Bezpečnost v IT

10. přednáška

Radek Janoštík

Univerzita Palackého v Olomouci

18. 4. 2024

Outline

- Aktuální (kyber)bezpečnostní situace
- RADIUS
- OAUTH
- Šifrování souborů, adresářů, disků, systému

Aktuální (kyber)bezpečnostní situace

- Sledujete zprávy z dění v kyberprostoru? Co se stalo?
- Eskalace práv v Linuxovém jádře
  - Na první pohled zní děsivě
  - Vždy důležité, jaké jsou podmínky – GSM modul, XEN
- Spectre v2 BHI má novou variantu „native BHI“
  - Linux + CPU intel
  - Čtení libovolné paměti rychlosti $\approx 3.5 kB/s$
- Politický boj o technologie stále trvá – Čína se chce zbavit závislosti
  - Státní firmy a úřady omezit „cizí“ procesory do roku 2027
  - Loni generoval čínský trh 27 % zisku Intelu
- Oblíbený SSH klient Putty měl 7 let zranitelnost
  - Chybná implementace podpisu pomocí *eliptických křivek*
  - Naštěstí postižena jen varianta `ecdsa-sha2-nistp521`

Remote Authentication Dial-In User Service (RADIUS)

- = síťový protokol pro autentizace, autorizaci a správu účtů uživatelů na síti
  - AAA protokol – *Authentication, authorization, accounting*
  - „Kdo se kam, s jakými oprávněními a nastavením může připojit“
- Počátky $\approx$ 1992, RFC-2865, RFC-2866 (accounting)
  - Postupně doplňován o funkcionalitu, zabezpečení (asi 40 RFC)
  - Široce rozšířen, implementován (téměř) všemi výrobci zařízení
- Mnoho implementací serveru (komerční i open-source)
  - Od primitivních – uživatelé v textovém souboru, bez správy účtu
  - Až po komplexní – uživatelé např v LDAP či AD
- Využívá UDP porty 1812 a 1813
- Možnost *Roamingu* – spolupracující organizace umožní autentizaci uživatelů pomocí „jejich“ RADIUS-serveru
  - Přístup uživatelů spolupracujících organizací do jejich sítí (možné jiné nastavení)
  - Např. „náš“ eduroam

RADIUS – Autentizace

- Modelová situace – přístup uživatele(počítače) do Wi-Fi sítě (např. zde na univerzitě)
- V roli RADIUS-klienta není uživatelův počítač, ale AP, ke kterému se chce připojit
  - Počítači ještě není umožněno komunikovat v síti
  - AP od klienta vyžádá jméno a heslo
  - A vyřídí za něj komunikaci s RADIUS-serverem
- AP vytvoří *access request* obsahující ID AP a autentizační data uživatele
  - Odešle jej šifrovaně na RADIUS-server
  - Je možné použít PAP, CHAP, EAP
- Server v databázi ověří správnost údajů a dá AP vědět, co vše může uživatel používat (TCP/IP)
- AP umožní přístup počítači do sítě s daným nastavením
- Obrázek

RADIUS – struktura paketu

- Paket má pro všechny zprávy stejnou strukturu
  - Rozšiřován pomocí *Attribute-value párů*
- 1B – Kód zprávy: `1-Access-Request, 2-Access-Accept, 3-Access-Reject, 4-Accounting-Request, 5-Accounting-Response, 11-Access-Challenge, 12-Status-Server, 13-Status-Client, 255-Reserved`
- 1B – ID zprávy – párování požadavku-odpovědi. Server duplikát (dle IP klienta)
- 2B – délka zprávy
- 16B – Autentikátor
  - Požadavku – XOR sdíleného tajemství klienta a serveru a MD5 hesla uživatele
  - Odpovědi – MD5 z kódu zprávy, ID zprávy, délky, autentikátoru požadavku, z atributu a sdíleného tajemství
- Volitelná délka – atributy(1B typ, 1B délka, hodnota). 64 předdefinovaných atributů

Open Authorization (OAuth) 2.0

- Autorizační framework pro (převážně) webové služby
- RFC-6749 – nahrazuje OAUTH 1.0
- Umožňuje poskytnout webovým službám (některá) data o uživatelích, aniž by služby znaly heslo
  - Delegování (částečného) přístupu k uživatelským datům
- Dnes v Internetu široce používáno (velké firmy jako Google, Facebook, GitHub, . . .)
  - Na webových stránkách možno vidět jako: „Přihlásit se pomocí . . . “ – není čistý OAuth
  - Přístupy k API službám
- Široká podpora ze strany webových frameworků
  - ASP.NET
  - Frameworky pro čtení dat z API

OAuth – delegace oprávnění (obrázek)

- *Klient(webová aplikace)* žádá *uživatele* o autorizaci(udělení přístupu) k jeho datům
- Uživatel oprávnění udělí
- Webová aplikace o uděleném oprávnění informuje *autorizační server*
- *Autorizační server* vytvoří *Access token*, kterým se bude webová aplikace prokazovat
- Webová aplikace přistupuje k *Resource serveru* s Access tokenem
- Resource server ověří platnost tokenu a zpřístupní uživatelova data, ke kterým dal povolení
- Výše zmíněné se reálně děje sérií přesměrování uživatelova prohlížeče

OAuth – autentizace

- OAuth je primárně autorizační protokol
- *Access token* nic neříká o tom, kdo jej používá
  - Pouze uděluje oprávnění ke konkrétním zdrojům
  - Paralela – přístupová karta v hotelu
- Mohou nad ním být postaveny autentizační protokoly
- Doporučuji pročíst: `https://oauth.net/articles/authentication/`
- Podrobnější studium OAuth ponechávám na vaše samostudium

Šifrování dat – motivace

- Na cvičeních jsme si předvedli, že s fyzickým přístupem k nezašifrovanému disku máme přístup prakticky kamkoliv
  - Můžeme číst/měnit data
  - Měnit hesla
  - Dělat vše pod rootem
- Pro rychlý servisní zásah se to hodí, pro počítače s důvěrnými/citlivými/drahými daty to je problém
- V praxi použití hlavně šifry `AES-192, AES-256` (rychlost)
- Možné však použít jakoukoliv šifru
- Možné offline bruteforce útoky (ale relativně pomalé)

Šifrování jednotlivých souborů

- Nic nám nebrání si šifrování naprogramovat sami
  - ⇒ možná chybovost, nízká uživatelská přívětivost
- Použití standardizovaných nástrojů

```
openssl aes-256-cbc -in soubor.txt -out sifrovany
openssl aes-256-cbc -d -in sifrovany -out desifrovany.txt
```

  - Při každé úpravě musím ručně dešifrovat, upravit, zašifrovat
- Lepší je použít standardizovaný formát
  - Šifrované PDF, LibreOffice, . . .
  - ⇒ uživatelská přívětivost

Šifrování adresářů

- Možnost „zabalit“ do archivu a ten šifrovat (např. 7zip)
  - Horší práce, rozbalení změna, zabalení
  - Bezpečné smazání mezikroku
- Windows umožňuje zapnout šifrování pro adresář
  - `Properties→Advanced→Encrypt contents to secure data`
  - Využita RSA
  - Možnost export certifikátu (a privátního klíče)
  - `start→Manage file encryption certificates`
- Linux – připojení šifrované složky pomocí `cryfs`
  - Transparentní práce
  - Výchozí AES-256, podpora více šifer

    ```
    cryfs --show-ciphers
    ```
  - Jak je na tom MacOS?

Šifrování oddílů

- $\Rightarrow$ Po spuštění se OS zeptá na heslo, poté je oddíl korektně připojen
- Transparentní práce
- V Linuxu zažitá praxe: oddělení `/home` od systému
  - Data zašifrována, systém nikoliv (výkon)
  - $\Rightarrow$ pořád možný chroot, nepřečtení dat, snadnější obnova
- Pozor citlivá data mohou být k přečtení v dočasných souborech nebo ve swap
- Linux – LUKS, cryptsetup
- Windows – Start$\rightarrow$ Settings $\rightarrow$ Privacy & security $\rightarrow$ Device encryption
- MacOS – ???

Šifrování celého systému

- Bez správného klíče k oddílům nezačne systém ani bootovat
- Bez spolupráce s UEFI je nutné mít nešifrovaný bootsector
  - Načte se „minimální kód nutný k dešifrování“
  - Poté již může vše řešit systém sám
- Možné zpomalení celého OS (nikoliv jen ukládání dat)
- Horší práce při „recovery“

Windows – Bitlocker

- Komplexní řešení pro šifrování celého systému a dat
- Spolupráce s kryptografickým čipem TPM (Trusted platform module) + UEFI Secure Boot
  - Generování privátních klíčů
  - Hashe HW konfigurace počítače ⇒ automatické odemknutí (+ detekce přepojení „jinam“)
  - Možno fungovat i bez TPM (heslo nebo HW klíč)
- Po zašifrování nezapomenout uložit „klíče pro obnovu“
  - Možnost zálohovat do Active Directory Domain Services
- Pro aplikace je práce transparentní „neví o tom“
- Úbytek výkonu do 10%

Bezpečné mazání souborů

- Co se reálně děje, pokud smažeme nějaký soubor na disku?
- Kvůli rychlosti se pouze odmažou metadata/smaže *inode*
  - „Jedničky a nuly dat“ zůstávají na místě
  - Různými *recovery* nástroje lze některá data získat
  - Často už jen fragmenty
- Je potřeba data reálně přepsat
  - Nástroje, které stejné místo na disku přepíší náhodnými data
  - `shred`, `sfill`, `srm`
  - Spolupráce s filesystémem
  - Komplikace na SSD (proč?)
- Surové přepsání celého oddílu

```
dd if=/dev/urandom of=/dev/sda1
```

  - Některé firmy(PČR) tvrdí, že i přes přepsaní se dá z HDD něco „vydolovat“ (otázka motivace)
  - Vícenásobný přepis

Doporučená četba

- Ciampa M. Security+ Guide to Network Security Fundamentals, Course Technology, Cengage Learning. 2012. ISBN 9781111640170
  - RADIUS
- Hassel J. Radius. O'Reilly Media. 2002. ISBN 9780596003227
- Richer J., Sanso A. OAuth 2 in Action, Manning 2017. ISBN 9781617293276
- `https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/`
  - Bitlocker oficiální dokumentace