

PB001: Úvod do informačních technologií

Luděk Matyska

Fakulta informatiky Masarykovy univerzity

podzim 2014

- 1 Mobilní systémy
- 2 Bezpečnost/Kryptografie

Mobilní systémy

- Inherentně distribuované
 - Přiměřeně malá zařízení přenášená uživateli
 - Trvale nebo občas připojená do sítě
 - Omezená procesní kapacita
- Klient/server nebo peer to peer model
 - Klient/server lépe přizpůsobitelný dostupnému výkonu mobilních zařízení
 - Nutno ošetřit práci v odpojeném stavu
 - Vyvažování mezi kvalitou připojení a lokálně dostupným výkonem
- Konvergence
 - Růst výkonu malých zařízení (smartphones)
 - Dostupnost a kvalita sítě
 - Sdílení aplikací
 - Často s využitím nemobilního serveru

Senzorové sítě

- Malá (mobilní) zařízení sledující jisté parametry okolí
 - Teplota okolí (požáry)
 - Tlak, vlhkost, ... (budovy, stavby obecně, ale i sledování osob)
- Komunikační zátěž
 - Omezená kapacita baterie
 - Nutné protokoly, které garantují „přiměřenou“ konektivitu, ale nezatěžují baterie
 - Cena výpočtu (vlastnost algoritmu/protokolu) vyjádřena ve Wattech, nikoliv počtu instrukcí
- Bezpečnostní aspekty
 - Senzoru se může útočník fyzicky zmocnit
 - Kompromitace senzoru nesmí ohrozit celou síť

Autentizace a autorizace

- Autentizace
 - Prokázání, že „já jsem já“
- Autorizace
 - Oprávnění přístupu ke službě/zdroji
- Delegace
 - Prokázání, že já mohu vystupovat za někoho jiného

Kryptografie

- Ochrana komunikace
 - Snaha zajistit, že konkrétní zprávu si nemůže přečíst neoprávněná osoba
- Další požadavky na předávané zprávy:
 - Integrita
 - Autenticita
 - Non-repudiability
- Šifrování
 - Zajišťuje pouze „nečitelnost“ zpráv

Symetrické a asymetrické šifry

- Šifrování pomocí sdíleného tajemství
 - Máme *klíč* a algoritmus, ten aplikujeme na zprávu
 - Stejný klíč pro šifrování a dešifrování
 - Je-li klíč delší než zpráva, nelze prolomit (velmi zjednodušeně]
 - Problém distribuce (sdílení) klíče
- Asymetrická kryptografie
 - Máme dva klíče (soukromý a veřejný)
 - Soukromý má jen majitel klíče, veřejný je volně dostupný
 - Oba mohou být použity pro šifrování i dešifrování, ale komplementárně
 - Zpráva zašifrovaná soukromým klíčem je dešifrovatelná pouze veřejným klíčem a naopak
 - Problém, jak prokázat, komu patří konkrétní veřejný klíč

Symetrická kryptografie

- Aktuálně nejpoužívanější AES (Rijndael)
 - Starší např. DES, DES3.
- Klíče délky 128–256 bitů (zpravidla)
- Rychlé algoritmy, snadno programovatelné přímo v hardware
- Použití v autentizaci
 - Nepošlu přímo tajemství (heslo)
 - Jedna strana zvolí náhodné číslo, zašifruje a pošle
 - Druhá dešifruje, provede dohodnutou operaci, znovu zašifruje a pošle zpět
 - Příjemce dešifruje a zkontroluje výsledek
 - Popsaný proces je základem *Challenge-Response* protokolu
- Rizika/problémy
 - Distribuce hesla
 - Kompromitace hesla
 - Vícebodová komunikace

Asymetrická kryptografie

- Nemá jednoduchou analogii v reálném světě
- Používá jednosměrné funkce
- Klíče délky 2048–4096 bitů
- Složité algoritmy, náročná implementace
- Použití v autentizaci
 - Jedna strana zvolí náhodné číslo a zašifruje veřejným klíčem druhé strany
 - Druhá strana dešifruje svým soukromým, provede operaci a zašifruje veřejným klíčem první strany
 - První strana dešifruje svým soukromým klíčem a ověří
 - Pozor: popsany princip pouze jednostranná autentizace
- Rizika/Problémy:
 - Autenticita veřejných klíčů
 - Nevhodné pro šifrování dlouhých zpráv

Digitální podpis

- Využití asymetrické kryptografie
- Hash zprávy – „otisk“ pevné délky
 - MD5, SHA1
 - Otisk je jedinečný pro konkrétní zprávu
 - Z otisku nelze rekonstruovat původní zprávu
- Podpis:
 - Ze zprávy proměnné délky vytvoříme „otisk“ pevné délky
 - Otisk zašifrujeme našim soukromým klíčem – *podpis zprávy*

Digitální podpis

- Využití asymetrické kryptografie
- Hash zprávy – „otisk“ pevné délky
 - MD5, SHA1
 - Otisk je jedinečný pro konkrétní zprávu
 - Z otisku nelze rekonstruovat původní zprávu
- Podpis:
 - Ze zprávy proměnné délky vytvoříme „otisk“ pevné délky
 - Otisk zašifrujeme našim soukromým klíčem – *podpis zprávy*
- Ověření
 - Ze zprávy proměnné délky vytvoříme „otisk“ pevné délky
 - Vezmeme připojený podpis a dešifrujeme jej veřejným klíčem podpisujícího
 - Podpis je pravý, pokud se náš a dešifrovaný otisk shodují
- Princip použitelný i na garanci integrity a autenticity zprávy

Certifikační autorita

- Přiřazení veřejného klíče konkrétní entitě
- CA je institut, který
 - Ověří, kdo je vlastník soukromého klíče k určitému veřejnému
 - Vydá certifikát, tj. potvrzení o této vazbě, které sama podepíše
- Jak věřit klíčům certifikačních autorit?
- Alternativy, např. pgp
 - Ring of trust

Delegace

- Potřebujeme pověřit nějakou entitu, aby mohla jednat našim jménem
- Naivní přístupy
 - sdělíme sdílené tajemství
 - svěříme soukromý klíčnekorektní, nebezpečné a zpravidla jdou proti pravidlům
- Vydáme nový certifikát, který podepíšeme
 - Entita se prokazuje tímto novým (má jeho soukromý klíč)
 - Druhá strana vidí náš podpis pod delegací, proto akceptuje

Kombinace přístupů

- Jak zašifrujeme dlouhou zprávu?
 - Nejspíš symetrickým klíčem (rychlejší, méně výpočetně náročné)

Kombinace přístupů

- Jak zašifrujeme dlouhou zprávu?
 - Nejspíš symetrickým klíčem (rychlejší, méně výpočetně náročné)
- Jak ovšem ten klíč sdělíme druhé straně?
 - Nejlépe využitím asymetrické kryptografie
 - Veřejným klíčem druhé strany zašifrujeme symetrický klíč a přiložíme ke zprávě

Důvěryhodnost

- Proč máme primární a sekundární heslo do informačních systémů MU?
 - Častější použití klíče zvyšuje pravděpodobnost odchyčení/zneužití
 - Některé systémy nemusí používat dostatečně spolehlivé systémy ověření (např. vyžadují poslání hesla)
- Souvisí s důvěryhodností
- Různé druhé strany považujeme za různě důvěryhodné
 - Snažíme se proto používat různé autentizační/komunikační mechanismy
 - Chráníme sdílená tajemství
- Explose sdílených tajemství (loginů a hesel)
 - Vhodný kompromis pouze s několika úrovněmi
- Další přístupy
 - Digitální karty
 - Poskytovatelé identit, federace identit