DATA SYS

Šifrování

Tancuj tak, jako když se nikdo nedívá. Šifruj tak, jako když se dívají všichni!

Martin Kotyk
IT Security Consultnant

Šifrování pevných disků

Don't send the encryption key by email!

Šifrování celého HDD / Full disk encryption (FDE)

- První na trhu v roce 1992
  - https://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software
- Automaticky šifruje celý disk na HW úrovni
  - I po zapojení do jiného počítače zůstává zašifrovaný
  - Přístupný pouze master boot record pro vložení hesla
  - Zranitelnost
    - malware na firmware HDD
    - Cold boot attack
- Filesystem-level encryption
  - Kryptografický filesystem na vrchu hlavního systému
  - Hesla jsou v aktivní paměti jen tehdy, když jsou používána

Šifrování pevných disků

Co je bez šifry, není pevné!

Šifrování HDD do „kontejnerů“ (container)

- Zašifruje složku se soubory do „kontejneru“
  - Ostatní mohou vidět soubory, ale nemohou je spustit
  - Všechny soubory přidané do „kontejneru“ jsou automaticky zašifrovány
  - Jasně nadefinované přístupy pro uživatele, procesy a sady zdrojů

Container vs. Full disk encryption

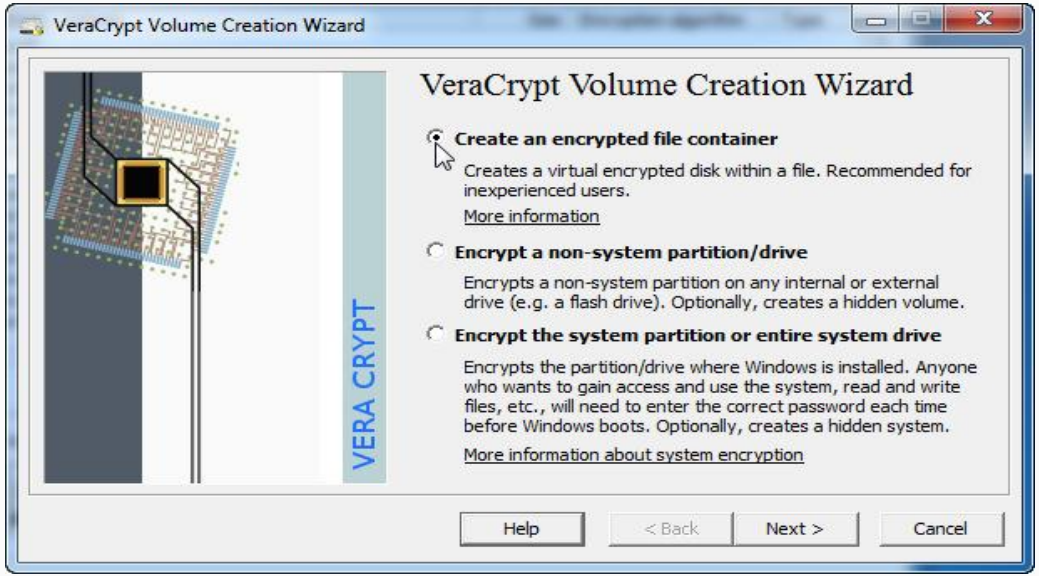
- FDE zabezpečí disk HW, Container ne
- FDE je on/off, Container šifruje kontinuálně
- Container umožňuje kopírovat šifrované časti na přenosná média, FDE ne

Šifrování pevných disků

Bitlocker vs. VeraCrypt

Bitlocker: Slabost zabezbečení: PIN/odšifrováná přihlášením do Windows/ USB

VeraCrypt: Freeware řešení (MacOs, Windows, LINUX)



Šifrování souborů na sdílených discích

Sdílet disk není to samé co sdílet hesla!

- Sdílené disky jsou jackpot
  - locky /2017/ - přes email s doc přílohou, zahesluje files s .locky příponou, a je požadováno výkupné
- Na sdílený disk má přístup X uživatelů
  - Každý individuální heslo
  - Log management
  - Container disk encryption v kombinaci s Full disk encryption
    - Nastavení záleží na tom, jaký je jeho účel ve firmě
  - U disků doporučené rozložení dat
    - Čím víc disků, tím větší šance, že nebudou zničena všechna data

Šifrování databází

Databáze je soubor informací, ze které je pomocí programu možné selektovat potřebná data

- Řešeno na aplikační vrstvě
  - Database abstraction layer (DBAL)
  - Conceptual/Logical level
- Transparent data encryption
  - Zaručená ochrana „neaktivních dat“ v době, kdy se s nimi nemanipuluje
  - Šifruje celou databázi
- Column – level encryption
  - Umožňuje šifrovat databázi po jednotlivých sekcích
  - Každá sekce může mít /a měla by mít/ jiné heslo

Šifrování databází

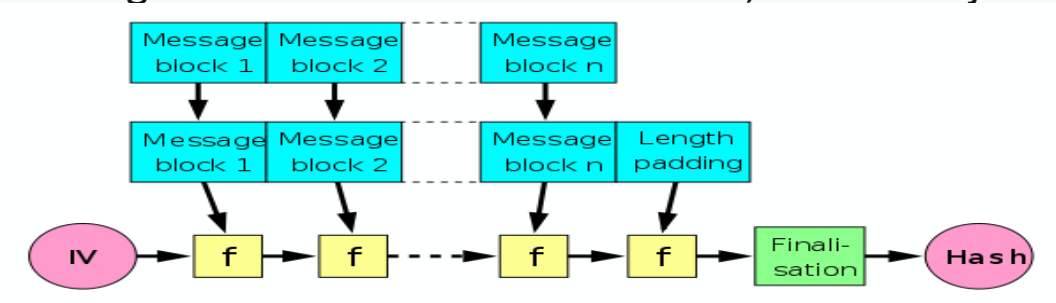
Problematika ochrany klíčů

- Užití klíčů
  - Master key – klíč, který vládne všem klíčům, doporučuje se používat v nouzi
  - Klíče pro uživatele, při column-level encryption mají jasně vymezený přístup
- Hardware security module (HSM)
  - Mezinárodně certifikovaný
  - Bezpečně generuje šifrovací klíče
  - Zajišťuje bezpečnou správu a uložení šifrovacích klíčů
  - Použití šifrovaných a citlivých dat
  - Uvolnění aplikačních serverů pro kompletní asymetrické a symetrické šifrování

Šifrování databází

Salt the Hash

- Hashing
  - Algoritmus mění vložená data na řetězce s pevnou délkou
  - Ideální pro šifrování hesel uživatelů a zajištění autentizace
  - Je nemožné stvořit dva identické hashe
  - Populární SHA 256 (Secure Hash Algorithm)
  - Salting hashes – čím více dat v řetězci, tím složitější šifra



Šifrování USB disků

Ochrana dat!

SW vs. HW

- Software
  - Potřeba udržovat klíče up-to-date
  - Síla ochrany závisí na uživateli
  - Nezastaví brute force hacking
- Hardware
  - Šifrováno speciálním firmware na USB
  - Nepoužívá hostitelskou RAM
  - Šifrování nezávislé na PC

Šifrování USB disků

USB disky slouží pro fyzický přenos dat, je nutné počítat s jejich ztrátou

BitLocker

- Full disk encryption pod Windows

VeraCrypt

- Open source; on-the-fly-encryption

HW:

IronKey; SafeStick; etc.

https://en.wikipedia.org/wiki/Comparison_of_encrypted_external_drives

Šifrování USB disků

USB disky slouží pro fyzický přenos dat, je nutné počítat s jejich ztrátou

- Veškeré počítače jsou pro USB dostupné
  - Vložení USB do neznámého počítače je rizikové
  - USB plní při přenosu virů podobnou roli jako diskety 3,5“
- Po odemčení SW šifrovaného disku se chtěný/nechtěný uživatel dostane k datům na něm uložených
- HW šifrování je silně odolné i vůči dešifrování po krádeži
- Nejen z bezpečnostních důvodů je nutné z USB mazat data, která na nich nepotřebujete mít

Šifrování e-mailové komunikace

Digitální paměť společnosti

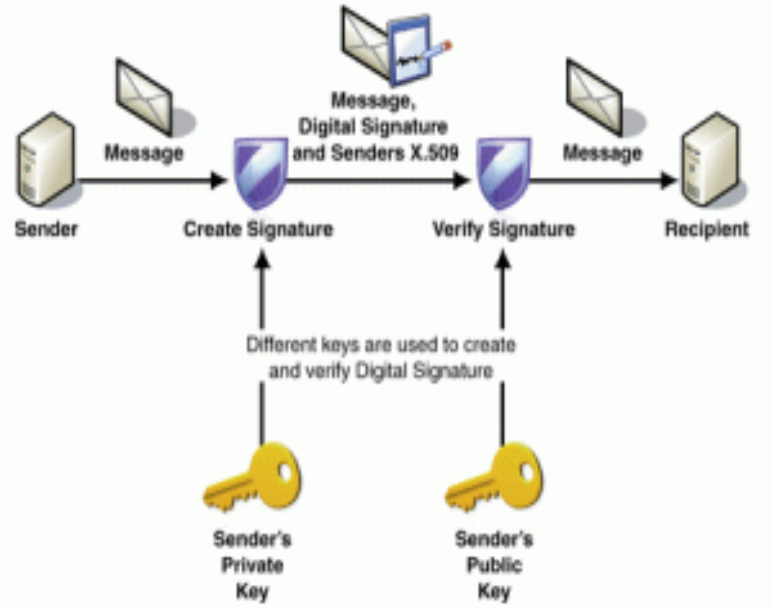
- Autentizace
  - Znalosti /heslo/; Vlastnictví /SW token/; Vlastnost /digitální podpis/
- Autorizace
  - Přístup k počítačovým a síťovým systémům na základě firemní politiky
- Šifrování
  - Zpřístupnění informacím pouze autentizovaným a autorizovaným osobám

X.509

Základní šifra

- X.509
  - Standardní certifikát veřejných klíčů
  - Používá se v TLS

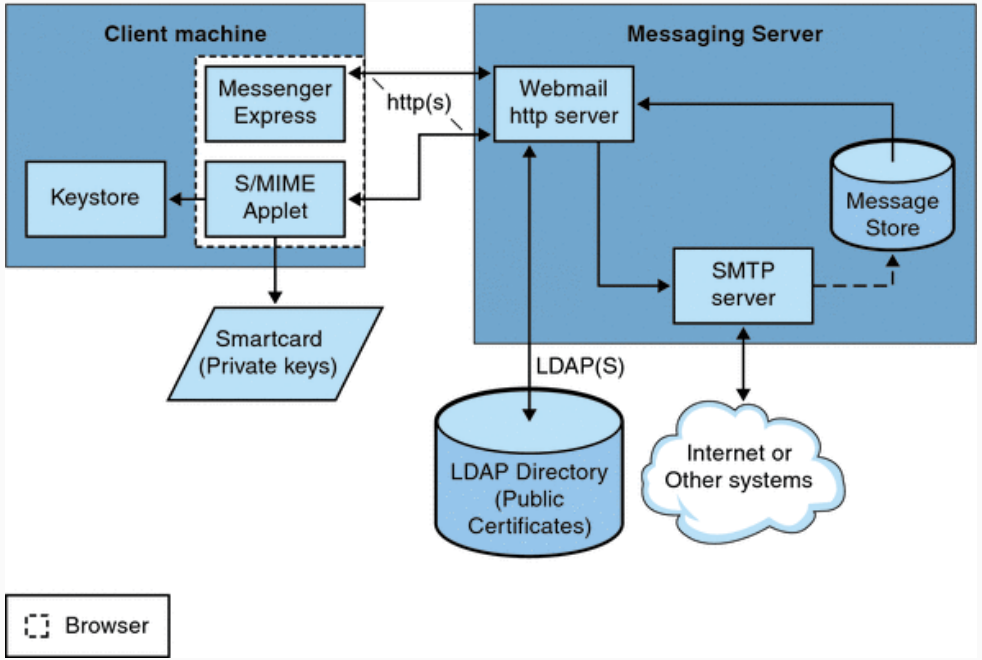
    /Transport Layer Security/
  - Symetrické šifrování
  - Stojí na důvěře v Certifikačních autority



S/MIME

Secure/Multipurpose Internet Mail Extensions

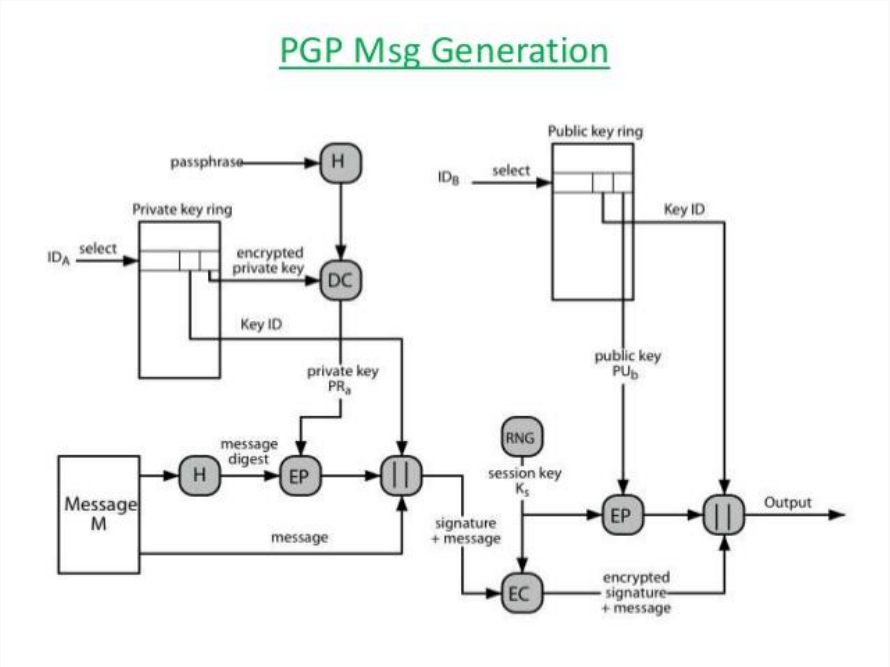
- S/MIME
  - Bezpečnost dat při přenosu
  - Privátní/veřejná certifikační autorita
  - Asymetrické šifrování



PGP

Pretty Good Privacy

- PGP
  - Asymetrické šifrování
  - Čistě P2P komunikace
  - Symetrická a asymetrická šifra
  - Není známo, jak hacknout
  - Periodické obnovy



Přílohy e-mailu

Email mimo VPN je lehce napadnutelný způsob přenosu dat

Šifrování

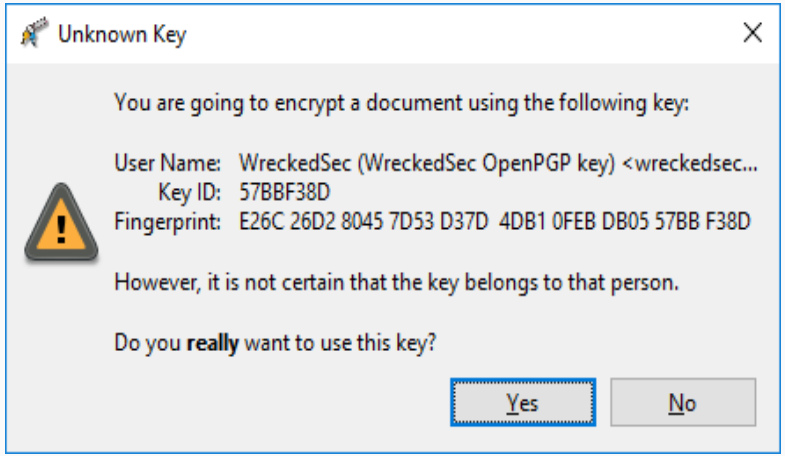
- Přiložené soubory šifrovat zipem /AES – 256/
  - Heslo k zipu poslat pomocí SMS či jiného nezávislého kanálu
  - pdf šifrovat jako takové
  - Spouštěcí soubory bývají detekovány antivirem
    - Splňuje základní příznaky viru:
      - Skrytý soubor
      - Spustitelný soubor
      - Schovaný mezi ostatními

Šifrování komunikátorů

Šifrování mezi známými

- End to End šifrování
  - Nutná důvěra v druhou stranu
  - Ochrana zprávy před externími riziky

    X
  - Ochrana před malwarem v ní obsažené
  - Obojí možná není
- Nutné komplexní zajištění komunikace
  - Mnoho firem nabízí služby
  - Z českých např. Babelnet



Šifrování

5 zásadních otázek

- Šifrujete?
- Chráníte své databáze?
- Šifrujete citlivé emaily?
- Školíte vaše zaměstnance v bezpečném použití komunikačních prostředků?
- Jsou zaměstnanci obeznámeni s možným dopadem malwaru?

Zabezpečení sítě z pohledu ochrany osobních údajů

S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování

Bezpečnost je drahá, ale ne nákladná!