HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

5. előadás – Hitelesítés, engedélyezés, hozzáférés-szabályzás

VIHIBB01 – Kódolás és IT biztonság (2023)

Ládi Gergő

CrySyS Lab, BME
gergo.ladi@crysys.hu

www.crysys.hu

MŰEGYETEM 1782

Alapfogalmak

- Authentication (authentikáció, hitelesítés)
  - Célja, hogy a rendszerrel kapcsolatba lépni kívánó felhasználó azonosítsa magát és hitelt érdemlően bizonyítsa kilétét
  - *"Ki vagy te? (Igazold!)"*
- Authorization (authorizáció, engedélyezés)
  - Célja, hogy a felhasználókkal kapcsolatban meghatározza, milyen objektumokon milyen műveleteket jogosultak elvégezni
  - *"Kinek mihez van engedélye?"*
- Access control (hozzáférés-szabályzás)
  - Betartatja a biztonsági házirendet
  - *"Van engedélyed elvégezni a(z) X műveletet a(z) Y objektumon?"*

Alapfogalmak

- Accounting / Auditing (elszámoltathatóság, auditálás)
  - Célja, hogy naplózzuk a felhasználók által végzett műveleteket
  - Érdemes nem csak a sikertelen, hanem a sikeres műveleteket is naplózni
  - *"Mikor és hogyan éltél (vissza) a jogosultságaiddal?"*

- Az {authentication, authorization, accounting} hármast együttesen **AAA**-nak szokás rövidíteni

```
R1# conf t
R1(config)# username admin secret Str0ngPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local
R1(config)# aaa local authentication attempts max-fail 5
```

Hitelesítés

A hitelesítés formái

- Tudásalapú (knowledge-based) – valami, amit **tudsz**
  - Jelszavak
  - PIN-kódok
- Birtokalapú (possession-based) – valami, ami **nálad van**
  - Mobil eszközök (SMS-ben küldött kódok, tokengenerátor alkalmazások)
  - Offline tokengenerátorok
- Tulajdonságalapú (inherence-based) – valami, ami **vagy**
  - Ujjlenyomat
  - Arc, fül geometriája
  - Retina és írisz
  - Kéz és/vagy erek geometriája
  - Hang
  - Gépelési dinamika

Kétfaktoros/multifaktoros authentikáció (2FA/MFA)

- Sikeres hitelesítéshez kettő (vagy több) hitelesítési módszer egyidejű használatát követeljük meg
  - Például: ha egy támadó megsejti a jelszavunkat, továbbra sem tud belépni, hacsak nem lopja el/fertőzi meg a telefonunkat is

- Ideális esetben a faktorok formában különböznek
  - Pl. az egyik tudást tesztel, a másik birtoklást
- A tipikus megvalósítás: jelszó + mobilos token
- A hitelesítő fél dönthet úgy, hogy adott feltételek teljesülése esetén nem kéri a második faktort
  - Pl. ha ugyanarról a gépről lépek be mint 10 perccel korábban

Hitelesítés

Tudásalapú hitelesítés

Jelszavak

- A leggyakrabban használt hitelesítési módszer
- Előnyök
  - A felhasználók hozzászoktak, jól ismerik a jelszavakat
  - Fejlesztői oldalról könnyen megvalósítható egy jelszavas védelem
- Hátrányok
  - A jelszavakat meg kell jegyezni*
    - » A felhasználók egyszerű jelszavakat fognak használni
    - » Ugyanazt a jelszót több helyen is fel fogják használni
  - A jelszavak könnyen ellophatók
    - » Hálózati forgalom lehallgatásával
    - » Keyloggerek, malware-ek segítségével
    - » Social engineering, shoulder surfing

Jelszavak elleni támadások

- Brute force ("nyers erő") támadások
  - A támadó kipróbál minden lehetséges jelszót
- Szótáras támadások
  - A támadó egy szótár szavait próbálja ki jelszóként
    - » A felhasználók néha egyszerű, szótári szavakat választanak jelszónak
    - » Az interneten elérhetők szótárfájlok a gyakori jelszavakkal
- Hibrid támadások
  - A fenti két módszer kombinációja
  - A támadó először a valószínűbb jelszavakat próbálja ki
    - » Mit tud az áldozatról? (nevek, születési dátumok, …)
    - » Szótár alapon, de mutációkkal (password -> pa$$w0rd)

Jelszavak elleni támadások

Select your Router Manufacturer

CISCO | Find Password

Router Passwords is officially the most updated default router password repository on the internet. To find the default password of your router select the manufacturer from the drop-down and click the Find Password Button.

CISCO DEFAULT ROUTER PASSWORDS

Find all the passwords for your **CISCO** router here.

Router Passwords makes it easy to find your default Router Password – simply look at the table below, locate your model and your username and password is located next to your model number.

Manufacturer	Model	Protocol	Username	Password
CISCO	CACHE ENGINE	CONSOLE	admin	diamond
CISCO	CONFIGMAKER		cmaker	cmaker
CISCO	CNR	CNR GUI	admin	changeme
CISCO	NETRANGER/SECURE IDS	MULTI	netrangr	attack
CISCO	BBSM	TELNET OR NAMED PIPES	bbsd-client	changeme2
CISCO	BBSD MSDE CLIENT	TELNET OR NAMED PIPES	bbsd-client	NULL
CISCO	BBSM ADMINISTRATOR	MULTI	Administrator	changeme
CISCO	NETRANGER/SECURE IDS	MULTI	root	attack
CISCO	BBSM MSDE ADMINISTRATOR	IP AND NAMED PIPES	sa	(none)

Forrás: https://www.routerpasswords.com

Jelszavak elleni támadások

Equifax used default 'admin' password to secure hacked portal

Lawsuit claims firm failed to take even 'the most basic precautions'

Graeme Burton

21 October 2019

EQUIFAX STAFFERS used the default 'admin' username and password to secure a portal containing sensitive customer information.

That's according to a **class-action lawsuit launched against the company in the US**, claiming securities fraud by the company over the 2017 data breach that spilled information on **around 148 million accounts of people in the US, Canada and the UK**.

"This case arises out of a massive data breach incident. The plaintiff alleges that the defendants committed fraud in connection with the data breach that caused a loss in value of [Equifax shares]," claims the lawsuit.

It alleges the company made "multiple false and misleading statements and omissions about the sensitive personal information in Equifax's custody, the vulnerability of its internal systems to cyber attack, and its compliance with data protection laws and cybersecurity best practices".

The lawsuit goes on to claim that the company failed to take even "the most basic precautions to protect its computer systems from hackers".

Forrás: https://www.theinquirer.net/inquirer/news/3082848/equifax-admin-password-hack-lawsuit

Jelszavak védelme – Hashelés

- A plaintext jelszó helyett egy egyirányú függvényen átfuttatott (hashelt) változatot tárolunk az adatbázisban
  - Tipikus hash algoritmusok: SHA-512, SHA-256, SHA-1, MD5
- A felhasználó belépésekor az általa beírt jelszót ismét lehasheljük, és az így kapott értéket összehasonlítjuk az adatbázisban lévő hashsel
- Ha egy támadó ellopja az adatbázist, nem fogja látni a plaintext jelszavakat
  - A hashekkel nem fog tudni belépni más oldalakra a felhasználó nevében
- A hashelés problémái
  - Ha a hash algoritmus ismert, létezhetnek {jelszó,hash} párokról adatbázisok gyenge jelszavakhoz
  - Ha több felhasználónál is ugyanaz a hash érték látható, akkor ugyanaz volt a jelszavuk is -> statisztikai támadások

Jelszavak védelme – Modern megoldások

- Salting (sózás)
  - Hashelésnél nem csak a jelszót használjuk fel, hanem egy, felhasználónként különböző random értéket is
  - Sózás mellett nem éri meg előre kiszámolni hash értékeket
    - » Saltonként más-más adatbázisra lenne szükség
  - A sózás elfedi, ha két felhasználónak ugyanaz a jelszava
- Stretching (nyújtás)
  - Mesterségesen megnöveljük a hash kiszámításának idejét
    - » Lassú vagy memóriaigényes műveletek felhasználásával
    - » Ugyanazon algoritmus sokszori egymás utáni futtatásával
  - Cél: lelassítani a támadókat
- Kulcsderiváló függvények (Key Derivation Function, KDF)
  - A KDF-ek egyszerre használnak erős hash függényeket, sózást és nyújtást
  - A jelszavak "tárolásának" ma is ajánlott módja
  - Példák: PBKDF2, scrypt, Argon2

Jelszavak védelme – Hashelés (esettanulmány)

- 2013-ban feltörték az Adobe egyik szerverét
- *"The breach occurred when hackers raided a backup server on which they found, and subsequently published, a 3.8 GB file containing 152 million usernames and poorly-encrypted passwords, plus customers' credit card numbers."* (The Register)

```
115103118-|--|-XXcsilla@XXX.hu-     |-8Nd+cNdQ360=- |-nevem|--
 62657676-|--|-nonXX@XXXXX.hu-      |-8Nd+cNdQ360=- |-|--
100898317-|--|-Xcsilla2@XXXX.hu-    |-8Nd+cNdQ360=- |-name|--
121149457-|--|-XXcsilla@XXXX.hu-    |-8Nd+cNdQ360=- |-nevem|--
123756555-|--|-barXXXX@XXXX.hu-     |-8Nd+cNdQ360=- |-kind|--
153339366-|--|-slXXX@XXX.hu-        |-8Nd+cNdQ360=- |-Asszony|--
114565459-|--|-zsolt.XXXX@XXX.hu-   |-8Nd+cNdQ360=- |-kislanyom|--
 63691377-|--|-X_csilla@XXXX.hu-    |-8Nd+cNdQ360=- |-|--
 66609165-|--|-archer.XXX@XXX.hu-   |-8Nd+cNdQ360=- |-|--
 67272237-|--|-ylvXXX@XXXXX.hu-     |-8Nd+cNdQ360=- |-|--
 74715082-|--|-lindusXX@XXXXX.hu-   |-8Nd+cNdQ360=- |-nevem|--
174992278-|--|-fXXXX.csilla@XXX.hu-|-8Nd+cNdQ360=- |-|--
177821115-|--|-putirXXXX@XXX.hu-    |-8Nd+cNdQ360=- |-|--
183285417-|--|-kXXX.csilla@XXX.hu-  |-8Nd+cNdQ360=- |-|--
 96471297-|--|-csillapXXX@XXX.hu-   |-8Nd+cNdQ360=- |-|--
 69058043-|--|-csillalXXX@XXX.hu-   |-8Nd+cNdQ360=- |-|--
```

Jelszavak védelme – Hashelés (esettanulmány)

- 2013-ban feltörték az Adobe egyik szerverét
- *"The breach occurred when hackers raided a backup server on which they found, and subsequently published, a 3.8 GB file containing 152 million usernames and poorly-encrypted passwords, plus customers' credit card numbers."* (The Register)

```
115103118-|--|-XXcsilla@XXX.hu-     |-8Nd+cNdQ360=- |-nevem|--
 62657676-|--|-nonXX@XXXXX.hu-      |-8Nd+cNdQ360=- |-|--
100898317-|--|-Xcsilla2@XXXX.hu-    |-8Nd+cNdQ360=- |-name|--
121149457-|--|-XXcsilla@XXXX.hu-    |-8Nd+cNdQ360=- |-nevem|--
123756555-|--|-barXXXX@XXXX.hu-     |-8Nd+cNdQ360=- |-kind|--
153339366-|--|-slXXX@XXX.hu-        |-8Nd+cNdQ360=- |-Asszony|--
114565459-|--|-zsolt.XXXX@XXX.hu-   |-8Nd+cNdQ360=- |-kislanyom|--
 63691377-|--|-X_csilla@XXXX.hu-    |-8Nd+cNdQ360=- |-|--
 66609165-|--|-archer.XXX@XXX.hu-   |-8Nd+cNdQ360=- |-|--
 67272237-|--|-ylvXXX@XXXXX.hu-     |-8Nd+cNdQ360=- |-|--
 74715082-|--|-lindusXX@XXXXX.hu-   |-8Nd+cNdQ360=- |-nevem|--
174992278-|--|-fXXXX.csilla@XXX.hu-|-8Nd+cNdQ360=- |-|--
177821115-|--|-putirXXXX@XXX.hu-    |-8Nd+cNdQ360=- |-|--
183285417-|--|-kXXX.csilla@XXX.hu-  |-8Nd+cNdQ360=- |-|--
 96471297-|--|-csillapXXX@XXX.hu-   |-8Nd+cNdQ360=- |-|--
 69058043-|--|-csillalXXX@XXX.hu-   |-8Nd+cNdQ360=- |-|--
```

Jelszavak védelme – Hashelés (esettanulmány)

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	

Forrás: http://stricture-group.com/files/adobe-top100.txt

Jelszavak védelme – Hashelés (esettanulmány)

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	**123456**

Forrás: http://stricture-group.com/files/adobe-top100.txt

Jelszavak védelme – Hashelés (esettanulmány)

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	**123456**
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	**123456789**

Forrás: http://stricture-group.com/files/adobe-top100.txt

Jelszavak védelme – Hashelés (esettanulmány)

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	**123456**
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	**123456789**
3.	345834	L8qbAD3jl3jioxG6CatHBw==	**password**
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYzKVeq8I=	111111
9.	83411	PMDTbP0LZxu03SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123
11.	76910	j9p+HwtWWT8/HeZN+3oiCQ==	1234567890
12.	76186	diQ+ie23vAA=	000000
13.	70791	kCcUSCmonEA=	abc123
14.	61453	ukxzEcXU6Pw=	1234
15.	56744	5wEAInH22i4=	adobe1
16.	54651	WqflwJFYW3+PszVFZo1Ggg==	macromedia
17.	48850	hjAYsdUA4+k=	azerty
18.	47142	rpkvF+oZzQvioxG6CatHBw==	iloveyou
19.	44281	xz6PIeGzr6g=	aaaaaa
20.	43670	Ypsmk6AXQTk=	654321
21.	43497	4V+mGczxDEA=	12345
22.	37407	yp2KLbBiQXs=	666666
23.	35325	2dJY5hIJ4FHioxG6CatHBw==	sunshine
24.	34963	1McuJ/7v9nE=	123321
25.	33452	yxzNxPIsFno=	letmein

Forrás: http://stricture-group.com/files/adobe-top100.txt

Jelszavak védelme – Hashelés (esettanulmány)

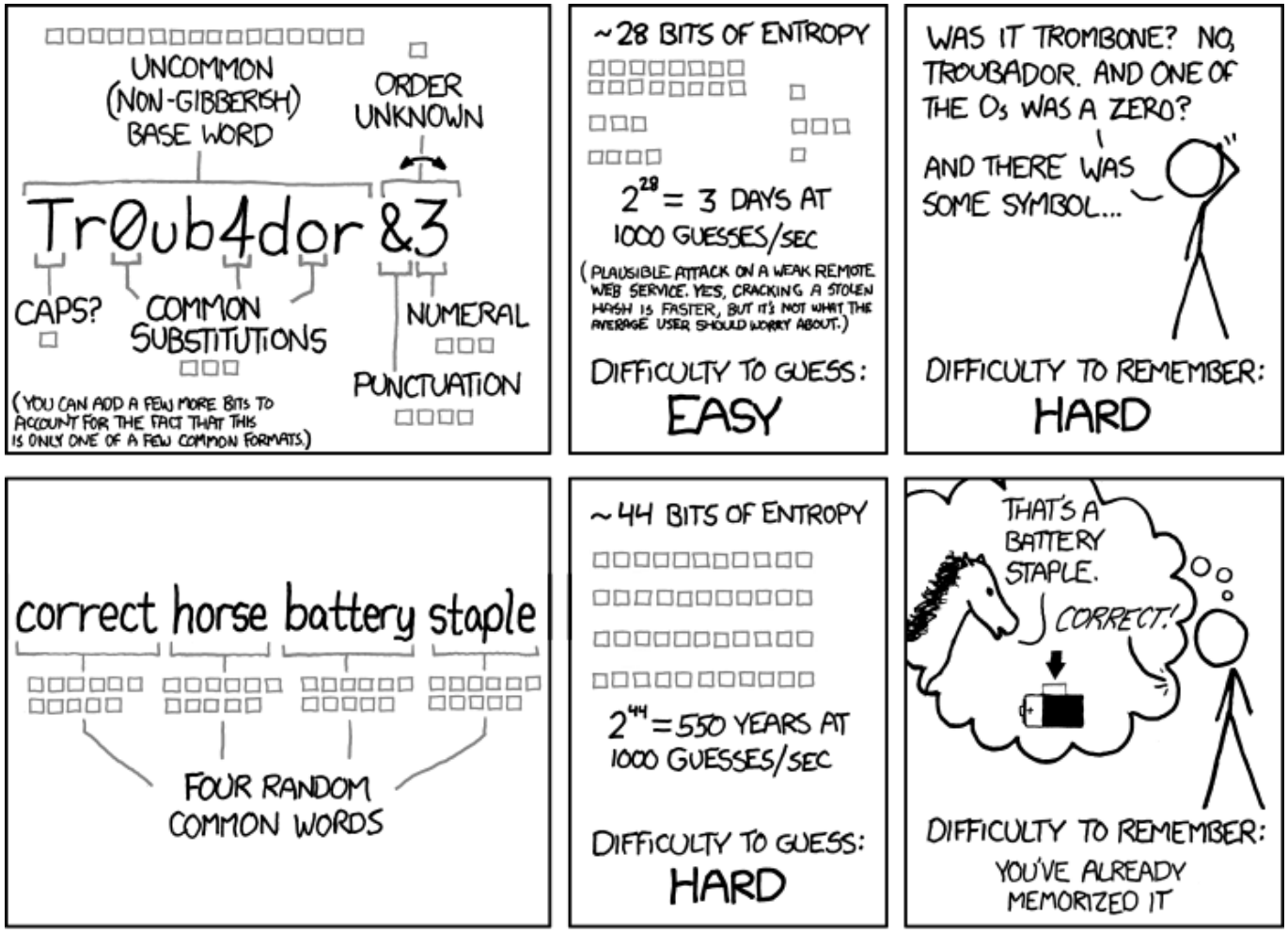
#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	**123456**
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	**123456789**
3.	345834	L8qbAD3jl3jioxG6CatHBw==	**password**
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYzKVeq8I=	111111
9.	83411	PMDTbP0LZxu03SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123
11.	76910	j9p+HwtWWT8/HeZN+3oiCQ==	1234567890
12.	76186	diQ+ie23vAA=	000000
13.	70791	kCcUSCmonEA=	abc123
14.	61453	ukxzEcXU6Pw=	1234
15.	56744	5wEAInH22i4=	adobe1
16.	54651	WqflwJFYW3+PszVFZo1Ggg==	macromedia
17.	48850	hjAYsdUA4+k=	azerty
18.	47142	rpkvF+oZzQvioxG6CatHBw==	iloveyou
19.	44281	xz6PIeGzr6g=	aaaaaa
20.	43670	Ypsmk6AXQTk=	654321
21.	43497	4V+mGczxDEA=	12345
22.	37407	yp2KLbBiQXs=	666666
23.	35325	2dJY5hIJ4FHioxG6CatHBw==	sunshine
24.	34963	1McuJ/7v9nE=	123321
25.	33452	yxzNxPIsFno=	letmein

Forrás: http://stricture-group.com/files/adobe-top100.txt

Hogyan kezeljünk, használjunk jelszavakat?

- Fejlesztőként
  - Tároláshoz használjunk KDF-eket
  - Használjunk létező függvénykönyvtárakat, ne írjunk saját megoldást
- Felhasználóként – a jó jelszó
  - Hosszú -> tartson sokáig a brute force támadás
  - Komplex -> tartson még tovább a brute force támadás
  - Nem szótári szó -> szótáras támadás ne működjön
  - Nem szótári szó mutációja -> hibrid támadás ne működjön
  - Rendszeresen változtatott -> kisebb időablak áll a támadó rendelkezésére
  - Lehet jelmondat (passphrase) is -> könnyen megjegyezhető
- Ne használjuk ugyanazt a jelszót több helyre

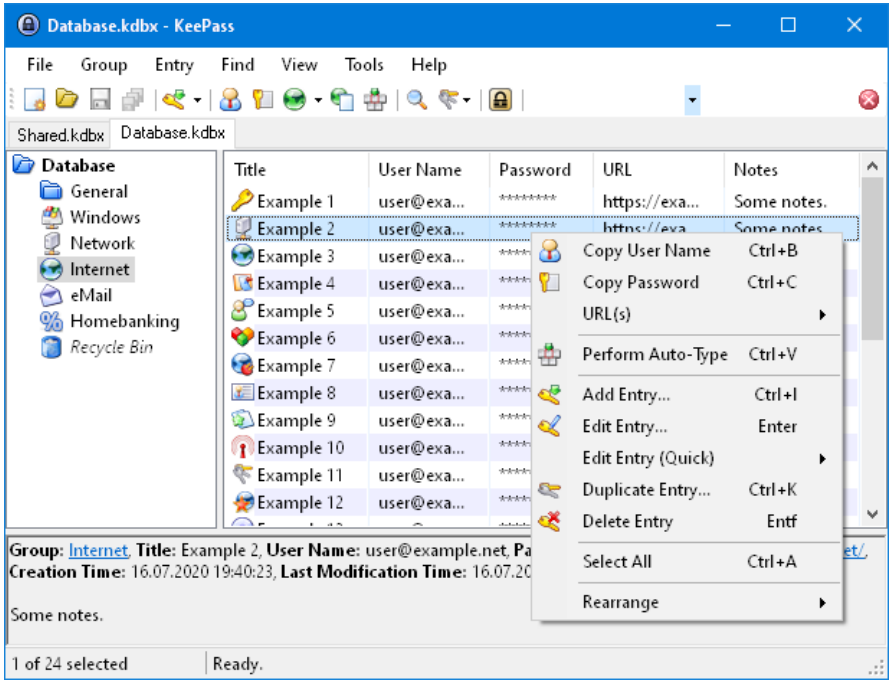
Hogyan kezeljünk, használjunk jelszavakat?

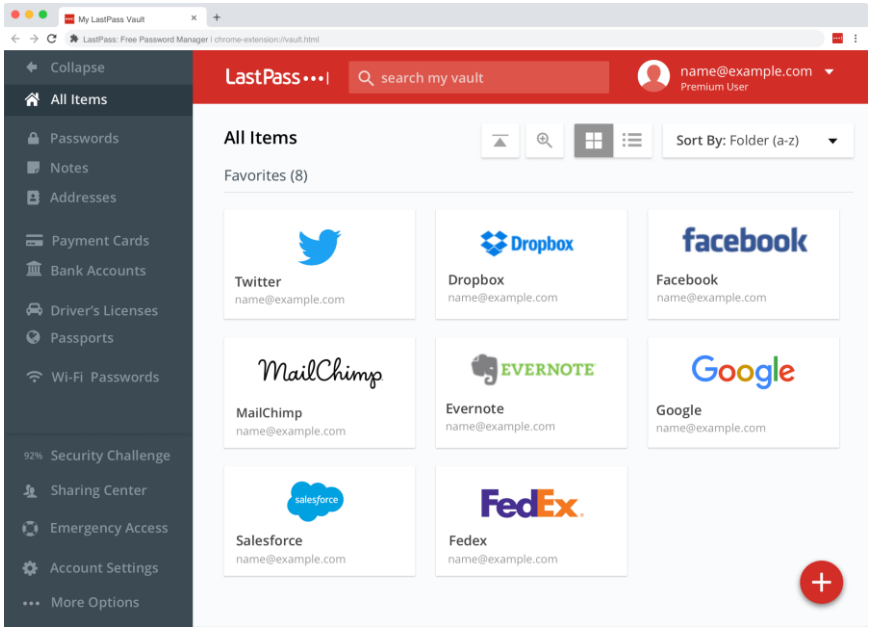


Forrás: https://xkcd.com/936/

Hogyan kezeljünk, használjunk jelszavakat?

- Nehezen megjegyezhetőség ellen: jelszókezelő szoftverek
  - Biztonságos generálás és tárolás
  - Böngészőbe épülő modulok (automatikus generálás, kitöltés)
  - Például: KeePass, LastPass, 1Password



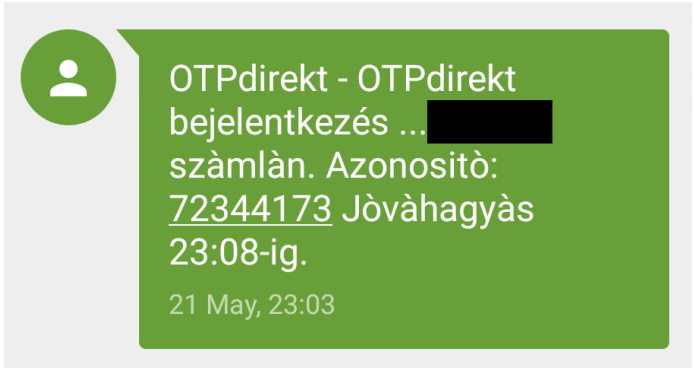


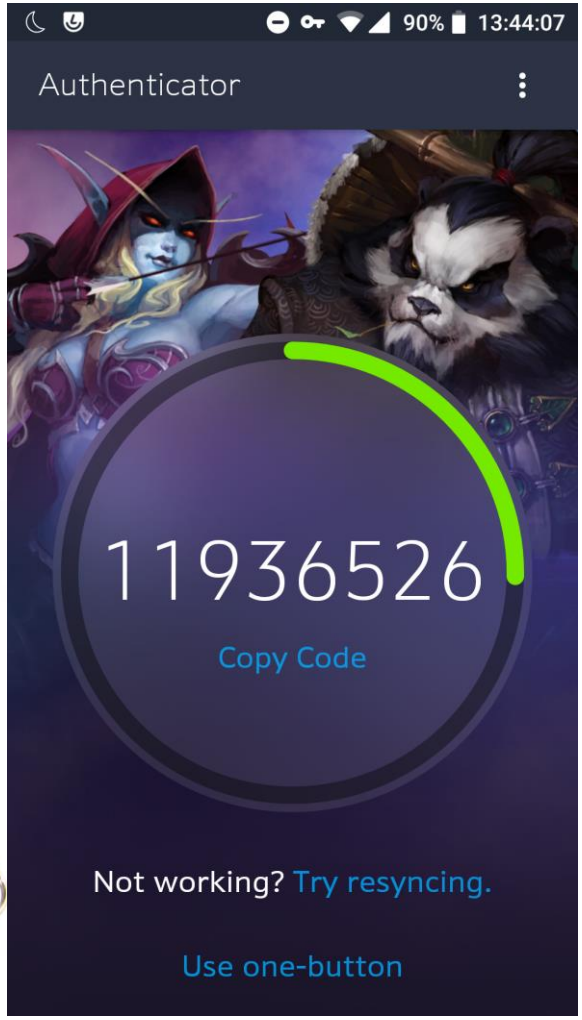
Hitelesítés

Birtokalapú hitelesítés

Birtokalapú hitelesítés

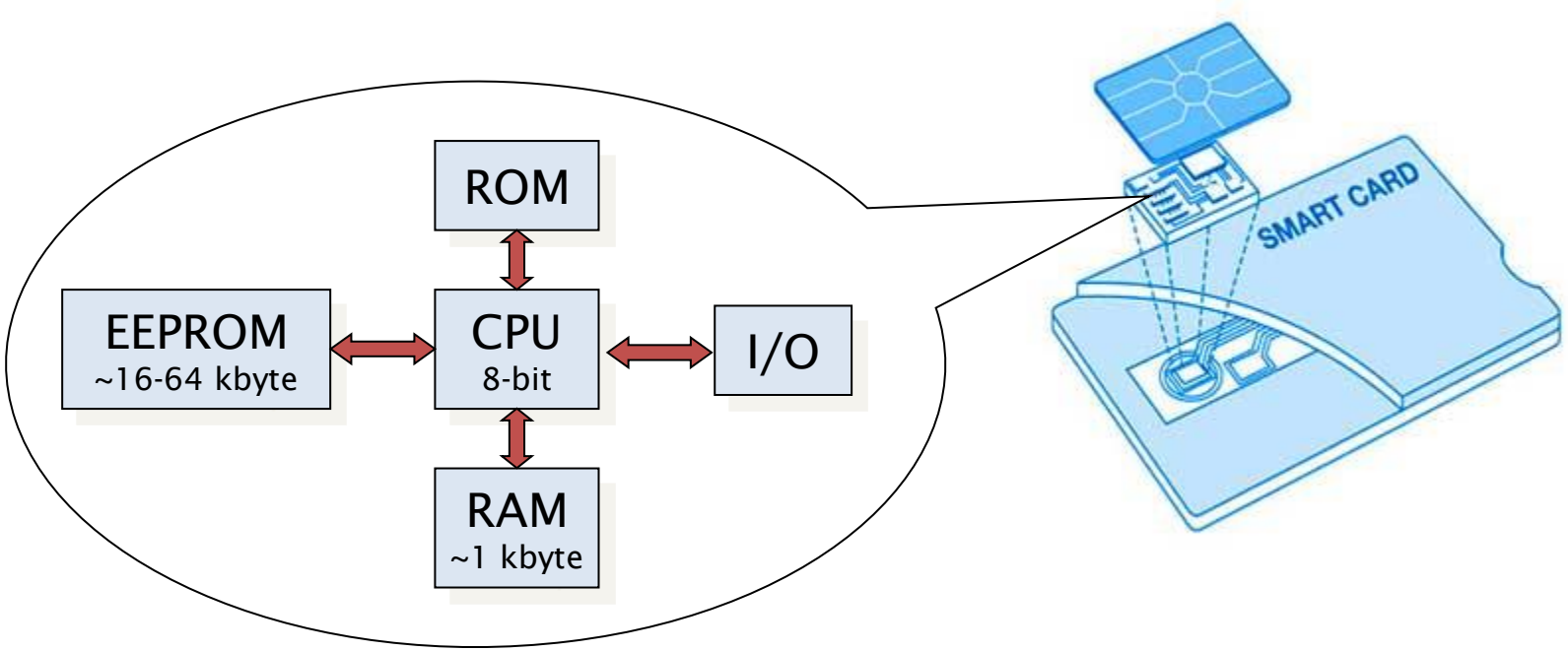
- Egyszer használatos jelszavak segítségével
  - Bejelentkezéshez meg kell adni egy kódot, amit
    - » SMS-ben kapunk meg
    - » Mobilos authentikátor alkalmazás ír ki
    - » Egy speciális fizikai eszköz (offline tokengenerátor) ír ki





Birtokalapú hitelesítés

- Smart kártyákkal
  - A kártyát egy kártyaolvasóba kell helyezni
  - A kártya egy mini számítógép, amely képes egyszerű kriptográfiai műveleteket elvégezni (pl. üzenetet aláírni)
    - » Ezzel igazolható a kártya nálamléte



A birtokalapú hitelesítés problémái

- Offline tokengenerátorok problémái
  - Lemerül az elem
  - Kiesik a szinkronból
- Mobilos tokenek problémái
  - Tönkremegy a telefon
  - Ellopják a telefont
  - Elvesznek az authentikátor alkalmazás adatai

- Ilyen esetekre általában van vészmegoldás
  - » Kinyomtatott backup kódok
  - » Alternatív kódküldés SMS-ben/e-mailben

A birtokalapú hitelesítés problémái

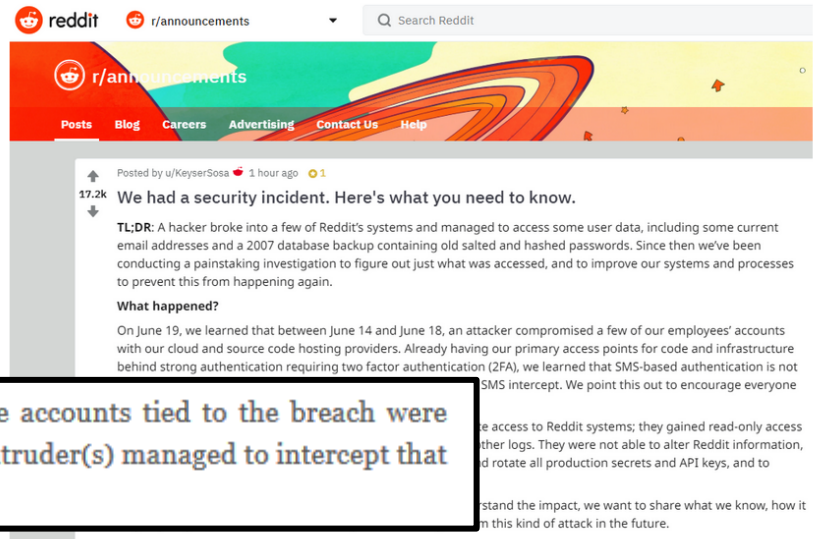
- SMS-alapú tokenek
  - A telefont ellopják, elhagyjuk
  - A beérkező SMS-eket olvashatják mobilos malware-ek is
  - A mobilszámok "ellophatók"
    - » Lásd: Reddit incidens, 2018
    - » SIM-cserés átverés
    - » Számhordozásos átverés
  - Kerülendő, ha van jobb lehetőség

01 AUG 18 **Reddit Breach Highlights Limits of SMS-Based Authentication**

Reddit.com today disclosed that a data breach exposed some internal data, as well as email addresses and passwords for some Reddit users. As Web site breaches go, this one doesn't seem too severe. What's interesting about the incident is that it showcases once again why relying on mobile text messages (SMS) for two-factor authentication (2FA) can lull companies and end users into a false sense of security.

In a post to Reddit, the social news aggregation platform said it learned on June 19 that between June 14 and 18 an attacker compromised a several employee accounts at its cloud and source code hosting providers.

Reddit said the exposed data included internal source code as well as email addresses and obfuscated passwords for all Reddit users who registered accounts on the site prior to May 2007. The incident also exposed the email addresses of some users who had signed up to receive daily email digests of specific discussion threads.



> Of particular note is that although the Reddit employee accounts tied to the breach were protected by SMS-based two-factor authentication, the intruder(s) managed to intercept that second factor.

Forrás: https://krebsonsecurity.com/

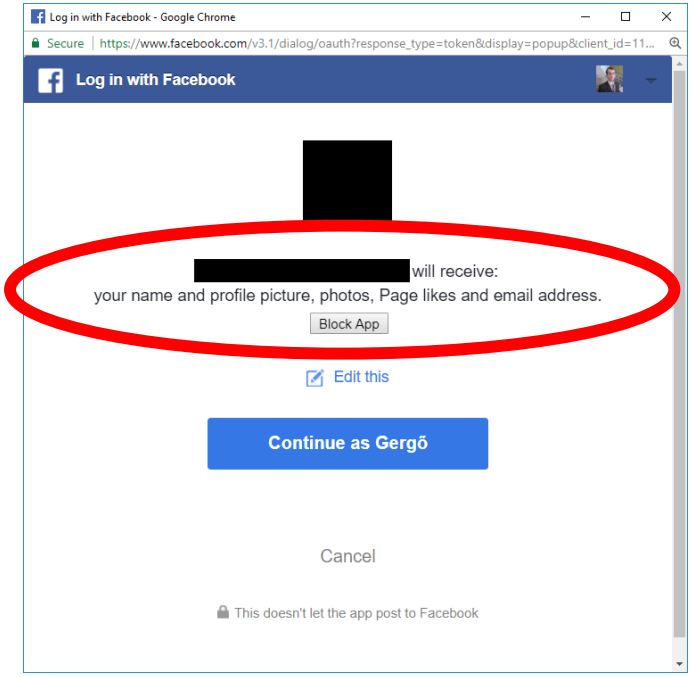
Engedélyezés és hozzáférés-szabályzás

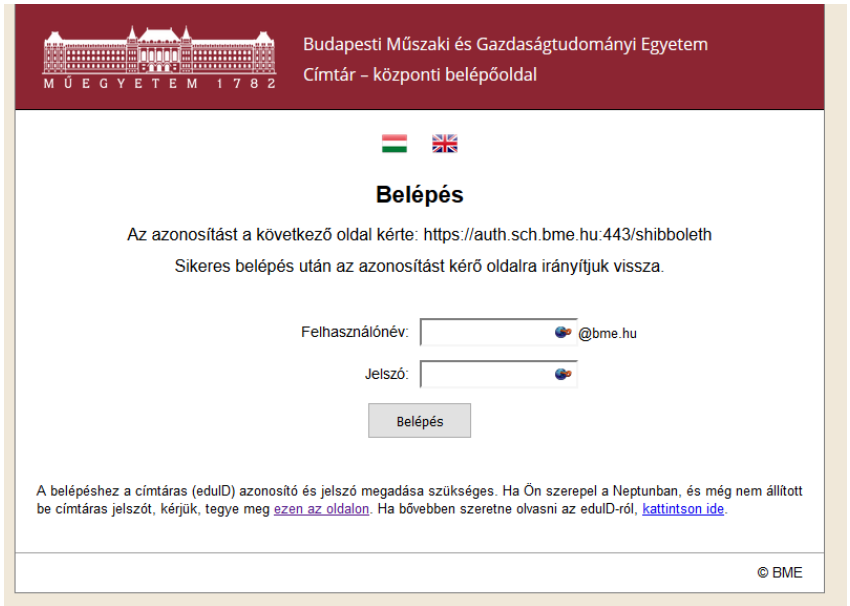
Fogalmak

- Művelet (Operation)
  - Az Alany által az Objektumon végezni kívánt cselekvés (pl. írás, olvasás, törlés)
- Alany (Subject)
  - A műveletet elvégezni kívánó fél
- Objektum (Object)
  - A művelet célpontja
- Biztonsági házirend (Policy)
  - A definiált engedélyezési szabályok összessége
  - A rendszer élete (működése) során is változhat
    - » Új alanyok és objektumok jöhetnek létre
    - » Új szabályok jöhetnek létre
    - » Meglévők megszűnhetnek, módosulhatnak

Engedélyezés

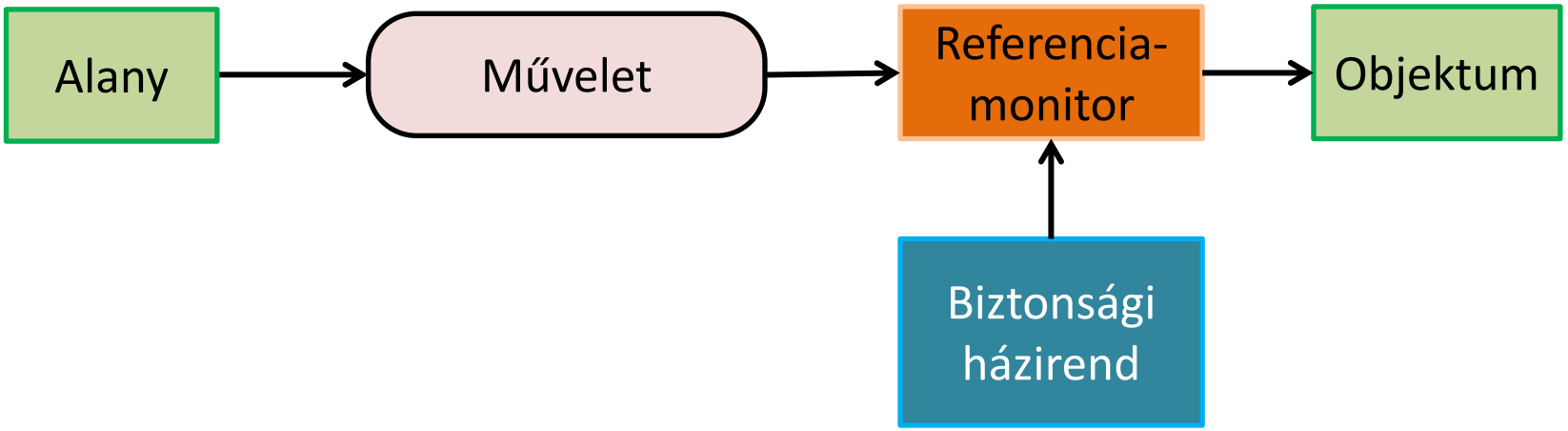
- Az engedélyek definiálhatók (példák)
  - A rendszer üzemeltetői által
  - Az objektumok tulajdonosai által
  - Engedélyezési (authorization) megoldások segítségével
    - » OAuth (pl. Facebook Graph API)
    - » SAML (pl. Shibboleth, BME címtár)





Hozzáférés-szabályzás – a modell

- Tudjuk, ki a felhasználó, és azt is, hogy mihez van jogosultsága
- Most már csak be kell tartatni a biztonsági házirendet
- Általános implementáció:



- Referenciamonitor: megvizsgálja az alanyt, az objektumot, valamint a kívánt műveletet, majd dönt a művelet végrehajthatóságáról a házirend alapján, ezáltal betartatva azt

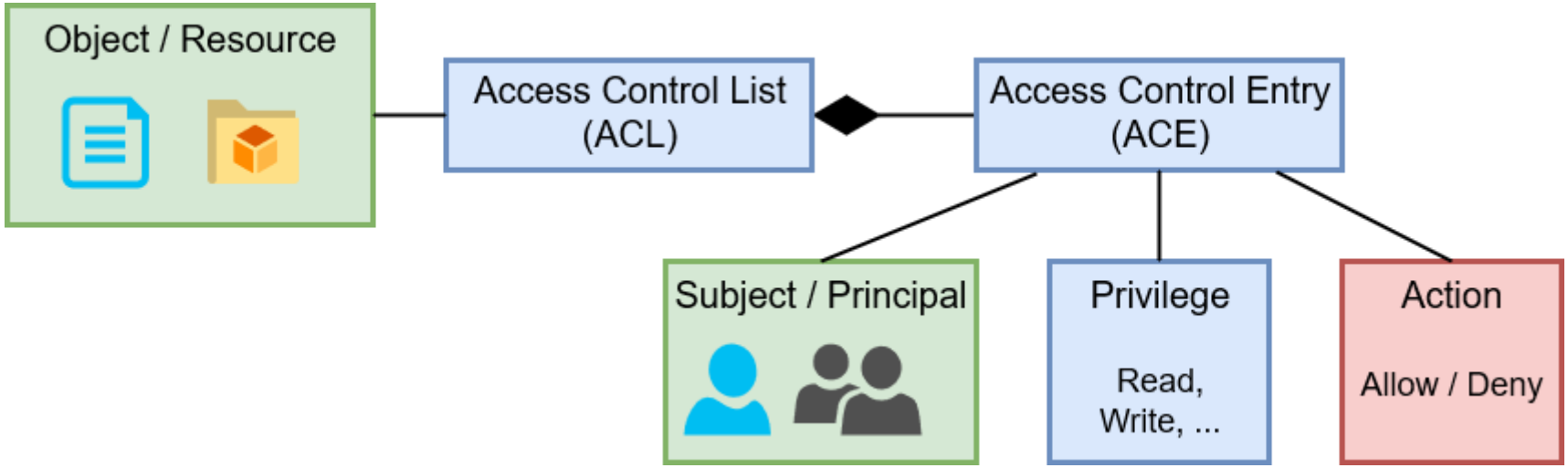
Hozzáférés-szabályzás a gyakorlatban

- Az alkalmazások nem közvetlenül érik el a hardvert, a fájlrendszert, vagy egymást, hanem az operációs rendszeren keresztül
  - A r*eferenciamonitor*t az operációs rendszerben célszerű implementálni

- Két, működési elvében eltérő megvalósítás
  - Discretionary Access Control (DAC) (kb.: belátás szerinti szabályzás)
  - Mandatory Access Control (MAC) (kb.: elrendelő szabályzás)

Discretionary Access Control

- Az objektumoknak tulajdonosaik vannak
- A tulajdonosok dönthetnek úgy, hogy más alanyoknak engedélyt adnak a saját objektumaikhoz
  - A tulajdonosok *saját belátásuk szerint* rendelkezhetnek az objektumaik felett
- Tipikusan hozzáférés-vezérlési listák (ACL) segítségével valósul meg
  - A Linux és a Windows is hasonló elveken működik



Mandatory Access Control

- Az alanyok és az objektumok címkézettek
  - A címkézést az adminisztrátorok végzik, a hagyományos felhasználók a címkéket nem módosíthatják
  - Címkék például:
    - "az Apache egy webszerver"
    - "a .php fájlok a /var/www/-ben webes szkriptek"
- A címkék között összerendeléseket hozunk létre
  - Pl.: "a webszerverek olvashatják és végrehajthatják a webes szkripteket"
- Példák
  - SELinux
  - AppArmor
  - (Windowsban is előfordul)

Engedélyezés és hozzáférés-szabályzás

Windows rendszerek

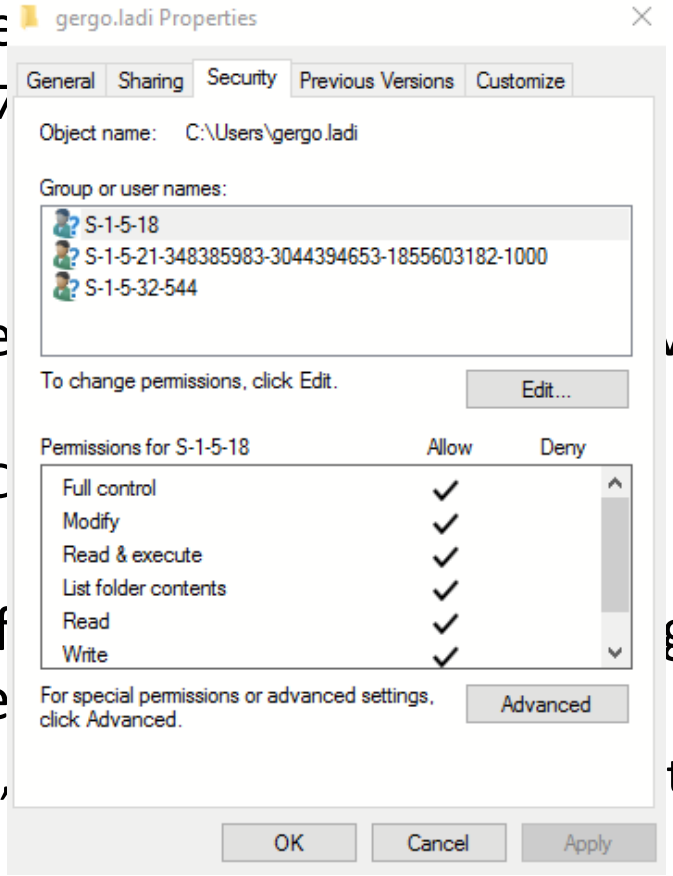
Felhasználókezelés

- Minden felhasználónak, csoportnak és a számítógépeknek egyedi azonosítója van: SID (Security Identifier)
  - Példa: `S-1-5-21-2052111302-1767777339-725345543-12819`
  - Az ACE-k ezekre a SID-ekre hivatkoznak

- Szintén tartozik mindenkihez egy egyedi, sAMAccountName nevű szöveges attribútum
  - Pl.: `gergo.ladi, MyGroup, Work-PC$`
  - Bejelentkezéskor ezeket írjuk be
- Vállalati (tartományi) környezetben a felhasználókhoz tartozik egy userPrincipalName nevű, szintén egyedi, szöveges attribútum is
  - Formailag úgy néz ki, mint egy e-mail cím, de nem feltétlenül van mögötte levelezőfiók, létező e-mail cím
  - Pl.: gergo.ladi@sch.bme.hu

Felhasználókezelés

- Minden felhasználónak, csoportnak és a számítógépeknek egyedi azonosítója van: SID (Security Identifie
  - Példa: `S-1-5-21-2052111302-176777`
  - Az ACE-k ezekre a SID-ekre hivatkoznak
- Szintén tartozik mindenkihez egy egye …vű szöveges attribútum
  - Pl.: `gergo.ladi, MyGroup, Work-PC`
  - Bejelentkezéskor ezeket írjuk be
- Vállalati (tartományi) környezetben a f …gy userPrincipalName nevű, szintén egye
  - Formailag úgy néz ki, mint egy e-mail cím, …te levelezőfiók, létező e-mail cím
  - Pl.: gergo.ladi@sch.bme.hu



Felhasználókezelés

- Minden felhasználónak, csoportnak és a számítógépeknek egyedi azonosítója van: SID (Security Identifier)
  - Példa: `S-1-5-21-2052111302-1767777339-725345543-12819`
  - Az ACE-k ezekre a SID-ekre hivatkoznak

- Szintén tartozik mindenkihez egy egyedi, sAMAccountName nevű szöveges attribútum
  - Pl.: `gergo.ladi, MyGroup, Work-PC$`
  - Bejelentkezéskor ezeket írjuk be
- Vállalati (tartományi) környezetben a felhasználókhoz tartozik egy userPrincipalName nevű, szintén egyedi, szöveges attribútum is
  - Formailag úgy néz ki, mint egy e-mail cím, de nem feltétlenül van mögötte levelezőfiók, létező e-mail cím
  - Pl.: gergo.ladi@sch.bme.hu

Felhasználókezelés – a SAM

- A felhasználókkal kapcsolatos információkat a Security Accounts Manager (SAM) adatbázis tárolja
  - Helye: C:\Windows\System32\config\SAM
  - A fájlt zárolva tartja az operációs rendszer, de léteznek módszerek, hogy ennek ellenére hozzá lehessen férni a tartalmához
- Az adatbázis titkosított (SYSKEY)
  - De a kulcs ott van a SAM mellett: C:\Windows\System32\config\SYSTEM ☺

Felhasználókezelés – a SAM

- A jelszavak kétféle hasheléssel is lehetnek tárolva
  - LMHASH
    - » Elavult, ma már visszafejthető hash algoritmus -> kerüljük
    - » Windows XP óta nem generálódik automatikusan, de kompatibilitási okokból visszakapcsolható
  - NTHASH
    - » MD4 alapú
    - » A rövid és egyszerű jelszavak könnyen törhetők
    - » A hash ellopása esetén az sok esetben jelszóekvivalensként használható, azaz nem szükséges visszafejteni, hogy fel tudjuk használni (pl. pass the hash támadás)

Felhasználókezelés – a SAM

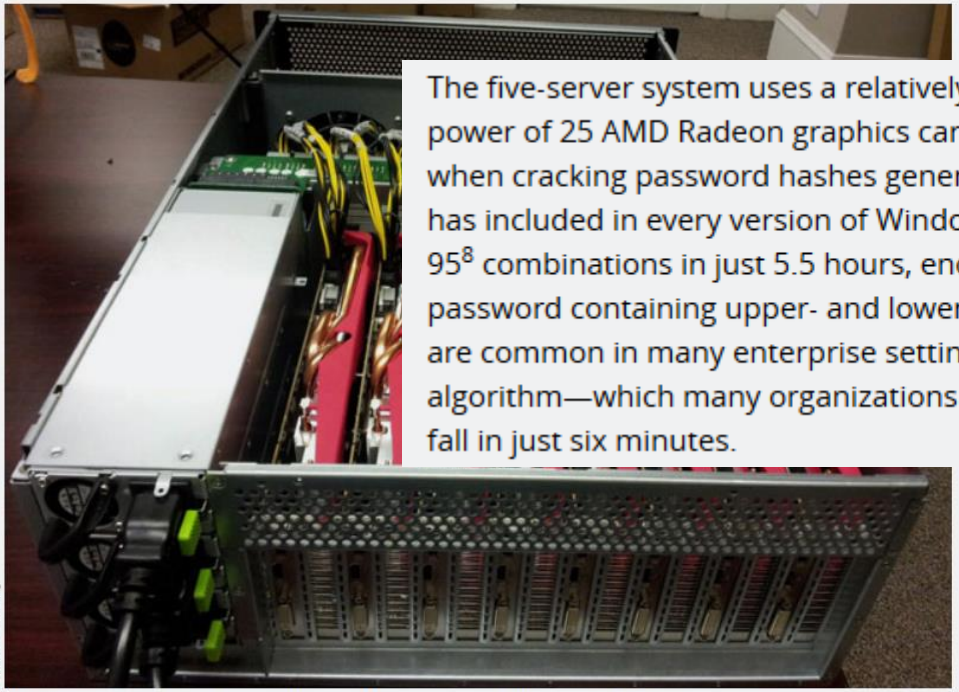
ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE F

BIZ & IT —

25-GPU cluster cracks every standard Windows password in <6 hours

All your passwords are belong to us.

DAN GOODIN - 12/10/2012, 1:00 AM



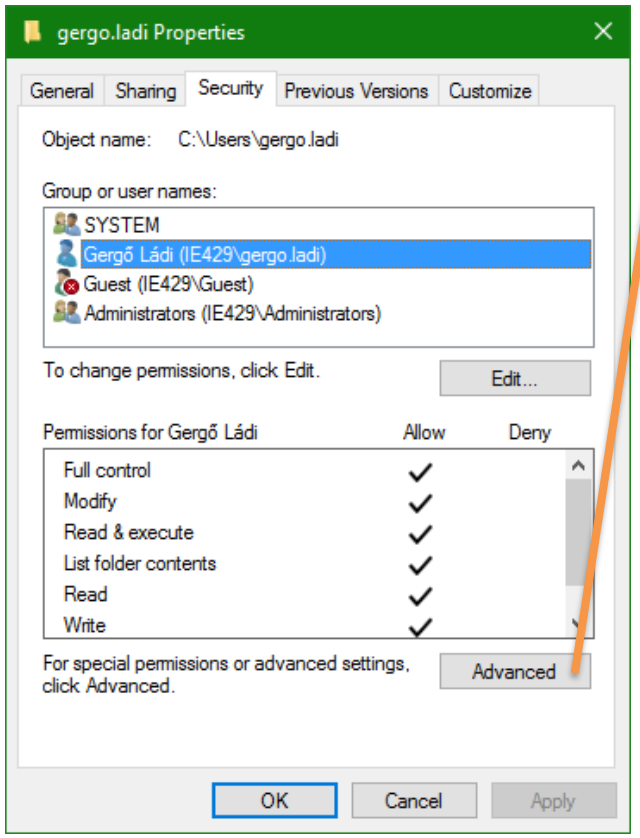
Jeremi Gosney

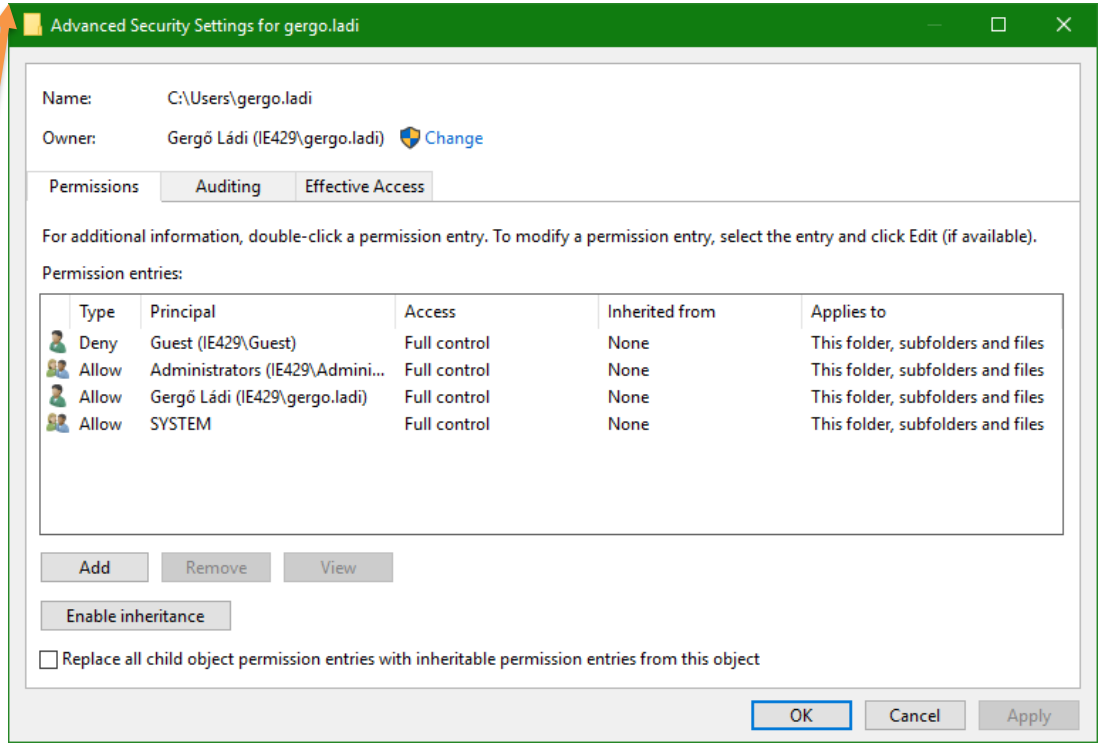
Welcome to Radeon City, population: 8. It's one of five servers that make up a high-performance password-cracking cluster.

The five-server system uses a relatively new package of virtualization software that harnesses the power of 25 AMD Radeon graphics cards. It achieves the 350 billion-guess-per-second speed when cracking password hashes generated by the NTLM cryptographic algorithm that Microsoft has included in every version of Windows since Server 2003. As a result, it can try an astounding 95^8 combinations in just 5.5 hours, enough to brute force every possible eight-character password containing upper- and lower-case letters, digits, and symbols. Such password policies are common in many enterprise settings. The same passwords protected by Microsoft's LM algorithm—which many organizations enable for compatibility with older Windows versions—will fall in just six minutes.

Hozzáférés-szabályzás

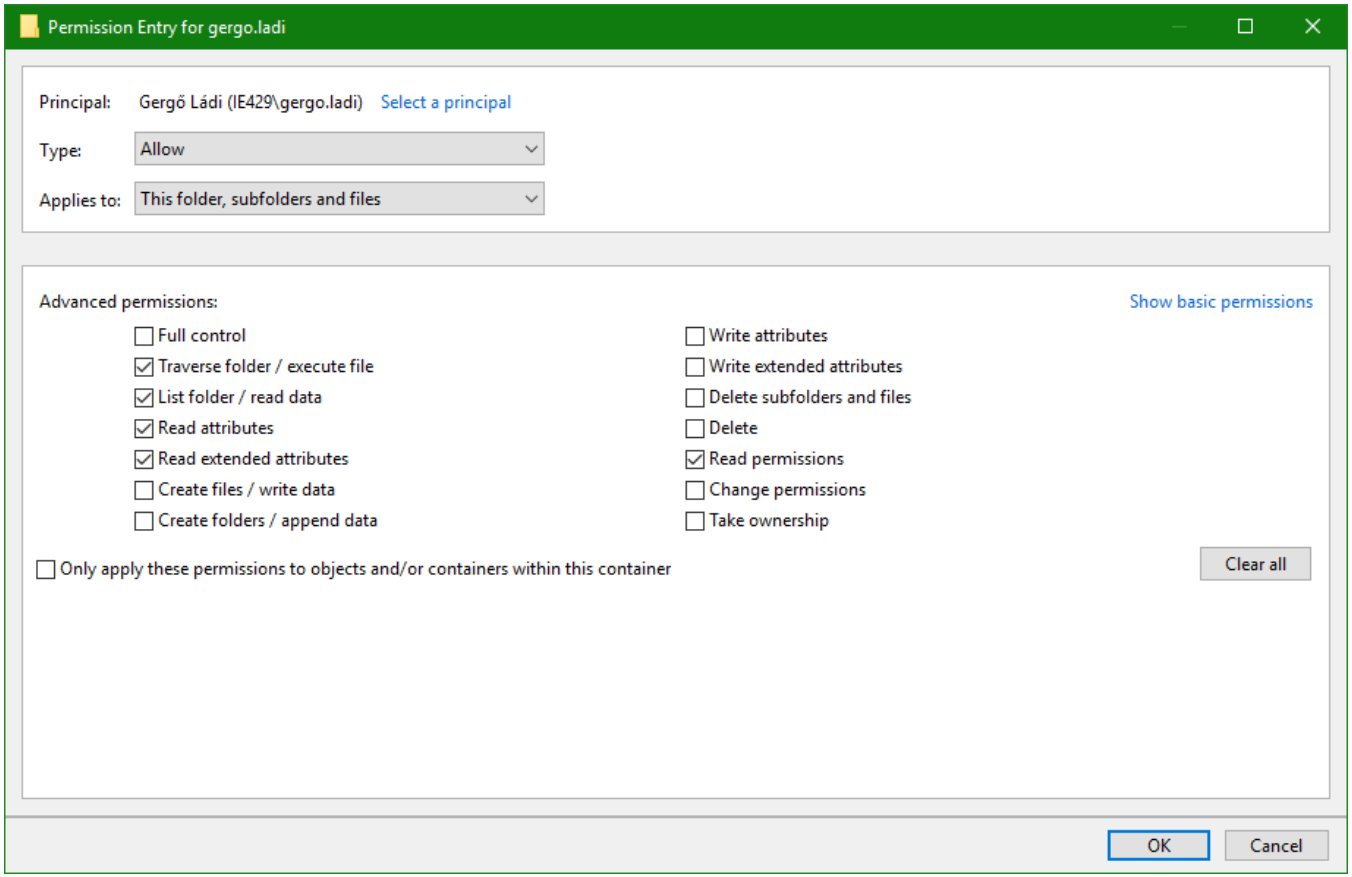
- A hozzáférés-szabályzás ACL-ek segítségével van megvalósítva
  - Az ACL-eket a fájlrendszer metaadat-szekciójában tároljuk
    - » A metaadatokat nem támogató fájlrendszerek esetén (pl. FAT16/32) nem tudunk ACL-eket használni





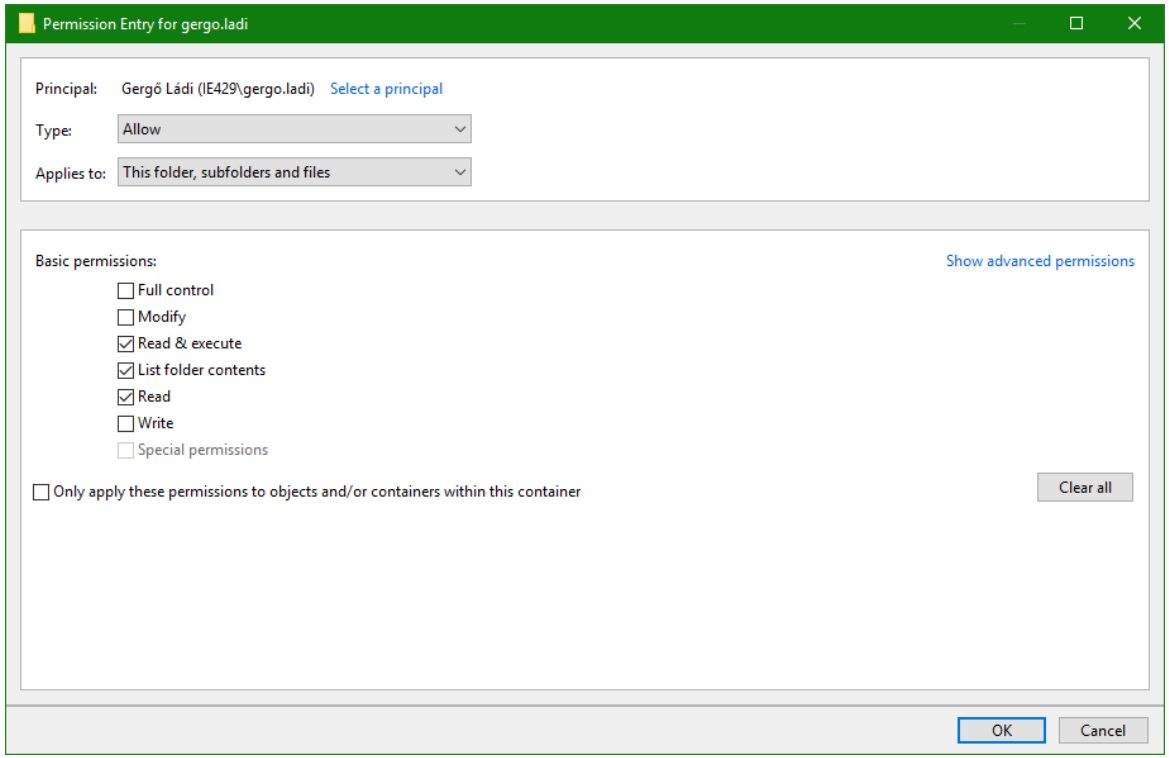
Hozzáférés-szabályzás – engedélyek

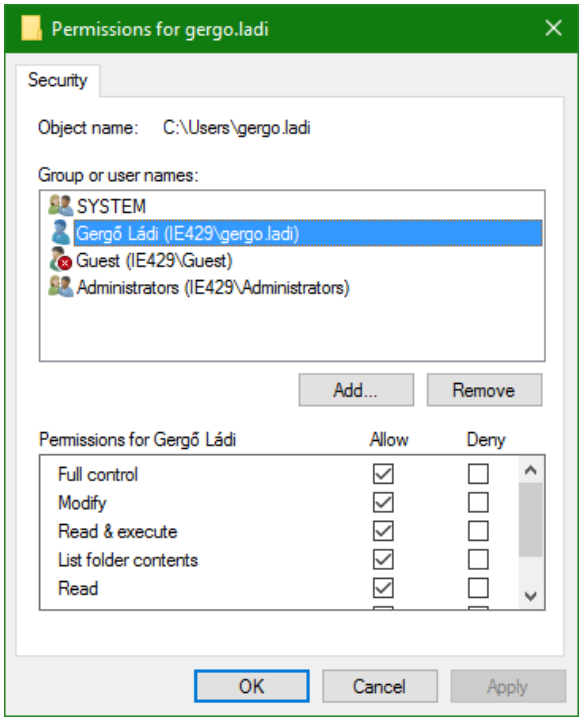
- Összesen 14 különböző engedély adható, de ezek között van átfedés (pl.: a Full Control magában foglalja a többi 13-at)



Hozzáférés-szabályzás – engedélyek

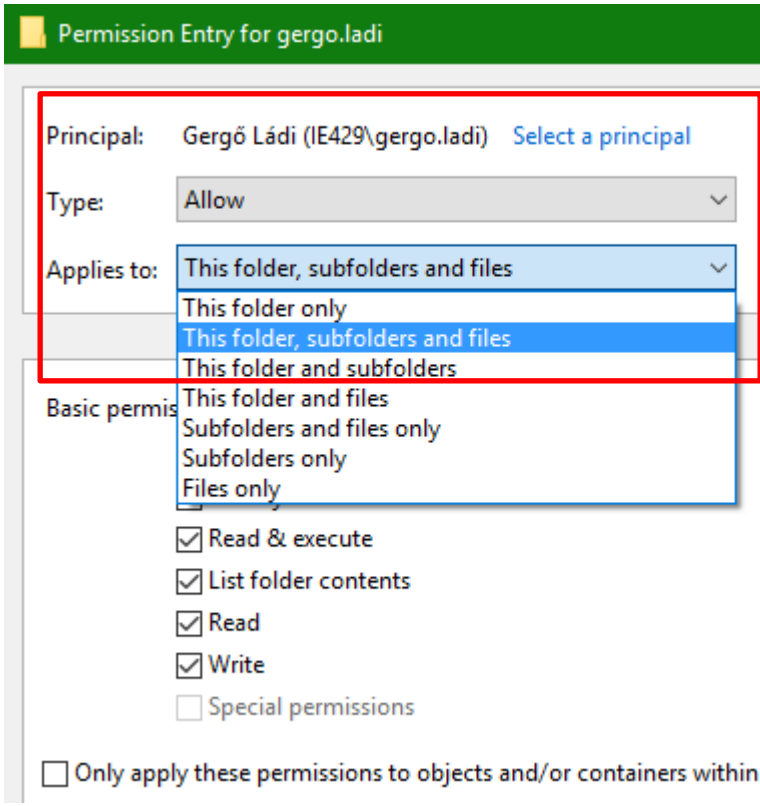
- Az egyszerű nézetben csak 6+1 engedély állítható
  - Ezek megadása/elvétele a háttérben a 14 lehetőséget kapcsolgatja
  - *Special permissions:* közvetlenül nem kattintható – ha be van jelölve, akkor a haladó nézetben olyan kombinációt választottunk, amit az egyszerűsített nézet nem támogat





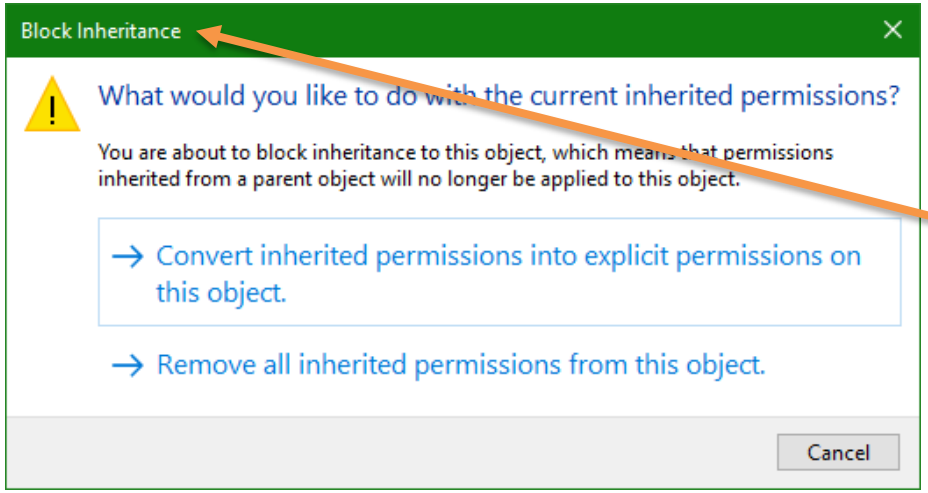
Hozzáférés-szabályzás – engedélyek

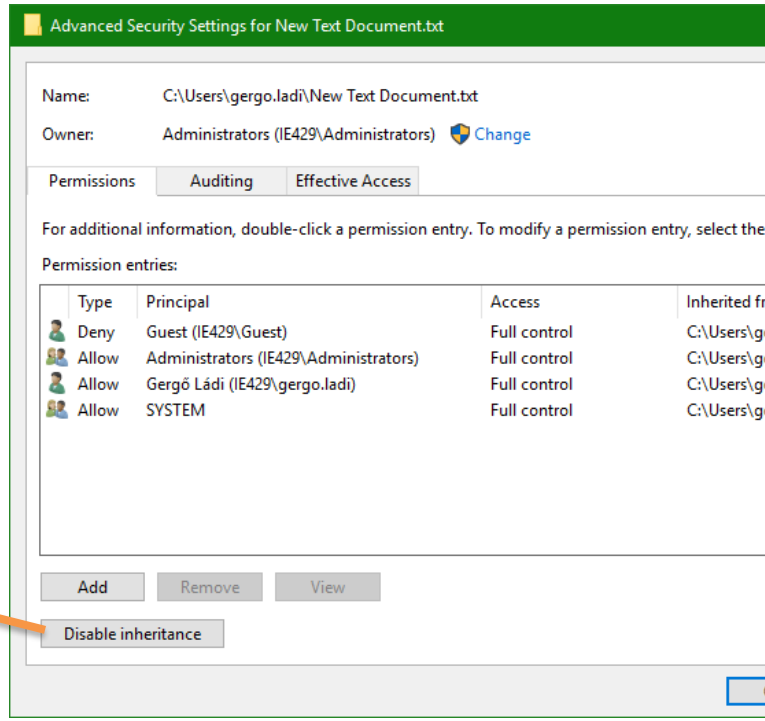
- Az engedélyek megjelölhetők öröklődőként
  - Csak mappák esetén
  - Ha bekapcsoljuk, az almappákra is érvé-nyesek lesznek ezek az engedélyek
- Az öröklődés megszakítható
  - Ez megállítja a lefelé terjedést
  - Ezután teljesen más ACE-ket adhatunk meg a lentebbi szinteken



Hozzáférés-szabályzás – engedélyek

- Az engedélyek megjelölhetők öröklődőként
  - Csak mappák esetén
  - Ha bekapcsoljuk, az almappákra is érvényesek lesznek ezek az engedélyek
- Az öröklődés megszakítható
  - Ez megállítja a lefelé terjedést
  - Ezután teljesen más ACE-ket adhatunk meg a lentebbi szinteken





Hozzáférés-szabályzás – engedélyek

- Egy engedély öröklődés szempontjából lehet
  - Implicit – ha örököltük valahonnan
  - Explicit – ha közvetlenül van az objektumhoz csatolva
- Az engedély – típusa szerint – lehet
  - Megengedő (Allow) vagy
  - Tiltó (Deny)

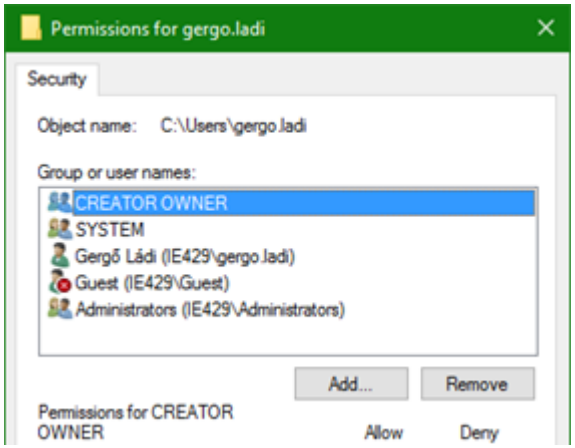
- A tiltás erősebb mint az engedélyezés
- Egy explicit engedély erősebb mint egy implicit
- Tehát: Explicit Deny > Explicit Allow > Implicit Deny > Implicit Allow
  - Ezzel nagyon fontos tisztában lenni, amikor egy komplexebb jogosultsági struktúrát szeretnénk kialakítani (például céges környezetekben)
  - Ha egy felhasználónak Implicit Allow joga sincs egy objektumra, akkor nincs hozzáférése (olvasásra sem)

Hozzáférés-szabályzás – engedélyek

- Egy objektum tulajdonosa mindig módosíthat az objektum jogosultsági listáján, még akkor is, ha ez valamiért explicit tiltva lenne neki

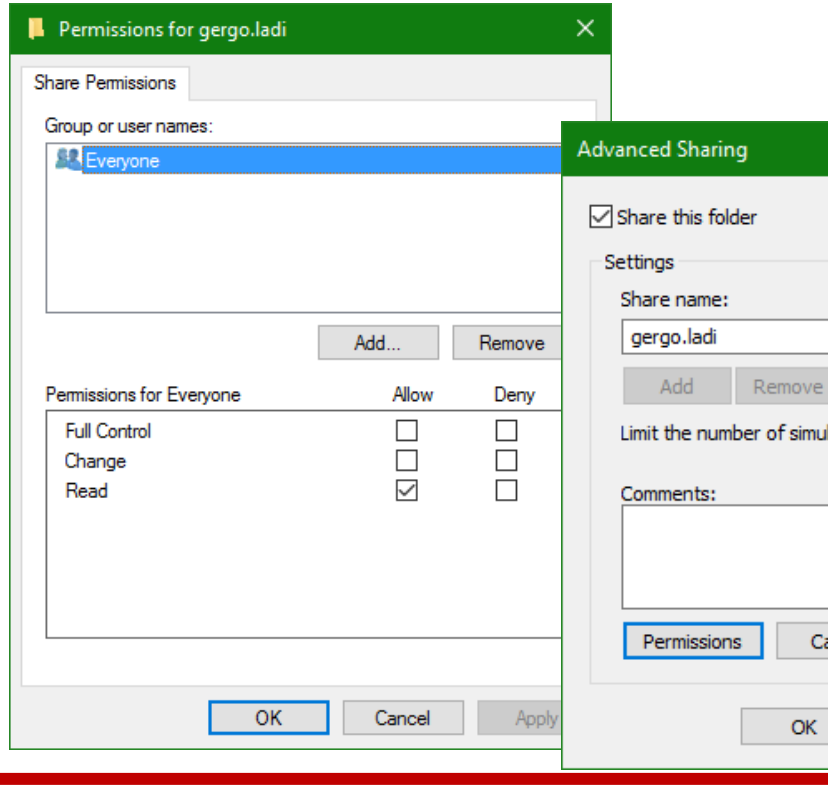
- Az Administrator jogosultságú felhasználók mindig átvehetik az objektumok tulajdonjogát, még akkor is, ha ez valamiért tiltva lenne nekik

- Különleges ACE alany: CREATOR OWNER
  - Ha új fájl vagy mappa létrehozásakor a CREATOR OWNER kapna jogosultságokat, helyette a létrehozó felhasználó kapja meg azokat



Fájlmegosztásra vonatkozó engedélyek

- Megoszthatunk fájlokat, mappákat, nyomtatókat (SMB protokoll)
- Ekkor viszont képbe kerül még egy féle jogosultságkezelés:
  - A megosztási engedélyek (share permissions)
    - » Csak három lehetőség: Full Control, Change, Read
- A hálózaton keresztüli elérésnél mind a korábbi, fájlrendszer szintű, mind a most bevezetett megosztási engedélyek számítanak
  - Eredő engedélyek: a két halmaz metszete
  - Például: Full Control fájlrendszer szinten és Read megosztás szinten -> Read



User Account Control

- A rendszergazda jogkörrel rendelkező felhasználók bejelentkezéskor két biztonsági tokent is kapnak (ha a UAC be van kapcsolva)
  - Egyet rendszergazdai jogosultságokkal
  - Egyet normál felhasználói jogosultságokkal
- A programok alapból a normál jogosultsági tokennel indulnak el
  - Ha ennél több jogosultságra van szükség, kapunk egy promptot, hogy szeretnénk-e admin jogosultságokkal futtatni az adott műveletet
    - » Az ablak egy másik munkamenetben jelenik meg, így egy rosszindulatú program nem tud helyettünk az Igen gombra kattintani

Engedélyezés és hozzáférés-szabályzás

Linux rendszerek

Felhasználókezelés – felhasználók

- Minden felhasználónak van egy egyedi azonosítója (UID)
  - … és egy egyedi felhasználóneve
- A felhasználókról tárolt információk a **/etc/passwd** fájlban vannak
  - A fájlt mindenki olvashatja
  - Régebben a felhasználók jelszavainak hashei is itt voltak

```
gergo.ladi@demovm:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
gergo.ladi:x:1001:1001:Gergő Ládi,,,:/home/gergo.ladi:/bin/bash
mysql:x:107:112:MySQL Server,,,:/nonexistent:/bin/false
redis:x:108:113::/var/lib/redis:/bin/false
```

Felhasználókezelés – felhasználók

- Különleges felhasználó: root (UID=0), mindenhez van joga

- A jelszóhashek a **/etc/shadow** fájlban vannak ($algorithm$salt$hash)
  - A root:root tulajdonában van, --rw------- engedélyekkel

```
gergo.ladi@demovm:~$ sudo cat /etc/shadow
root:!:17804:0:99999:7:::
daemon:*:17804:0:99999:7:::
bin:*:17804:0:99999:7:::
sys:*:17804:0:99999:7:::
sync:*:17804:0:99999:7:::
_apt:*:17804:0:99999:7:::
sshd:*:17804:0:99999:7:::
gergo.ladi:$6$Qfz(...)YZ$sQMCjdFnL.d1o2P(...)NWbu60:17804:0:99999:7:::
mysql:!:17804:0:99999:7:::
redis:*:17805:0:99999:7:::
```

Felhasználókezelés – csoportok

- Minden csoport egyedi csoportazonosítóval (GID) rendelkezik
  - … és minden csoportnak van egy egyedi csoportneve is
- Egy felhasználónak lehet ugyanaz a neve, mint egy csoportnak
- Minden felhasználóhoz tartozik egy csoport, aminek csak ő a tagja
  - Általában ez a felhasználó elsődleges csoportja
- A csoportokról tárolt információk a **/etc/group** fájlban tárolódnak

```
gergo.ladi@demovm:~$ cat /etc/group
root:x:0:
daemon:x:1:
sudo:x:27:gergo.ladi
www-data:x:33:
gergo.ladi:x:1001:
mysql:x:112:
redis:x:113:
```

Hozzáférés-szabályzás

- Minden fájl
- A hozzáférést *engedélyek* szabályozzák
  - A tulajdonosnak (u), a tulajdonos csoportnak (g), és mindenki másnak (o)

```
gergo.ladi@demovm:~$ ls -lah
total 40K
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 12:56 .
drwxr-xr-x 3 root       root       4.0K Sep 30 21:08 ..
-rw------- 1 gergo.ladi gergo.ladi   25 Oct  6 12:56 .bash_history
-rw-r--r-- 1 gergo.ladi gergo.ladi  220 Sep 30 21:05 .bash_logout
-rw-r--r-- 1 gergo.ladi gergo.ladi 3.5K Sep 30 21:09 .bashrc
drwxrwx--- 2 gergo.ladi inboxusers 4.0K Oct  6 16:23 Inbox
-rw-r--r-- 1 gergo.ladi gergo.ladi  675 Sep 30 21:05 .profile
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 16:23 Public
```

Hozzáférés-szabályzás

- Az első betű adja meg a fájl típusát
  - Normál fájl (-)
  - Könyvtár (directory) (d)
  - Link (l)
  - Socket (s)
  - Named pipe (p)
  - Eszköz (device) (blokkos: b, karakteres: c)

```
gergo.ladi@demovm:~$ ls -lah
total 40K
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 12:56 .
drwxr-xr-x 3 root       root       4.0K Sep 30 21:08 ..
-rw------- 1 gergo.ladi gergo.ladi   25 Oct  6 12:56 .bash_history
-rw-r--r-- 1 gergo.ladi gergo.ladi  220 Sep 30 21:05 .bash_logout
-rw-r--r-- 1 gergo.ladi gergo.ladi 3.5K Sep 30 21:09 .bashrc
drwxrwx--- 2 gergo.ladi inboxusers 4.0K Oct  6 16:23 Inbox
-rw-r--r-- 1 gergo.ladi gergo.ladi  675 Sep 30 21:05 .profile
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 16:23 Public
```

Hozzáférés-szabályzás

- 2-3-4. betűk: a fájl tulajdonosának engedélyei
  - r vagy - (olvashat-e?) (könyvtáraknál: tartalom listázása)
  - w vagy - (írhat-e?) (könyvtáraknál : fájlok létrehozása, törlése)
  - x vagy - (lefuttathatja-e?) (könyvtáraknál : fájlok olvasása, írása)
- 5-6-7. betűk: ugyanez, a tulajdonos csoportra
- 8-9-10. betűk: ugyanez, mindenki másra vonatkozóan

```
gergo.ladi@demovm:~$ ls -lah
total 40K
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 12:56 .
drwxr-xr-x 3 root       root       4.0K Sep 30 21:08 ..
-rw------- 1 gergo.ladi gergo.ladi   25 Oct  6 12:56 .bash_history
-rw-r--r-- 1 gergo.ladi gergo.ladi  220 Sep 30 21:05 .bash_logout
-rw-r--r-- 1 gergo.ladi gergo.ladi 3.5K Sep 30 21:09 .bashrc
drwxrwx--- 2 gergo.ladi inboxusers 4.0K Oct  6 16:23 Inbox
-rw-r--r-- 1 gergo.ladi gergo.ladi  675 Sep 30 21:05 .profile
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 16:23 Public
```

Hozzáférés-szabályzás

- 2-3-4. betűk: a fájl tulajdonosának engedélyei
  - r vagy - (olvashat-e?) (könyvtáraknál: tartalom listázása)
  - w vagy - (írhat-e?) (könyvtáraknál : fájlok létrehozása, törlése)
  - x vagy - (lefuttathatja-e?) (könyvtáraknál : fájlok olvasása, írása)
- 5-6-7. betűk: ugyanez, a tulajdonos csoportra
- 8-9-10. betűk: ugyanez, mindenki másra vonatkozóan

```
gergo.ladi@demovm:~$ ls -lah
total 40K
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 12:56 .
drwxr-xr-x 3 root       root       4.0K Sep 30 21:08 ..
-rw------- 1 gergo.ladi gergo.ladi   25 Oct  6 12:56 .bash_history
-rw-r--r-- 1 gergo.ladi gergo.ladi  220 Sep 30 21:05 .bash_logout
-rw-r--r-- 1 gergo.ladi gergo.ladi 3.5K Sep 30 21:09 .bashrc
drwxrwx--- 2 gergo.ladi inboxusers 4.0K Oct  6 16:23 Inbox
-rw-r--r-- 1 gergo.ladi gergo.ladi  675 Sep 30 21:05 .profile
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 16:23 Public
```

Hozzáférés-szabályzás

- 2-3-4. betűk: a fájl tulajdonosának engedélyei
  - r vagy - (olvashat-e?) (könyvtáraknál: tartalom listázása)
  - w vagy - (írhat-e?) (könyvtáraknál : fájlok létrehozása, törlése)
  - x vagy - (lefuttathatja-e?) (könyvtáraknál : fájlok olvasása, írása)
- 5-6-7. betűk: ugyanez, a tulajdonos csoportra
- 8-9-10. betűk: ugyanez, mindenki másra vonatkozóan

```
gergo.ladi@demovm:~$ ls -lah
total 40K
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 12:56 .
drwxr-xr-x 3 root       root       4.0K Sep 30 21:08 ..
-rw------- 1 gergo.ladi gergo.ladi   25 Oct  6 12:56 .bash_history
-rw-r--r-- 1 gergo.ladi gergo.ladi  220 Sep 30 21:05 .bash_logout
-rw-r--r-- 1 gergo.ladi gergo.ladi 3.5K Sep 30 21:09 .bashrc
drwxrwx--- 2 gergo.ladi inboxusers 4.0K Oct  6 16:23 Inbox
-rw-r--r-- 1 gergo.ladi gergo.ladi  675 Sep 30 21:05 .profile
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 16:23 Public
```

Hozzáférés-szabályzás

- 2-3-4. betűk: a fájl tulajdonosának engedélyei
  - r vagy - (olvashat-e?) (könyvtáraknál: tartalom listázása)
  - w vagy - (írhat-e?) (könyvtáraknál : fájlok létrehozása, törlése)
  - x vagy - (lefuttathatja-e?) (könyvtáraknál : fájlok olvasása, írása)
- 5-6-7. betűk: ugyanez, a tulajdonos csoportra
- 8-9-10. betűk: ugyanez, mindenki másra vonatkozóan

```
gergo.ladi@demovm:~$ ls -lah
total 40K
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 12:56 .
drwxr-xr-x 3 root       root       4.0K Sep 30 21:08 ..
-rw------- 1 gergo.ladi gergo.ladi   25 Oct  6 12:56 .bash_history
-rw-r--r-- 1 gergo.ladi gergo.ladi  220 Sep 30 21:05 .bash_logout
-rw-r--r-- 1 gergo.ladi gergo.ladi 3.5K Sep 30 21:09 .bashrc
drwxrwx--- 2 gergo.ladi inboxusers 4.0K Oct  6 16:23 Inbox
-rw-r--r-- 1 gergo.ladi gergo.ladi  675 Sep 30 21:05 .profile
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 16:23 Public
```

Hozzáférés-szabályzás

- 2-3-4. betűk: a fájl tulajdonosának engedélyei
  - r vagy - (olvashat-e?) (könyvtáraknál: tartalom listázása)
  - w vagy - (írhat-e?) (könyvtáraknál : fájlok létrehozása, törlése)
  - x vagy - (lefuttathatja-e?) (könyvtáraknál : fájlok olvasása, írása)
- 5-6-7. betűk: ugyanez, a tulajdonos csoportra
- 8-9-10. betűk: ugyanez, mindenki másra vonatkozóan

```
gergo.ladi@demovm:~$ ls -lah
total 40K
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 12:56 .
drwxr-xr-x 3 root       root       4.0K Sep 30 21:08 ..
-rw------- 1 gergo.ladi gergo.ladi   25 Oct  6 12:56 .bash_history
-rw-r--r-- 1 gergo.ladi gergo.ladi  220 Sep 30 21:05 .bash_logout
-rw-r--r-- 1 gergo.ladi gergo.ladi 3.5K Sep 30 21:09 .bashrc
drwxrwx--- 2 gergo.ladi inboxusers 4.0K Oct  6 16:23 Inbox
-rw-r--r-- 1 gergo.ladi gergo.ladi  675 Sep 30 21:05 .profile
drwxr-xr-x 4 gergo.ladi gergo.ladi 4.0K Oct  6 16:23 Public
```

Hozzáférés-szabályzás

- Mindig a felhasználóra leginkább illő számhármas érvényesül
  - Pl.: ha én vagyok a tulajdonos, csak a tulajdonos engedélyei számítanak
  - Ez lehetővé tesz furcsa kombinációkat is, mint pl.: ----rwxrwx
- Az engedélyek leírhatók számokkal is
  - r = 4, w = 2, x = 1
  - 775 megfelelője: -rwxrwxr-x
- Egy fájl jogosultságai a `chmod` paranccsal változtathatók
  - Csak a tulajdonos változtathat (vagy különleges engedéllyel rendelkezők)
- Egy fájl tulajdonosa a `chown` paranccsal változtatható
- Egy fájl tulajdonos csoportja a `chgrp` paranccsal változtatható
  - Utóbbi két parancshoz különleges engedélyek kellenek (vagy root user)

Hozzáférés-szabályzás

- Különleges jogosultsági értékek
  - *setuid* – ha egy futtatható állományra be van állítva, az mindig a tulajdonos nevében fut, függetlenül attól, hogy ki indította el
    - » Pl.: `-rwsrwxr-- root root` mindig root nevében fog futni
    - » Könyvtárakon nincs hatása
    - » Nincs hatása, ha a tulajdonosnak nincs *x* engedélye (ilyenkor nagy S látszik)
  - *setgid* – setuidhoz hasonló, de a tulajdonos csoportot állítja át
    - » Pl.: `-rwxrwsr-- gergo cloudmgmt` úgy fog futni, mintha valaki a *cloudmgmt* csoportból indította volna el, de a tulajdonos felhasználó nem változik
    - » Ha a tulajdonos csoportnak nincs *x* engedélye, nagy S látszik
    - » Ha könyvtárra van beállítva, akkor az ott létrejövő új fájlok tulajdonos csoportja a könyvtáré lesz, és nem pedig a fájlt létrehozó felhasználóé
  - sticky bit – ha be van állítva egy könyvtárra, az itt lévő fájlokat csak a tulajdonosuk törölheti
    - » Pl.: `drwxrwxrwt` könyvtárból mindenki csak a saját fájljait törölheti
    - » Fájlokra közvetlenül nincs hatással
    - » Ha *mindenki más*nak nincs *x* engedélye, nagy T látszik

Hozzáférés-szabályzás

- Alapértelmezett engedélyek
  - Új fájl létrejöttekor annak engedélyei 666 (-rw-rw-rw-) lesznek
  - Könyvtárak esetén ez 777 (drwxrwxrwx)
- Ez a viselkedés az `umask` paranccsal átállítható
  - A maszk értéke kivonódik az alapértelmezett engedélyekből
  - Pl.: ha az umask 022, az új könyvtárak 755-ként (drwxr-xr-x) jönnek létre

Kérdések?

Köszönöm a figyelmet!

Egyebek

Érdeklődők figyelmébe (angol nyelven)

- FIDO – Fast Identity Online
  https://fidoalliance.org/
- WebAuthn
  https://webauthn.io/
- Az OAuth-ról bővebben
  https://developer.okta.com/blog/2017/06/21/what-the-heck-is-oauth
- A SAML-ről röviden
  https://www.varonis.com/blog/what-is-saml/

- Az SID-król bővebben
  https://en.wikipedia.org/wiki/Security_Identifier
- LMHASH-ről és NTHASH-ről bővebben
  https://medium.com/@petergombos/lm-ntlm-net-ntlmv2-oh-my-a9b235c58ed4

Ellenőrző kérdések

- Micsoda és mire való az authentikáció (hitelesítés)?
- Micsoda és mire való az authorizáció (engedélyezés)?
- Micsoda és mire való az access control (hozzáférés-szabályzás)?
- Micsoda és mire való az accounting (naplózás)?
- Mit jelent az AAA rövidítés?

- Milyen formái vannak az authentikációnak? Mindegyikre adj példát!
- Mi az, hogy 2FA, MFA? Mi a célja, alapötlete?

Ellenőrző kérdések

- Hogyan lehetséges jelszóalapú rendszereket megtámadni?
- Hogyan érdemes fejlesztőként jelszavakat kezelni, tárolni?
  - Hashing
  - Salting
  - Stretching
  - KDF-ek
- Hogyan érdemes felhasználóként jelszavakat választani?

- Ismertesd a birtokalapú hitelesítési módszereket!
  - Ezeknek mik lehetnek a hátrányai?

Ellenőrző kérdések

- Ismertesd az engedélyezés alapfogalmait és modelljét!
- Tipikusan kik és hogyan definiálhatnak engedélyeket?

- Mi az, hogy Discretionary Access Control?
- Mi az, hogy Mandatory Access Control?

Ellenőrző kérdések

- Hogyan néz ki Linux és Windows esetében … ?
  - A felhasználók kezelése
  - Az engedélyeik kezelése
  - A hozzáférés-szabályzás
- Linux
  - Mit jelent, ha egy fájl jogosultságáról azt látom, hogy 755?
  - Mi a setuid, setgid és a sticky bit szerepe a hozzáférés-szabályzásban?
- Windows
  - Mi az öröklődés szerepe a jogosultságok tekintetében?
  - Mi az engedélyek precedenciasorrendje?
  - Hogyan működnek a megosztásszintű engedélyek (share permissions)?