Bezpečnost síťových aplikací

2019/2020

Př 2

Ověření identity, úrovně oprávnění

- Autentizace
  - Hesla, jednorázová hesla, klíče, Kerberos, LDAP, databáze, Radius
- Autorizace
  - Oprávnění k přístupu, práva, ACL

Autentizace

- Proces ověřující identity
  - uživatele, procesu, serveru, služby …
  - eliminovat možnost podvržení, odhadnutí
  - **Problém “nepohodlí” x bezpečnosti**
- Využívá se k realizaci
  - obecně neznámých informací
  - zdrojů s omezenou dostupností
  - matematických modelů

“Tajný zdroj”

- Využívá neznalosti
  - Existence
  - Lokace
  - Principu přístupu
- Historicky patrně nejstarší metoda
- Odhalitelná sledováním, odposlechem
- http://15.4.6.3:425/~ns/112/Slskw/xs/

Hesla

- Využívá “tajemství”
- Nejčastěji používaná metoda
- Hesla musí splňovat:
  - Minimální délku a složitost

Použité znaky \ Délka hesla		4	5	6	7	8
		Kombinací	Kombinací	Kombinací	Kombinací	Kombinací
		100 hesel/sec	100 hesel/sec	100 hesel/sec	100 hesel/sec	100 hesel/sec
0-9	10 znaků	10 000	100 000	1 000 000	10 000 000	100 000 000
		2 minuty	16 minut	3 hodiny	1 den	11 dní
a-z; 0-9	36 znaků	7311616	380204032	2×10^{9}	8×10^{10}	3×10^{12}
		5 hodin	7 dní	8 měsíců	25 let	900 let
a-z; A-Z; 0-9	62 znaků	14776336	916132832	5×10^{10}	4×10^{12}	2×10^{14}
		2 dny	3 měsíce	18 let	1 000 let	70 000 let
a-z; A-Z; 0-9; ščáéě...;@#$^*?!...	85 znaků	52200625	443705312	3×10^{11}	3×10^{13}	3×10^{15}
		6 dní	1 rok	120 let	10 000 let	800 000 let

Hesla

- Omezenou životnost
- Zamezení opakování a slovníkových výrazů
- Šifrované uložení nebo otisk
- Sůl
  - Náhodnou – musí být někde uložena
  - Pevně danou – vychází z nějakého modulu

Typická hesla

TOP10 - 2016

- 123456
- password
- 12345678
- qwerty
- 12345
- 123456789
- football
- 1234
- 1234567
- baseball

TOP10 – 2017

- 123456
- Password
- 12345678
- qwerty
- 12345
- 123456789
- letmein
- 1234567
- football
- iloveyou

Získání hesla

- Odposlechnutí
  - tcpdump, wiresharek
- Odpozorování
  - Opakovaně vidím heslo zadávat
- Odhadnutí / uhádnutí
  - Na základě znalostí o uživateli
- Nešifrované uložení / slabá šifra
  - Zobrazení v DB, /etc/passwd, .htpasswd

Odposlechnutí hesla

telnet localhost 110

Trying ::1...

Connected to localhost.

Escape character is '^]'.

+OK ewz Cyrus POP3 git2.4.17+0-Debian-2.4.17+nocaldav-0+deb8u2 server ready <1846844126.1519250603@ewz>

user pepa

+OK Name is a valid mailbox

pass pepa

Odposlechnutí hesla

tcpdump -n -X -i lo port 110

23:03:26.874879 IP6 ::1.47623 > ::1.110: Flags [P.], seq 1:12, ack 106, win 342, options [nop,nop,TS val 635787252 ecr 635786464], length 11

0x0000: 6000 0000 002b 0640 0000 0000 0000 0000 `....+.@........

0x0010: 0000 0000 0000 0001 0000 0000 0000 0000 ....

0x0020: 0000 0000 0000 0001 ba07 006e 9680 c9fb ....n....

0x0030: 225f 4a61 8018 0156 0033 0000 0101 080a "_Ja...V.3......

0x0040: 25e5 57f4 25e5 54e0 7573 6572 2070 6570 %.W.%.T.user.**pep**

0x0050: 610d 0**a**

- 23:03:28.897627 IP6 ::1.47623 > ::1.110: Flags [P.], seq 12:23, ack 135, win 342, options [nop,nop,TS val 635787757 ecr 635787252], length 11

  0x0000: 6000 0000 002b 0640 0000 0000 0000 0000 `....+.@........

  0x0010: 0000 0000 0000 0001 0000 0000 0000 0000 ....

  0x0020: 0000 0000 0000 0001 ba07 006e 9680 ca06 ....n....

  0x0030: 225f 4a7e 8018 0156 0033 0000 0101 080a "_J~...V.3......

  0x0040: 25e5 59ed 25e5 57f4 7061 7373 2070 6570 %.Y.%.W.**pass.pep**

  0x0050: 610d 0**a**

Systémy uložení hesel

- Textové soubory /etc/shadow
  - Vždy šifrované!!!!
  - S omezeným přístupem *go-rwxs*
- Databáze
  - SQL, Radius, LDAP, **Kerberos**
  - Může řešit jen hesla nebo i uživatele
    - LDAP x Kerberos

Pozor na zcizení binárních dat!!!

Databáze - SQL

- Libovolný databázový systém
- Účty a hesla jsou uložena v relačních tab-ulkách
- Snadné napojení například na webové služby, poštovní služby
- Ověření pro přístup jménem a heslem
  - Ověření sama v sobě - MySQL

Radius

- *Remote Authentication Dial In User Service*
- Protokol pro přenos informací
  - Autentizace, autorizace, konfigurace, ...
- Umožňuje centrální správu uživatelských učtů
- Snadné propojení s AD
  - role Microsoft Windows Serveru

Radius

- Vysoce bezpečný přenos
- Šifruje na základě sdíleného tajemnství
  - To se NIKDY nepřenáší po síti
- Hesla jsou během přenosu šifrována
  - MD5, SHA1,....
- Hesla v konfiguraci Radiusu NEMUSÍ být šifrována == chyba!
- Typické použití v síťovém ověřování

Radius Linux

……

Address

client 10.0.0.10 {

secret = **TajneHeslo**

shortname = routerXYZ

}

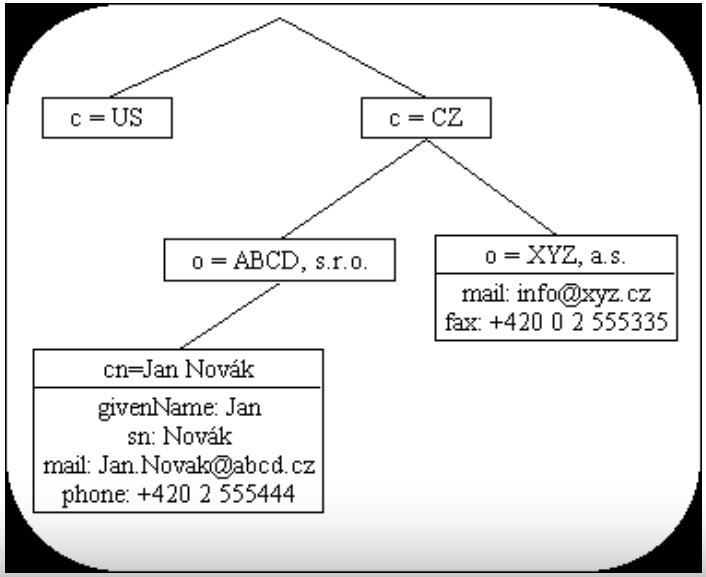
……..

LDAP

- *Lightweight Directory Access Protocol*
- Adresářové služby – dříve např Novel
- Kompletní identifikace uživatele
- Hesla mohou a nemusí být součástí
- Společně s Kerberosem základ MS AD

LDAP

- LDIF záznamy – struktura
- Šifrovaný i nešifrovaná přístup
- Hierarchický model



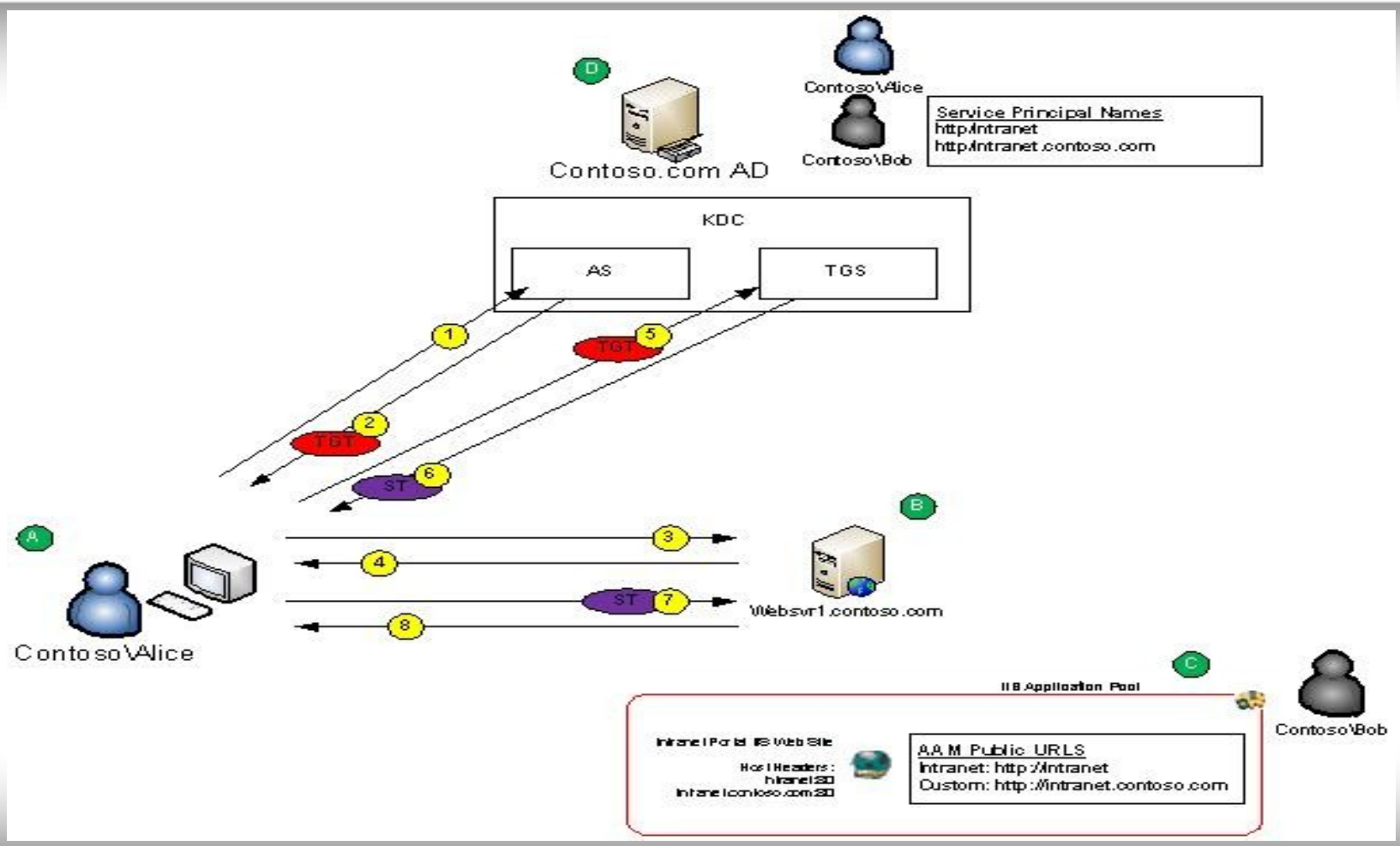
Kerberos

- Autentizační mechanismus
- Vznikl na MIT jako projekt Athena
- Dnes více implementací
  - *MIT, Heimdal, Microsoft*
- Zabraňuje odposlechu a opakovaní
- Heslo není nikdy přenášeno sítí
- Využívá důvěryhoné třetí strany - KDC

Kerberos

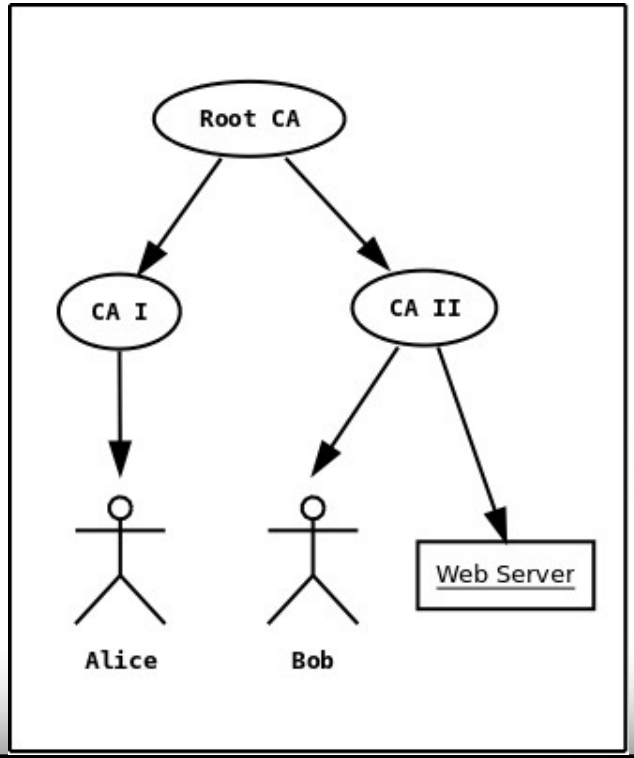
- Používané zkratky
  - AS – autentizační server
  - SS – servisní středisko
  - TGS – řídící server
  - TGT – ticket
- Závislý na relativně přesném času a funkčním překladu jmén
- !!! Pozor ticker jde zcizit !!!

Kerberos



X.509

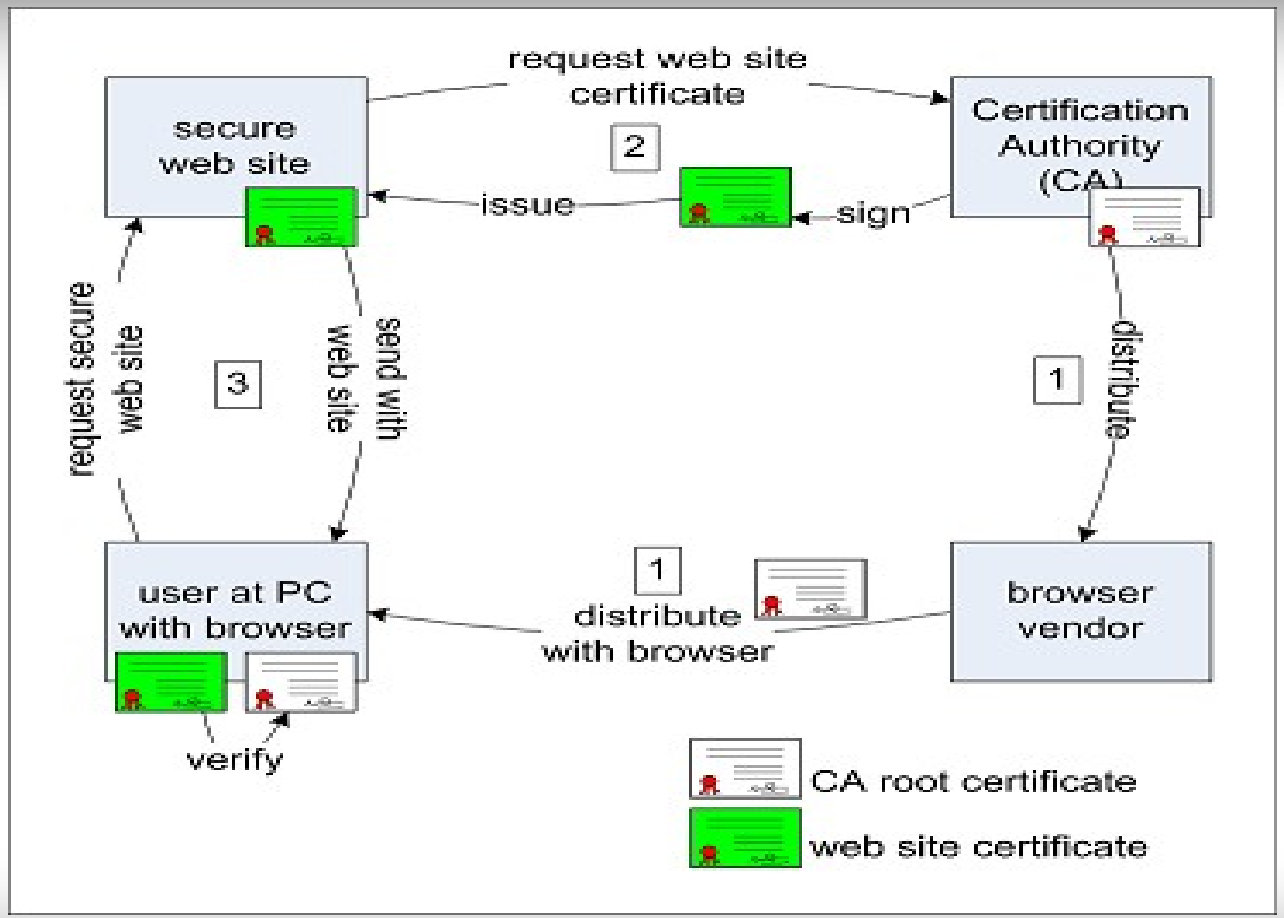
- Standard pro systémy založené na veře-jném klíči - certifikáty
- Aktuální verze v3
- Vychází ze starší X.500
  - Nikdy neimplementováno



Certifikáty

- “Velmi složitá hesla” s přidanou hodnotou
  - Hierarchická organizace
  - Identifikace uživatele
  - Identifikace vydavatele
  - Omezená platnost
  - Možnost zrušit vydaný certifikát
  - Veřejná / neveřejná část

Certifikáty



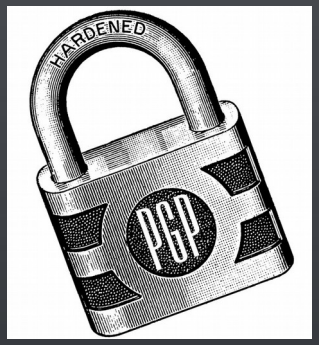
Certifikáty

- Nejtypičtější použití WWW
  - Ověření serveru
- Podpis zdrojových kódů v Java
- Různé úrovně ověření
  - SSL 123
  - SSL Web
  - WildCard
  - Code Signing

Certifikáty

- Různá důvěryhodnost CA
- Nutnost importovat vlastní CA
- Snadné generování přes *openssl*
- Veřený / soukromý vydavatel
  - Thawte, Verisign, Česká pošta, …
  - Let`s Encrypt – budoucnost ??
    - Electronic Frontier Foundation (EFF), Mozilla Foundation, Akamai, Cisco Systems, OVH, Chrome

Pretty Good Privacy



- Založen na asymetrickém šifrování
  - RSA a IDEA / Diffie-Hellman/El Gamal a CAST
- Umožňuje *šifrovat a podepisovat* zprávy
- Vytváří sítě důvěry
  - Sám si podepíšu klíč *A*
  - Pak podepíšu klíč *B*, kterému věřím
  - Pokud *C* je podepsané *B*, věřím mu

Pretty Good Privacy - PGP

- Problém ztráty klíče
- Možnost šifrovat soubory
- Typické při elektronické komunikaci
- Zpráva může být šifrována více uživateli
  - Každý pro koho je jediná zpráva přešifrována ji může přečíst
- Více implemetací
  - PGP, GnuPG, OpenPGP

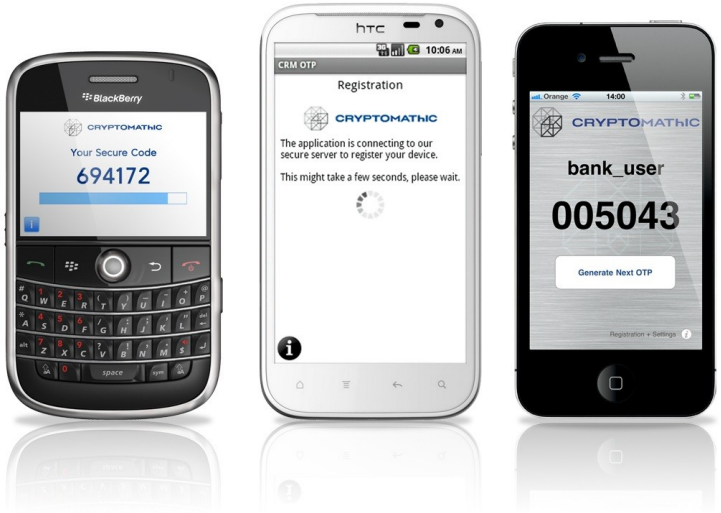
OTP - One Time Password

- “Jednorázová hesla”
- Tajné heslo
  - Bezpečné heslo nebo spíše fráze
- Seed
  - Řetězec 1-16 znaků, generuje server i klient
- Hash funkce SW / HW (klíčenka)
  - heslo+seed se opakovaně použije jako vstup
  - Výsledkem je sada N 1x platných hesel

OTP - One Time Password

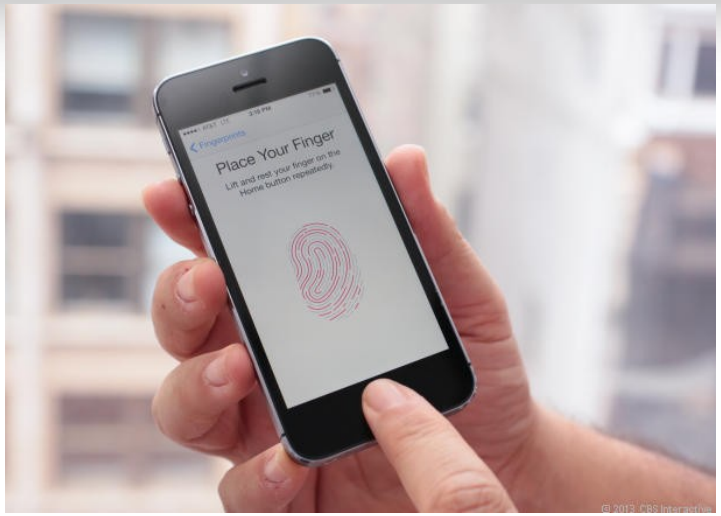
- Nutnost reinicializace
  - Nový seed
- Bezpečnost závisí na hash funkci a hesle
  - MD5, SHA1, SHA256, SHA384, SHA512
- Neřeší odcizení session, man-in-the-midlle
- Úspěšně brání odposlechnutí a opakován

OTP - One Time Password



Biometrické ověřování

- Novinka poslední let
  - Otisk prstu
  - Sken sítnice
  - Sken duhovky
  - Obličej
  - Geometrie ruky
  - DNA
  - Analýza hlasu
  - Dynamika stisku kláves



Násobné ověření

- Více způsobů spojených pro jedno ověření
  - 1. ověření certifikátu – SSL
  - 2. ověření jménem a heslem
  - 3. Odesílání druhé fáze novou cestou SMS, email
  - 4. zpětné zadání obdržených údajů do systému, ktede se autentizuji
- Typicky banky

Násobné ověření

- Vysoká bezpečnost – musím překonat více překážek
- Relativně snadná implementace
  - HTTPS + webform + SMS brána / email
- I zde je riziko zneužití
  - Aplikace v telefonu odchytává SMS
  - *Vždy nutná soudnost uživatele ;)*

Autorizace

- Kontrola oprávnění na základě autentizace
- Neřeší kdo jsem
  - To už vím – autentizace
  - Nemusím vědět – nepřihlášený uživatel
- Zjednodušeně řečeno *práva*

DAC x MAC

- Dva možné přístupy:
  - DAC: Diskreční řízení přístupu
    - klasický model vycházející s ACL
    - Vlastník rozhoduje kdo má práva
  - MAC: Mandatorní řízení přístupu
    - Systém definuje práva objektů
    - Definuju domény – sandboxy
    - Program / uživatel nesmí opustit sandbox
    - Například Meduse, Selinux, GRSec

Unixová práva

- Uživatel, skupina, ostatní
  - *Read* – čtení
  - *Write* – zápis
  - *Execute* – spuštění souborů nebo otevření adresáře
  - *Setuid* – Spuštění s právy vlastníka
  - *SetGid* - Spuštění s právy skupiny / dědění skupiny vlastníci adresář
  - *sTickybit* – každý může tvořit vlastní data

Access Control List

- Rozšíření Unix práv
- Možnost násobných vlastníků na object
- Ne jen na filesystému – cisco ACL
- V rámci filesystému né vždy podporován
  - NE : ext2, fat
  - Ano: ext3,ext4, xfs, ntfs, openafs, ...

SELinux

- MAC systém přímo v jádře linuxu
- Bezpečnostní kontext
  - Identita: user_u,system_u
  - Role: sysadmin_r,system_r,user_r
  - Typ/doména: file_t,default_t,user_home_dir_t
  - Subject: proces / uživatel
  - Object: soubor, adresář, socket

SELinux

- Type Enforcement
  - Object i subject má definovaný typ
  - Funguje na základě přechodu a přístupů
- Přechodová pravidla
  - Soubor: nastavují typy souborů, dědění
  - Proces: definují doménu a její přístupový bod
- Přístupová pravidla
  - Jaký typ má jaká práva na přístup k jinému typu

Kombinace více systémů

- V jednom systému může být více modelů současně
- Záleží pak na prioritě – jak vysoko je vrstva na které práva řeším
  - OpenAFS x Unix perm
  - Unix perm x SELinux