Bezpečnost v Linuxu a obecně

SUT

“These security related updates may disable your ability to copy and/or play Secure Content and use other software on your computer.”

-- From the EULA of a 'security update' to Microsoft Windows Media Player.

Ondřej Čečák <ondrej@cecak.cz>

Bezpečnost v Linuxu, Obsah

- co to je bezpečnost
- uživatelé a práva
- hesla a práce s nimi
- bezpečnost software
- bezpečnostní politiky
- časté podvody a útoky

Co to je bezpečnost?

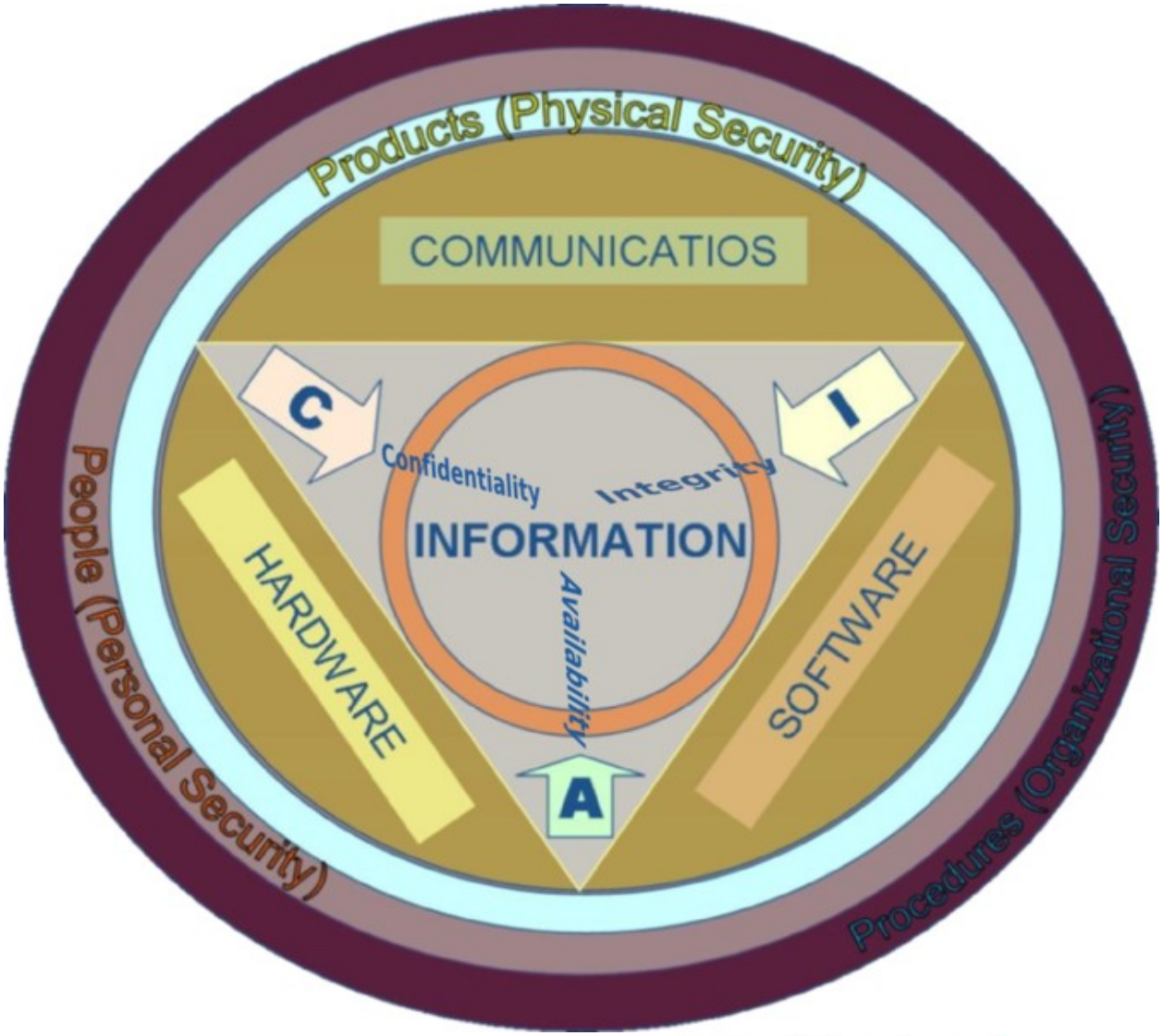
- “Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.”

  -- 44 U.S.C § 3542

Co to je bezpečnost?

- Od dob Julia Caesara nám jde o tyto základní principy (tzv. CIA Triad):
  - utajení
    - chráníme informace před nežádoucím získáním
  - neporušenost
    - chráníme data před nedovolenou změnou
  - dostupnost
    - data musí být dostupná, když jsou potřeba

CIA Triad


Products (Physical Security)
COMMUNICATIOS
C
I
Confidentiality
Integrity
INFORMATION
Availability
A
HARDWARE
SOFTWARE
People (Personal Security)
Procedures (Organizational Security)

Systém uživatelů a práv v Linuxu

- v Linuxu pracujeme s uživateli, kteří jsou typicky sdružováni do skupin
  - o přístupu k datům nebo zařízením je pak rozhodováno na základě identity nebo příslušnosti k nějaké skupině
  - příkazy `chown, chmod`
  - práva nastavujeme až na úroveň souborů

Rozšířená práva

- nativní linuxové filesystémy nabízí kromě klasického konceptu “unixových práv” také pokročilejší ACL (Advanced Control List) s širší možností konfigurace včetně dědění
  - příkazy `setfacl, getfacl`

Superuživatel

- v systému je běžně superuživatel `root`, který má obvykle téměř absolutní vládu nad systémem (obvykle proto, že existují mechanizmy, jak práva superuživatele omezit, například pomocí ultimátního Security-Enhanced Linux)

Superuživatel

- v systému je běžně superuživatel `root`, který má obvykle téměř absolutní vládu nad systémem
- koncept “minimálních potřebných práv”
  - superuživatelský účet využíváme jenom je-li to nezbytně nutné, jak pro správu, tak pro běh aplikací

Heslo a práce s ním

- heslo je základní a přesto zásadní autentizační mechanizmus
  - při dobré volbě hesla a správným zacházením jde o bezpečný způsob ověření
    - jak zvolit?
    - jak je používat?
    - jak a kam zadávat?

Volba hesla

- nesmí být krátké
  - při brute-force attacku je pak rychle zlomitelné

Volba hesla

- nesmí být krátké
- nesmí být moc jednoduché
  - slovníkový útok snadno odhalí existující slova, jména a názvy

Volba hesla

- nesmí být krátké
- nesmí být moc jednoduché
- nesmí být moc dlouhé a složité
  - uživatelé si pak hesla nepamatují a různě si je zapisují, snaží se je měnit na hodně triviální
  - 8 znaků, které tvoří a-zA-Z0-9 a speciální symboly

Volba hesla

- nesmí být krátké
- nesmí být moc jednoduché
- nesmí být moc dlouhé a složité
- ideálně náhodně vygenerované
  - nejlépe zapamatovatelné, jenom pozor, že se zapamatovatelností počítá i útočník

Volba hesla

- ideálně náhodně a dobře vygenerované
  - generovat můžeme například pomocí `apg`

```
$ apg
Please enter some random data (only first 8 are significant)
(eg. your old password):>
hiOlbat2 (hi-Olb-at-TWO)
rudVeen5 (rud-Veen-FIVE)
VeHeuHam9 (Ve-Heu-Ham-NINE)
Glajcowjus9 (Glaj-cow-jus-NINE)
Melcygshem8 (Mel-cygsh-em-EIGHT)
AthHomsh9 (Ath-Homsh-NINE)
```

Top 10 – SSH útoky

- 123456
- Password
- Admin
- Test
- 111111
- 12345
- administrator
- Linux
- Root
- test123

http://www.securityfocus.com/infocus/1876

Jak dlouho trvá zlomit heslo?

- 8 znaků z 26 x 2 + 10 + 4
  - 66 ^ 8 možností ~ 3 e 14
    - útočník zvládne on-line 10 hesel/sekunda
      - 1.141.681 let na vyzkoušení všech kombinací
    - off-line útok v roce 2008 na typickém CPU zkusí 137.438.953.472 možností za hodinu
      - ~ 3000 let na vyzkoušení všech kombinací (kterých je víc)
    - pravděpodobně bude stačit polovina pokusů

Použití hesla

- důležitá je volba různých hesel pro různé služby
  - rozdělením do skupin podle důležitosti, podle provozovatele, podle typu služby
  - motivací je zabránit situaci, kdy cracker prolomením jedné služby získá přístup na všechny naše heslem chráněné služby

Jak a kam zadávat heslo?

- heslo bychom měli zadávat na důvěryhodných systémech
  - ne například v internetových kavárnách s keyloggery nebo na zavirovaných (v tom lepším případě) počítačích známých
  - bezdrátové klávesnice?

Jak a kam zadávat heslo?

- heslo bychom měli zadávat na důvěryhodných systémech
- i při zadávání na bezpečném systému musíme být v pozoru
  - před zvědavým kolegou, vtipně umístěnou kamerou, mikrofonem

Jak a kam zadávat heslo?

- heslo bychom měli zadávat na důvěryhodných systémech
- i při zadávání na bezpečném systému musíme být v pozoru
- hesla zadávat jistě
  - není možné zkoušet různě důležitá platná hesla pro jednu službu

Jak a kam zadávat heslo?

- heslo bychom měli zadávat na důvěryhodných systémech
- i při zadávání na bezpečném systému musíme být v pozoru
- hesla zadávat jistě
- a opravdu na cílový systém!
  - fingerprinty certifikátů, ...

Pozor na uložená hesla

- v konfiguračních souborech
- na nefunkčních discích
- v příkazové řádce jako parametr

Pozor na uložená hesla

- v konfiguračních souborech
- na nefunkčních discích
- v příkazové řádce jako parametr

- ale také pozor na ztrátu hesla

Chyby v software

- nejjednodušší dělení chyb:
  - objevené
  - neobjevené

Chyby v software

- nejjednodušší dělení chyb:
  - objevené
    - od doby objevení do opravy je software potenciálně napadnutelný
    - zneužití známé chyby na kterou existuje chyba je hodně hloupé – software pravidelně updatujeme, informujeme se o bezpečnostních chybách (např. bugtraq) a opravách (z novinek od distributora)
  - neobjevené

Chyby v software

- nejjednodušší dělení chyb:
  - objevené
  - neobjevené
    - může se stát, že se nějaká chyba objeví, minimalizujeme možnost jejího zneužití a dopadu (oddělení služeb a dostupnosti dat, řízení přístupu apod.)

Co chráníme?

- “Bezpečnost je stejně důležitá jako vaše data a jako služby, na které spoléháte.”
  - pozornost věnujeme třeba také zálohování zdroje elektrické energie, konektivity k síti, redundantnosti komponent nebo systémů
  - zkuste si představit, co by se dělo v případě výpadku

Stručná bezpečnostní politika

- správně pracovat s hesly, záplatovat software
- dobře zabezpečit důležitá data nebo je vůbec nezadávat do snadno dostupných systémů
- nepřihlašovat se z nedůvěryhodných systémů, bez ověření protistrany
- nevytvářet body, jejichž ovládnutím získá útočník vše

Zálohování a obnova

- v porovnání s předchozím může být zálohování trochu nudnou záležitostí, ale velmi ho oceníte v případě, že byste bez záloh o data přišli
  - všechna data, která nám za to stojí, musíme zálohovat (pozor na nedůležitá data, živelné katastrofy, dostupnost záloh a vůbec jejich dostatečnou obnovitelnost)

Sociální inženýrství

- uživatel Linuxu se od uživatele Windows nijak zásadně neliší :)
  - pozor na podvodné emaily,
  - telefonáty,
  - pokusy o získání přístupu

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).
United States Marshals Service NCIC entry number: (NIC/ W721460021).

NAME: .....MITNICK, KEVIN DAVID
AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:
Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).
If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102: (24 hour telephone contact) NLETS access code is VAUSM0000.

Form USM -132
(Rev. 3/2/82)

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

November 1992

Trojské koně

- program nebo funkce, která útočníkovi zpřístupní náš systém, nečastěji v “normálním” software
  - používáme pouze software z důvěryhodných zdrojů (repository distribuce, ověřování md5sumů, PGP podpisů, ...)

Fyzický útok

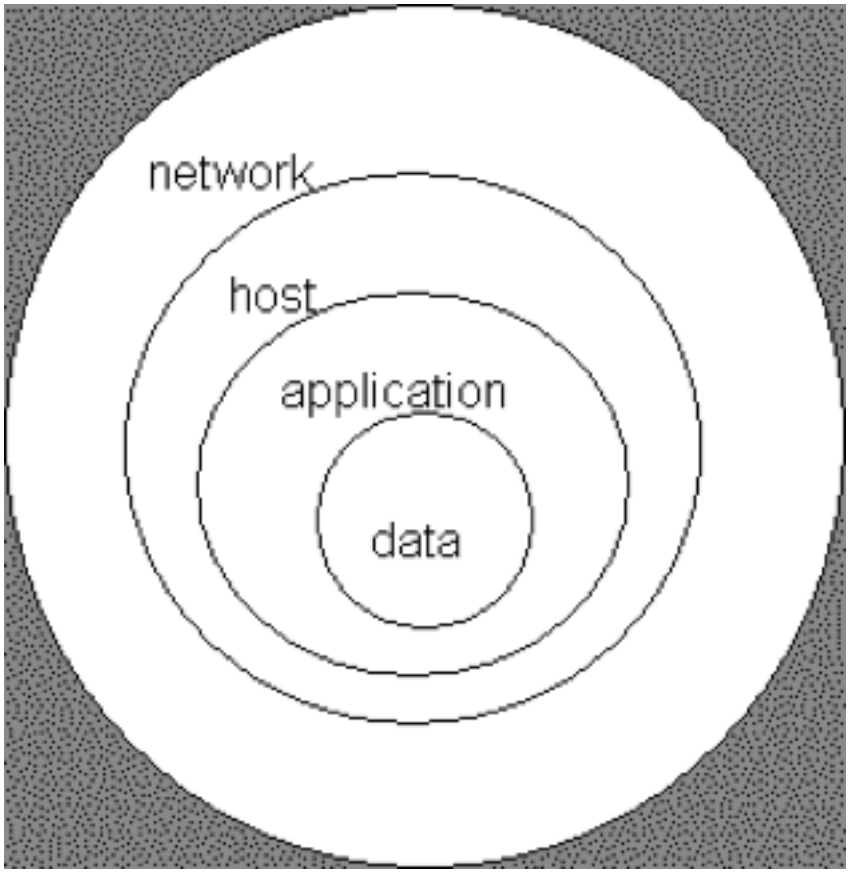
- fyzická bezpečnost je vždy klíčová
  - vyjmutí disku ze serveru
  - boot z vlastního média
  - dostupnost systému vs. lokální bezpečnost (například při šifrování filesystému)

Útoky z venčí

- cílem může být získání lokálního účtu
  - útočník si počká na local-root exploit
  - může využívat systémové prostředky na útoky, rozesílání spamu
- pro vzdálené přihlášení k službám můžeme používat “security through/by obscurity”, ale ...

Obrana v úrovních

- firewall
- tcpwrappery
- autentizace
  - zjištění identity
- autorizace
  - rozhodnutí o oprávnění



... děkuji za pozornost

Použité zdroje:

- Wikipedia [http://www.wikipedia.org]
- Prezentace také dostupná na www.cecak.cz