FAKULTA
INFORMATIKY
Masarykova univerzita

PB001: Úvod do informačních technologií

Luděk Matyska

podzim 2020

Obsah přednášky

Ochrana a bezpečnost

Bezpečnost/Kryptografie

FAKULTA INFORMATIKY
Masarykova univerzita

Ochrana a bezpečnost

- Obecná ohrožení:
  - Přístup (čtení)
    - Nezanechává přímo stopy
  - Zápis (modifikace)
    - Následné využití útočníkem modifikovaných dat
    - Zahrnuje i smazání/přepsání
  - Znepřístupnění služby (denial of service)
- Možné útoky
  - Přihlášení, impersonifikace, ...
  - Trojský kůň
  - Viry

Více o útocích

- Sociální inženýrství
  - Uhodnutí nebo získání hesla
  - Využívá důvěřivosti a naivity lidí
  - Technologie může pomoci jen do jisté úrovně
    - Nutnost koordinované shody dvou či více lidí – 7 klíčů k korunovačním klenotům
    - Kombinace fyzických nástrojů a tajemství (po krádeži karty je třeba ještě získat pin a naopak, samotný pin bez karty není k ničemu)
- Využití technických nedostatků
  - Bezpečnostní „díry“, „zadní vrátka“ apod.
  - Je možné minimalizovat korektními programátorskými praktikami
  - a pravidelnou aplikací záplat
  - Automatizované nástroje pro „ot̓ukání“ systému
- Botnety
  - Sítě již napadených počítačů
  - Využitelné k dalším útokům

Principy návrhu bezpečných systémů

- Zveřejnění šifrovacích a souvisejících algoritmů
- Standardní nastavení = žádný přístup
  - Správce/uživatel musí aktivně rozhodnout, co komu dovolí
- Minimální oprávnění
- Pravidelné kontroly
  - „Díry“, nadbytečná oprávnění, …
- Jednoduchý a uniformní mechanismus
  - Složitost vede k nepochopení a to k chybám
- Úrovně oprávnění
  - Delegace oprávnění na konkrétní akci

Ochrana souborů

- Základní operace:
  - čtení, zápis (včetně vytvoření), smazání, prodloužení a spuštění souboru
- Základní ochrana
  - Různá pro různé operace
  - Specifikace, kdo smí co: Ochranné domény:
    - Skupina, která má stejná práva
    - Statické versus dynamické
    - Např.: Já, moji přátelé, ostatní
    - POSIX (UNIX): user:group:other
    - Možná i jiná schemata

Řízení přístupu k souborům

Access Control List, ACL (seznamy přístupových oprávnění)

- ke každému souboru je připojen seznam přístupových oprávnění
- sestává se z uspořádaných dvojic *(*doména,operace)

Zjednodušená varianta (z UNIXových systémů):

- pouze tři záznamy: *u* uživatel, *g* skupina, *o*: ostatní
- operace:
  - `r`: čtení souboru (čtení obsahu adresáře)
  - `w`: zápis souboru (včetně vytvoření)
  - `x`: spuštění (sestoupení do podadresáře)
- Příklad
  - rw-r-----
  - Uživatel může číst i zapisovat, skupina smí jen číst, ostatní nesmí nic

Řízení přístupu k souborům

Plné ACL:

- libovolný počet záznamů
- více práv: smazání, změna oprávnění…
- negativní záznamy (explicitní odepření operace)
- dynamická dědičnost – propagace změn do podadresářů
- např. AFS, Windows od verze 2000, ext4 s ACL

Řízení přístupu k souborům

Capability List, CL

- Uspořádání podle domén, nikoliv podle souborů
- Schopnost (capability) tj. práva přístupu patří procesu a ten je může:
  - předávat dalším procesům (delegace)
  - modifikovat (degradovat, nemůže rozšířit práva)
  - smazat
- Proces se při přístupu k souboru prokazuje odpovídající schopností
- Možnost transferu schopností mezi procesy: vhodné pro distribuované systémy

Ochrana přístupu uvnitř OS

- Kernel a uživatelský prostor
- Oddělení na hw úrovni
- Každá stránka někomu patří
- Pouze kernel má přístup k hardware
  - Kontroluje práva přístupu
  - Obsluhuje zařízení (pro všechny)
  - Garantuje serializaci přístupu
- Uživatelské procesy používají *volání* kernelu (jádra)
- Korektnost kernelu kritická

Přístup k paměti

- Příslušnost virtuálních stránek k procesu
- Výpadek stránky: nepovolený přístup
- Ochrana
  - Mezi procesem a jádrem
  - Mezi procesy
  - Uvnitř procesu

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: popsaný 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 – dnes již nedůvěryohodné
  - SHA2, SHA3
  - 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 – dnes již nedůvěryohodné
  - SHA2, SHA3
  - 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 klíč

  nekorektní, 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?
  - Některé systémy nemusí používat dostatečně spolehlivé systémy ověření (např. vyžadují poslání hesla)
  - Některé systémy vyžadují přístup k uživatelským heslům
- Souvisí s důvěryhodností
- Různé druhé strany považujeme za různě důvěryhodné
  - Snažíme se proto používat různé autentizační/komunikační mechanismy
  - Chráníme sdílená tajemství

Single Sign On (SSO)

- Explose sdílených tajemství (loginů a hesel)
  - Důsledek aplikace principu omezené důvěry
  - V konečném důseldku méně bezpečné
- „Jedno heslo vládne všem”
  - Delegujeme ověřování hesla na jednu (spolehlivou) entitu
  - Jednotlivé služby jí věří
- Poskytovatelé identit
  - Entity, schopné ověřit autenticitu uživatelů
  - Např. vlastní zaměstnanci, vlastní studenti, ...
- Federace identit
  - Vzájemná dohoda poskytovatel identit
  - Příkladem Eduroam

Phishing

- Konkrétní aplikace **sociálního inženýrství**
- Snaha získat přihlašovací (autentizační) údaje uživatele
  - Podvržení přihlašovací stránky
    - Přes zaslaný e-mail
    - Falešným DNS
- SSO může pomoci ochrannými mechanismy
  - Uživatelé „znají" svou přihlašovací stránku
  - Kontrola chování uživatele při přihlášení
- Klíčové ale zůstává chování uživatele
  - Školení
  - Pozornost při práci s IT systémy