Bezpečnost síťových aplikací

2019/2020

Př 3

Zabezpečení dat “mimo” přenos

- Zabezpečení uložených dat
  - Omezení přístupu, šifrování
- Datová integrita
  - Kontrola kompletnosti, aktuálnosti a nezměněnosti dat
- Důvěryhodnost dat
  - Podepisování data
- Zalohování lokálních dat

Zabezpečení uložených dat

- Omezení přístupu
  - Práva, ACL, viz minulá přednáska
- Omezení rozsahu dat
  - Uchovávat jen potřebé
  - Oddělená uložiště
    - Vývoj
    - Produkce
    - Archiv
    - Záloha

Zabezpečení uložených dat

- Analýza dat z hlediska obsahu
  - Důvěrnost/citlivost dat
    - “Pocitová”
    - Obchodní
    - Zákonná, zákon č. 101/2000 Sb., GRPD
- Omezení rozsahu dat
  - Uchovávat jen potřebné

Zabezpečení uložených dat

- Oddělená uložiště
  - Vývoj
    - Nejdivočejší prostředí, nejzásadnější zdrojové kódy
  - Produkce
    - Aktivní data a data o zákaznících
  - Archiv
    - Neaktuální, “méně” důležitá data – často PROBLÉM
  - Záloha
    - Oddělená od předchozích, verzovaná, na více míst

Zabezpečení uložených dat

- Šifrování uložených dat
  - Šifrování vybraných částí
    - Selektivní výběr, Hesla v soubor/DB, osobní údaje
    - “Base64”, MD5, SHA,... + “Sůl”
  - Šifrování bloků dat
    - Nevybírám jednotlivá data, ale celé soubory / řádky DB
    - GPG/ZIP/RAR/TAR – Problém při ztrátě klíče
  - Šifrování disků
    - Více zatěžuje systém, SW i HW implemetace
  - Šifrování strojů
    - NTB/PC heslo už při svém spustění + vazba na disk

Datová integrita

- Snaha zajistit / ověřit že:
  - Data jsou kompletní
  - Nejsou změněna
  - Jsou od udávaného zdroje
- Řešíme podle druhu dat
  - Integrita systému a jeho částí
  - Integrita dat

Datová integrita - metody

- Kontrolní součty
  - Parita, Modulo, Hammingův kód, CRC
- Hashovací funkce - podepisování
  - Matematická funkce, pevná délka výsledeku
  - Malá změna vstupu tvoří velkou změnu výstupu
  - Téměř nemožné zpětné dešifrování
  - MD5, SHA1, GPG, …..

Datová integrita - metody

- Samodetekující kódy
  - Matematické funkce
  - Například rodná čísla od 1986 jsou VŽDY dělitelná 11
- Žurnálovací funkce
  - Typicky na filesystému
  - Ukládám změny přes mezikrok
  - Ověřuji správnost zápisu

Důvěryhodnost dat

- Snaha ověřit pravost dat na základě metadat
- Snaha určit verzi
- Snaha identifikovat autora

Důvěryhodnost dat

- Kontrola medatat
  - Souborového systému
  - Databázových záznamů
  - Logy z přístupu

```
 stat  ahoj.txt
  Soubor: „ahoj.txt“
Velikost: 88            Bloků: 8         I/O blok: 4096  běžný soubor
Zařízení: fd01h/64769d            I-uzel: 4326236    Odkazů: 1
Práva: (0644/-rw-r--r--)  UID: ( 1000/ brandon)  GID: ( 1000/ brandon)
Přístup: 2016-03-03 00:06:22.866685501+0100
Změna obsahu: 2016-03-03 00:06:22.86665501 +0100
Změna i-uzlu: 2016-03-03 00:06:22.866685501 +0100
Vznik: -
```

Důvěryhodnost dat

- Verzování
  - Identifikace verze přímo v datech
    - Serial v DNS
  - Verzování na souborovém systému
    - Schopnost uchovávat různé verze
    - Zpoděné promazávání journálu
    - Zpožděná replikace

Důvěryhodnost dat

- Otisky dat
  - Tvorba HASH otisku dat MD5, SHA1, GPG
  - Důvěryhodná databáze otisků
    - Na samostatném stroji
  - Pravidelná kontrola
    - Cron
    - Změna inodů
  - Tripware

Důvěryhodnost dat

- Elektronický podpis
  - Ověření pravosti na základě přidaných dat
  - Vlastnosti
    - Autenticita
    - Integrita
    - Nepopiratelnost
    - Časové ukotvení

Elektronický podpis