosu (kterékoliv síťové aplikaci). Bezpečnostní mechanismy vyšších vrstev (nad protokoly TCP/UDP, kde pracují TLS/SSL, SSH apod.) naproti tomu vyžadují podporu aplikací.

Základní protokoly IPsec (jsou často používány zároveň, protože se vzájemně doplňují) jsou:

Authentication Header (AH) – zajišťuje autentizace odesílatele a příjemce, integritu dat, ale vlastní data nejsou šifrována. Při použití AH každý paket obsahuje zvláštní hlavičku, která obsahuje autentizační informace, následované daty samotného protokolu.

Encapsulating Security Payload (ESP) – přidává šifrování paketů, přičemž vnější hlavička není nijak chráněna a není zaručena její integrita. Protokolem je tedy zajišťována důvěrnost přenášených dat. Stejně jako u AH je k paketu protokolu IP připojena dodatečná hlavička, která obsahuje bezpečnostní parametry a pak následují zašifrovaná data. ESP používá dva režimy činnosti. V transportním režimu obsahuje ESP paket data některého z vyšších protokolů, jako je například TCP protokol nebo UDP protokol. V tunelovacím režimu obsahuje ESP paket pouze datagram na úrovni protokolu IP.

Protokol IPsec má několik nevýhod a problémů. IPsec neobsahuje žádné automatizované

prostředky pro správu kryptografických klíčů. Kryptografické klíče jsou obvykle distribuovány manuálně, což nelze považovat za vyhovující. Při praktickém používání protokolu je třeba použít jak AH, tak ESP. Pokud je použit pouze jeden z těchto protokolů, je IPsec náchylný k některým typům kryptografických útoků. Přes tyto nedostatky je však tento protokol možno při zachování jistých bezpečnostních zásad bezpečně používat.

Bezpečnost ukládání dat

Pro zabezpečení uložených dat je možno využít mnoho dostupných šifrovacích nástrojů. Jedním z nich, který je velice propracovaný a volně dostupný je program TrueCrypt.

TrueCrypt je open source nástroj pro OTFE (On The Fly Encryption - transparentní šifrování za běhu) šifrování obsahu dat na disku pro operační systémy Microsoft Windows, Linux a Mac OS X. Nástroj umožňuje vytváření virtuálních disků v podobě souboru, který lze snadno připojit a pracovat s ním jako s jakýmkoliv jiným pevným diskem (HDD), nebo je možno zašifrovat celý diskový oddíl. Šifrování/dešifrování probíhá transparentně při zápisu/čtení z disku na pozadí a uživatel se nemusí o nic starat. K souborům lze po připojení jednotky k souborovému systému počítače přistupovat běžným způsobem, což se stane až po zadání hesla - šifrovacího klíče. V případě, že je médium chráněno proti zápisu, tak disk bude připojen, ale nebude umožněno na něj zapisovat.

TrueCrypt podporuje více šifrovacích algoritmů, v současné verzi je možné vytvořit virtuální disky s algoritmy AES, Twofish, Serpent a jejich kombinacemi AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES a Twofish-Serpent. Dříve bylo možno využít i šifrování s algoritmy Blowfish, DES, Triple DES a CAST-128. Nicméně dříve vytvořené soubory a jednotky je nadále možné připojit a pracovat s nimi.

Uživatel má na výběr ze tří hashovacích algoritmů: RIPEMD-160, SHA-512 a Whirlpool. Ty jsou využívány pro tvorbu prázdné výplně pro skrytí šifrovaných dat (viz. steganofrafie).

Vypracoval: Petr Manoušek pro účely studia v uzavřeném kruhu studentů ČVUT-FEL
Použité zdroje: Velký průvodce protokoly TCP/IP - Bezpečnost, Wikipedia, zpravodaj ÚVT MU
Poslední revize: 2011-11-27