

PA159 – Bezpečnost na síti II

2. 11. 2007

Autentizační protokoly

- PAP (RFC 1334)
 - slabá autentizace
 - plain-text hesla přes síť
 - * Předpokládal přístup přes telefon přímo k autentizačnímu serveru
- CHAP (Challenge Handshake, RFC 1994)
 - Challenge-response
 - Neposílá hesla přes síť
 - Obě strany znají otevřené heslo
 - Používá MD5 (sdílené_heslo—autentizační požadavek)

Autentizační služby

- Služba pro autentizaci (a případnou následnou autorizaci) přístupu
- TACACS, Terminal Access Controller Access Control System (RFC 1492)
- RADIUS, Remote Authentication Dial In User Service (RFC 2865)

TACACS

- Původně pro autentizaci volaných modemů
- Autentizaci neprovádí terminál server, ale autentizační server (služba pro více terminál serverů/modemů); uživatel přímo s autentizačním serverem nekomunikuje
- Zahrnuje i autorizaci: *Uživatel Jan smí linku použít jen v úterý od 10:00 do 16:00.*
- Klient používá pro komunikaci UDP port 49 nebo lokálně dohodnutý TCP port
- Analogie PAP protokolu pro vlastní autentizaci

RADIUS

- Postaven na principu challenge-response
 - Integrovatelný i s PAP, kde login/heslo je požadovaná „response“
- Hierarchická struktura
 - Může použít jako klient další RADIUS servery
- Používá UDP
 - Transakční protokol, zajištění ve vyšších vrstvách
 - Musí umět použít záložní server
 - Jednodušší implementace (bezstavový server)
- Rozšiřitelný protokol
- Podpora mobility

Distribuce klíčů

- Základní problém: Komu patří (veřejný) klíč K?
- Důvěryhodný prostředník (trusted intermediary):
 - Symetrické klíče: Key Distribution Center (KDC)
 - Asymetrické klíče: Certifikační autorita (CA)
- Příklad KDC: Kerberos (RFC 1510)
 - Kerberos authentication server

Certifikační autorita

- Podepisuje veřejné klíče
- Registrační autorita
 - Kontrola totožnosti: asociace entita × klíč
 - Potvrzenou asociaci předává CA
- Chráněný soukromý klíč CA
 - Používán na podpis asociace entita × klíč
- Revokace klíčů

Bezpečný e-mail

- **Bezpečnost na více vrstvách**
 - více různých požadavků: přenos vs. autentizace příjemce i odesilatele
- **Požadavky:**
 - zabezpečená komunikace
 - integrita zpráv
 - autentizace odesilatele i příjemce

Bezpečný e-mail – realizace

- Symetrická kryptografie: distribuce klíče
- Asymetrická kryptografie: problém šifrování velmi dlouhých zpráv
 - Klíče seance (session keys)
 - * jednorázový symetrický klíč
 - * asymetricky zašifrován
 - * dešifrován příjemcem
- Použití hash funkcí pro zajištění integrity

PGP

- Pretty Good Privacy

- Původně Phil Zimmermann (1991)
- Sloužil jako de-facto standard pro šifrování pošty

- Garantuje:

- Šifrování zprávy symetrickým klíčem (CAST, 3DES, IDEA)
- Autentizaci uživatele pomocí asymetrické kryptografie (RSA)
- Integritu zprávy hash funkcí (MD5, SHA)
- (v podstatě poskytuje digitální podpis)

- Šíření klíčů: Web of trust

- Já určuji, do jaké míry získanému veřejnému klíči věřím
- Já určuji, komu věřím, že mi sděluje důvěryhodné klíče

SSL – bezpečnost v komerčním světě

- Secure Socket Layer
- Poskytuje:
 - Autentizace serveru
 - Autentizace klienta
 - Šifrování zprávy (SSL session)
- Základ pro TLS (Transport Layer Security, RFC 2246)
- Zabezpečená *cesta* (na rozdíl od jednotlivých zpráv/paketů)

SSL handshake

- **Postupné kroky:**

1. Prohlížeč pošle číslo verze SSL a preferované šifrovací protokoly (pro dohodu mezi serverem a prohlížečem)
2. Server pošle číslo verze SSL, preference šifrovacích protokolů a svůj certifikát
3. Prohlížeč zkontroluje certifikát. Pokud kontrola neproběhne (uživatel akceptuje neznámý certifikát resp. certifikát podepsaný neznámou CA), pak komunikace není autentizována.
4. Prohlížeč vygeneruje symetrický klíč a zašifrovaný jej pošle serveru. Současně pošle zprávu, že tímto klíčem bude dále šifrovat.
5. Server akceptuje klíč a potvrdí, že jím bude nadále šifrovat.

- **Zprávy šifrovány symetrickým klíčem (klíč seance)**

- **Umožňuje znovupoužití – handshake má určitou dobu platnosti**

Secure Electronic Transactions, SET

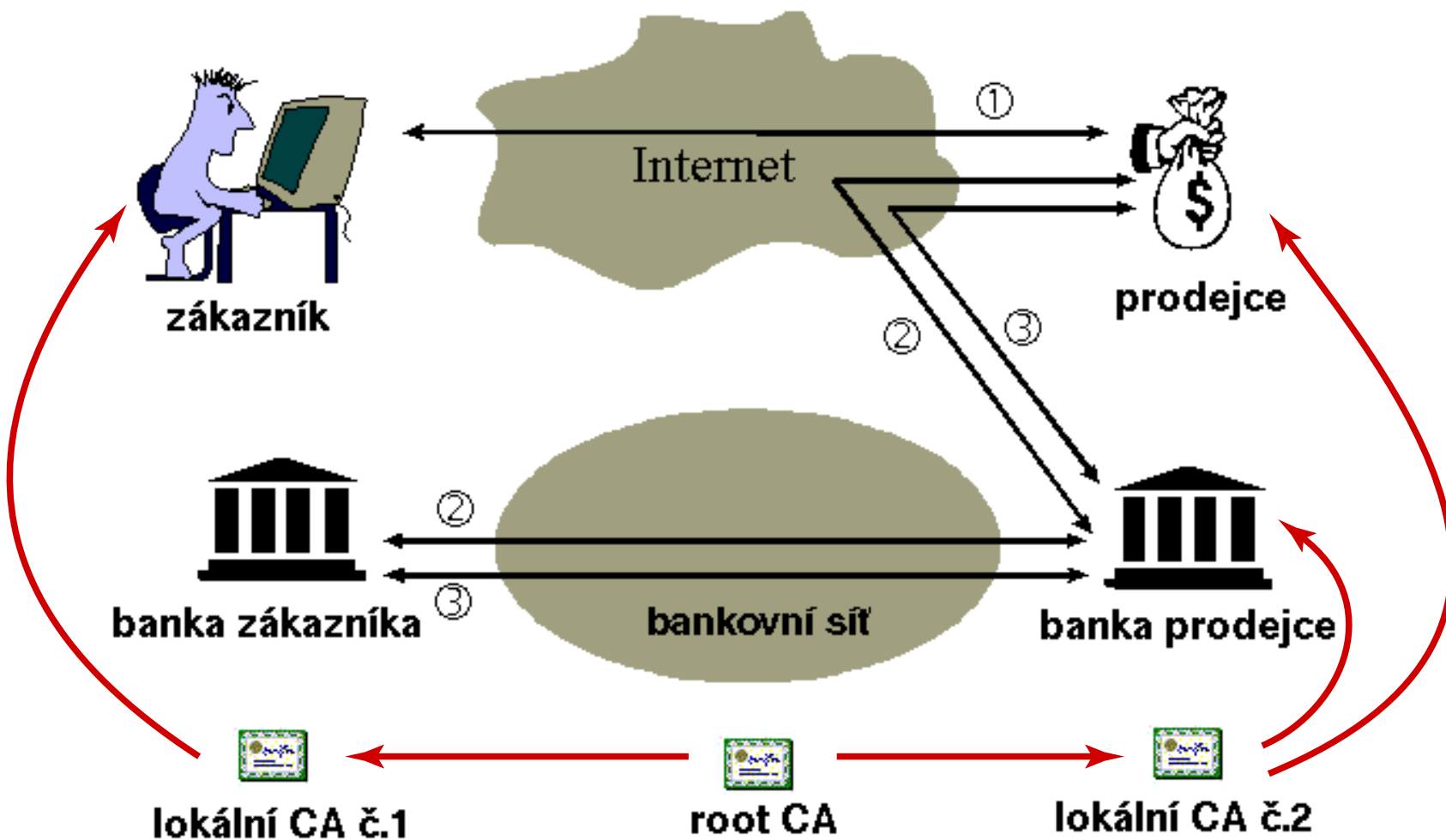
- Speciální protokol pro platby, není vhodný pro obecné šifrování dat
- Určen pro zajištění anonymity
 - Obchodník nemusí znát identitu plátce, stačí mu garance banky
- Komunikace mezi třemi komponentami:
 - Nakupující, resp. jeho elektronická peněženka
 - Obchodník, resp. jeho server
 - Banka, resp. její brána
- Každý ze zúčastněných má certifikát
 - SET přidává sémantiku konkrétním polím

SET – základní komunikace

- Náčrt protokolu
 - Obchodník požádá banku o garanci na konkrétní platbu
 - Nakupující prostřednictvím obchodníkovy terminálu předloží bance svou peněženku a ta z ní vyjme příslušnou částku; případně částku odečte z jeho účtu v bance
 - Banka potvrdí obchodníkovi platbu
- Obchodník se nedostane do styku s identitou zákazníka



Secure Electronic Transactions



IPsec

- Bezpečnost na síťové vrstvě
- Několik desítek RFC, základní 2401 a 2411
- Základní protokoly
 - Authentication Header (AH), RFC 2401
 - * Autentizace odesilatele a příjemce
 - * Integrita dat
 - * Data nejsou šifrována
 - Encapsulation payload security (ESP), RFC 2406
 - * Přidává šifrování paketů

IPsec – Security Agreement

- IPsec vytváří logické kanály, zvané *security agreements*, SA
- Vždy jednosměrné (dva SA pro duplex)
- SA je definován
 - Identifikátorem protokolu (AH nebo ESP)
 - Zdrojovou IP adresou kanálu
 - 32bitovým identifikátorem spojení (Security Parameter Index, SPI)

AH protokol

- Další hlavička mezi IP a TCP/UDP hlavičkou
- IP protokol č. 51
 - Příjemce z něj pozná, že musí zpracovat AH
- Pole AH
 - Next header: říká, co následuje za protokol
 - SPI
 - Sekvenční číslo datagramu
 - Pole autentizačních dat: digitální podpis datagramu

ESP protokol

- Nejen hlavička, ale i vlastní data jsou chráněna
- Přidává také „na konec“ (ocas):
 - ESP Trailer
 - ESP Auth (poslední část ESP datagramu)
- IP protokol č. 50
- ESP Header neobsahuje Next header
 - Ten je uložen v ESP traileru
- Šifrován původní datagram plus ESP trailer
 - Používá DES-CBC

IPsec a distribuce klíčů

- Internet Key Exchange (IKE, RFC 2409)
- Internet Security Association and Key management Protocol (ISKMP, RFC 2407, 2408)
 - Definuje postupy pro sestavení a zrušení SA

Ochrana sítě, dat a uživatelů

- Komplikovaný problém bez jednoduchého řešení
 - Autentizace a šifrování pouze technickým základem
 - Podstatné organizační a
 - sociální aspekty
- Člověk zpravidla nejslabším článkem (sociální inženýrství)

Hrozby

- Získání přístupu k soukromým datům
- Modifikace soukromých i veřejných dat
 - včetně zrušení či odstranění informací
- Nežádoucí zasahování do provozu
 - až po zrušení služeb (Denial od Service)

Ochrana proti zneužití

- Fyzická
 - Zabránění přístupu
- Programová
 - Autentizace
 - Šifrování
 - Synchronní zásah (monitorování provozu a okamžitá reakce)
 - * Intrusion detection system (IDS)
- Právní
 - Definice *žádoucího a nežádoucího* chování

Firewally

- V podstatě logické odpojení od Internetu
 - „Vnitřní“ a „vnější“ síť
 - Povoluje jen určité služby (zpravidla formou otevřených/zavřených portů)
 - Oboustranný blok
- NAT (Network Address Translation)
- Filtr paketů
- Aplikační brána

NAT

- „Skrývá“ vnitřní síť
 - Vnitřní adresy „neviditelné“ (proto *překlad*)
 - Fakticky rozšiřuje adresní rozsah
 - Udržuje spojení (speciální typ *proxy*)
- Původně reakce na vyčerpání IPv4 adres
- Zpravidla kombinován s filtrováním paketů
- NAT sám o sobě není firewall

Filtrování paketů

- Analyzuje hlavičky každého datagramu
- Kontroluje (zpravidla)
 - Odesílatelovu IP adresu
 - Cílovou IP adresu
 - TCP/UDP výchozí a cílový port („protokol“)
 - Řídící data (ICMP, TCP SYN a ACK, ...)
- Umí zachytit IP spoofing (podvržení interních adres)

Příklad

- Blokování spojení z jedné strany
- Kontrola směru navázání spojení:
 - Akceptuje iniciaci interním uzlem („zevnitř“)
 - Blokuje spojení iniciované externím uzlem
- Možné řešení:
 - TCP ACK pole nastaveno na 0 – blokuje spojení
 - ACK nese číslo prvního „chybějícího“ oktetu, 0 znamená pokus o navázání spojení

Aplikační brána

- Kontrola obsahu datagramů
- Problematické pro šifrovaná data (včetně IPsec)
- Princip *prostředníka* (proxy)
 - Brána se vydává za druhou stranu spojení
- Specifické brány pro konkrétní aplikace
 - web/http, telnet, ...
 - e-mail: kontrola virů, označování možného spamu

Firewally – shrnutí

- Součást komplexní ochrany
 - Není jisté, zda skutečně nutná součást – nejsou všelékem
 - * Řada útoků vedena zevnitř
 - * Zvyšují riziko rychlého šíření nákazy
 - falešný pocit bezpečí
 - interní síť často není dostatečně chráněna
 - uživatelé „zleniví“ (a nejsou informovaní ani proškolení)
 - * Zpravidla zdrojem zpomalení při vysokých rychlostech
 - * „Akceptovatelné“ překonávání firewalů
 - Funkcionalita výborná pro zastavení probíhajícího útoku
 - Aplikační brány: nebezpečí chyb (a ochrana soukromí)
 - Např. falešná detekce virů

Denial of Service

- Základní model útoku
 - Přetížení serveru
 - Zastavení (zhroucení) serveru
- Útok z jediného zdroje
 - Nepříliš nebezpečný
 - Lze zastavit (na nejbližším aktivním prvku)

Distributed Denial of Service, DDoS

- Synchronizovaný útok z více míst
- Těžko rozpoznatelný
 - Jednotliví útočníci mohou mít sami o sobě legitimní požadavky
- Neexistuje univerzální ochrana
- Zastavení vyžaduje spolupráci v rámci sítě

DDoS – ochrana v aktivní síti

- První fází rozpoznání útoku: označení jednotlivých proudů
- Každý směrovač ví, od jakého souseda jdou takto označené pakety
- S každým přijatým datagramem pošle požadavek na zastavení „nahoru“ (proti proudu toku paketů)
- Každý datagram přiblíží zastavení blíže k útočníkovi
- V konečném počtu kroků všichni útočníci zablokováni
 - Kontrolní otázka: Proč nelze vše zastavit na aktivním prvku nejbliže napadenému serveru?

Počítačové viry

- Reprodukující se kódy
 - Často se schopností mutace
- Motivace tvorby (ne vždy jasná)
 - Zpočátku zpravidla možnost „ukázat se“ (před uzavřenou komunitou)
 - Potenciál pro využití (průmyslová a vojenská špionáž, terorismus)
- Ochrana:
 - Lokální: Koncových stanic a serverů
 - V síti: proti šíření – vhodná filtrace na branách/aktivních prvcích
 - Detekce útoků (korelace dat)

Viry – poučení

- Technologie sama nestačí
 - Zpravidla využity dávno známé chyby
 - Nicméně technologie je nezbytná pro zastavení útoku
- Nezbytností operační systémy s přístupovými právy
 - Chyba, pokud běžná práce vyžaduje administrátorské privileje
- Nezbytnou součástí je *výchova uživatelů*
 - „Počítačová hygiena“

Cílené napadení (hacking)

- Snaha získat přístup k síti a/nebo do ní zapojeným zdrojům
- Klukovská zábava („jít sousedovi na hrušky“) až vojenské/teroristické akce
- Využití
 - Přístup k datům a jejich modifikace
 - * krádež identity (kreditní karta a ID)
 - phishing patří do kategorie sociálního inženýrství
 - * změna webových stránek
 - „Nástupní“ platforma pro další činnost (např. DDoS)
 - * Často zneužívány stroje univerzit (rychlé spojení, liberální prostředí, ale především stále noví nepoučení uživatelé)

Ochrana proti napadení

- Řízení a kontrola přístupu na všech úrovních
 - Použití vhodných operačních systémů s ochranou přístupu
- Pravidelná údržba (patche, povyšování, ...)
 - Další součást „počítačové hygieny“
- Monitoring provozu
 - Sledování provozu na síti
 - Sledování procesů na stanicích a serverech
- Výchova uživatelů

Společná ochrana proti útokům

- Nespoléhat na jediný ochranný mechanismus
- Nepodceňovat uživatele
 - Distribuovaný monitoring poučenými uživateli
 - Možnost rychle zastavit útok
- Monitorovat provoz a vyhodnocovat
 - včetně „chytrého“ (nemodifikovatelného) ukládání citlivých dat
- Mít připraveny postupy pro případ rozeznaného útoku