



IT KOLLEDŽ  
TALLINNA TEHNIKAÜLIKOOL

# Kasutajate haldamine

Operatsioonisüsteemid ja nende haldamine ICA0001

Edmund Laugasson

[edmund.laugasson@taltech.ee](mailto:edmund.laugasson@taltech.ee)

[https://wiki.itcollege.ee/index.php/User:Edmund#eesti\\_keeles](https://wiki.itcollege.ee/index.php/User:Edmund#eesti_keeles)

Käesoleva dokumendi paljundamine, edasiandmine ja/või muutmine on sätestatud ühega järgnevatest litsentsidest kasutaja valikul:

\* GNU Vaba Dokumentatsiooni Litsentsi versioon 1.2 või uuem

\* Creative Commons Autorile viitamine + Jagamine samadel tingimustel 4.0 litsents (CC BY-SA)

# Ohud

- igapäevane kasutamine tavakasutajana
  - isegi kui olete ise arvuti omanik
  - ka pahavaral on samad õigused kasutajaga
  - süsteemikahjustuste vältimine (kogemata kustutamine, võimalik pahavara)
- kas olete mõnel tuttaval arvuti OSi pahavarast puhastanud?
- kas sooviksite seda tööd ka tulevikus teha?
- <https://www.gnu.org/proprietary/>
- <https://www.fsf.org/windows>



## Ohud 2

- saladuste hoidmine
  - kui selgub, et üks töötaja polnud lojaalne
  - müüs firma saladused maha
  - kas on täpselt teada, mis infole tal ligipääs oli?
- **minimaalsed** vajalikud õigused
  - on tüütud
  - on hädavajalikud





## Kasutajate haldamine

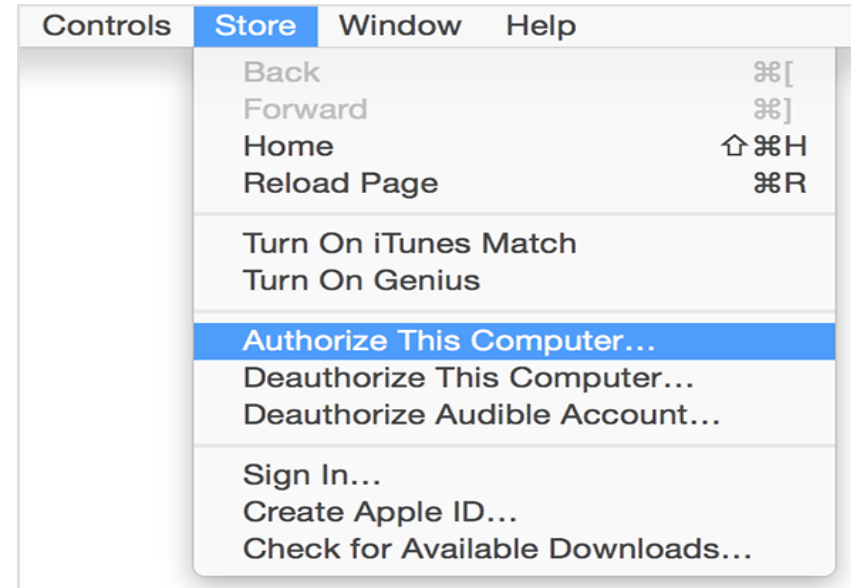
- Muudatused infosüsteemis peavad jätma oma jälje
  - Kes muutis
  - Mis ajal muutis
  - Inimesed tuleb tuvastada
- Infosüsteemi andmete muutmist võivad teostada vaid **volitatud** isikud
  - Kasutaja õiguseid on vaja kontrollida ja reguleerida ehk rakendada pääsukontrolli

# Autentimine ja autoriseerimine

- isikutuvastus e autentimine (*authentication*)
- autoriseerimine – pääsukontrolli rakendamine (*authorization*)



<http://docs.oracle.com/javaee/5/tutorial/doc/figures/security-httpBasicAuthentication.gif>



[https://support.apple.com/library/content/dam/edam/applecare/images/en\\_US/mac\\_apps/itunes/yosemite-itunes12\\_store-authorize\\_this\\_computer.png](https://support.apple.com/library/content/dam/edam/applecare/images/en_US/mac_apps/itunes/yosemite-itunes12_store-authorize_this_computer.png)



## Kasutaja

- Infosüsteemi sisenev kasutaja tuvastatakse
- Kasutajale tagatakse pääs vaid neile ressurssidele, mis on tema rollile lubatud ehk kasutaja autoriseeritakse
- Infosüsteemi kasutamist ja väärkasutamist jälgitakse ehk **auditeeritakse**

# Isikutuvastus (*authentication* -> *autentimine*)

- Kasutatakse
  - Midagi, mida kasutaja **teab** – salafraas (vt järgmine slaid), PIN
  - Midagi, mida kasutaja **omab** – kiipkaart, magnetkaart
  - Midagi, mis on **kasutaja osa**:) – sõrmejalg ja muud biomeetrilised vahendid
  - vt lisa [https://en.wikipedia.org/wiki/Category:Authentication\\_methods](https://en.wikipedia.org/wiki/Category:Authentication_methods)
  - <https://en.wikipedia.org/wiki/Authenticator>
  - [https://en.wikipedia.org/wiki/Multi-factor\\_authentication](https://en.wikipedia.org/wiki/Multi-factor_authentication)
  - [https://en.wikipedia.org/wiki/Category:Cryptographic\\_hardware](https://en.wikipedia.org/wiki/Category:Cryptographic_hardware)
  - [https://en.wikipedia.org/wiki/Security\\_token](https://en.wikipedia.org/wiki/Security_token)
  - [https://en.wikipedia.org/wiki/Single\\_sign-on](https://en.wikipedia.org/wiki/Single_sign-on)
  - <https://serverfault.com/questions/653792/ssh-key-authentication-using-ldap>



<https://www.yubico.com/wp-content/uploads/2017/09/yubikey-4-series-sept-2017-444x444.png>

<https://en.wikipedia.org/wiki/YubiKey>

<https://onlykey.io/>

<https://everykey.com/>



[https://upload.wikimedia.org/wikipedia/commons/thumb/8/8f/SecurID\\_token\\_new.JPG/220px-SecurID\\_token\\_new.JPG](https://upload.wikimedia.org/wikipedia/commons/thumb/8/8f/SecurID_token_new.JPG/220px-SecurID_token_new.JPG)

# Salasõna -> salafraas

- Kasutaja salafraasile võib (peab) esitama nõudeid
  - peab olema raskesti äraarvatav, kuid soovitatavalt kergesti meelde jäetav – näiteks kokkukirjutatud lause, sh numbrid ja erisümbolid kuid eesti täpitähti ei soovita kasutada
  - pikkus peab olema vähemalt 8 märki, soovitatavalt 20 ja rohkem (kuni 15-kohalised MS Windowsi salasõnad on murtavad alla poole tunni) – see kõik muutub arvutusvõimsuse kasvades (NB! [kvantarvutid!](#))
  - ei tohi sisaldada sõnastikus leiduvaid sõnu
  - peab sisaldama suur ja väiketähti ning numbreid ja soovitatavalt erimärke
- salasõna ei tohi teistega jagada (kaasneb ka halduse vastutus!)
- salasõnale tuleb eelistada salafraasi, kiipkaarti, biomeetrikat vms
- võimalusel kasutada mitmeastmelist autentimist
- <https://howsecureismypassword.net/> - tasub aeg-ajalt kontrollida olemasolevate salafraaside arvutuskiirust
- <https://haveibeenpwned.com/> - mis on juhtunud...





## Kasutaja infosüsteemis

- Uue kasutaja puhul
  - Kasutaja lisatakse vastavatesse gruppidesse või rolli
  - Kasutajale antakse identifitseerimiseks parool või kiipkaart
- Kasutaja muudab firma sees oma rolli
  - Kasutaja eemaldatakse olemasolevatest gruppidest/rollist
  - Kasutaja lisatakse uude gruppi/rolli



## Kasutaja lahkub firmast

- Kasutaja lahkumisel
  - Võetakse kasutajalt ligipääs infosüsteemi ressurssidele
  - Arhiveeritakse kasutaja loodud andmed ja e-mail postkast
  - Suunatakse kasutaja e-post teise postkasti
  - Eemaldatakse kasutaja andmed süsteemist



## Protsessid

- Firmas peab olema kirjalik protsess kasutajaõiguste saamiseks, muutmiseks ja kustutamiseks
- Asjad ei käi nii, et süsteemiadministraator valib ise õiguste nimekirja, mis uuele kasutajale lubatakse
- Firmas peab olema ülevaade kasutajate ja rollide õigustest



## Kasutajate rollid

- kasutajad kuuluvad rollidesse, nt
  - insener
  - tootearendaja
  - administraator
  - jne
- rolle realiseeritakse sageli gruppidega
  - grupp insenerid
  - jne
- Igal rollil on omad juurdepääsureeglid infosüsteemi ressurssidele



## Kasutaja ID

- Igal kasutajal on infosüsteemis oma ID
  - UNIXilaadsetes (sh Linuxis) UID – user ID
    - Näiteks 500
    - UID = 0 -> Juurkasutaja
  - Windows süsteemides SID Security Identifier
    - Näiteks S-1-5-21-domeeni\_id-500
    - <http://support.microsoft.com/kb/243330>



## Kasutaja andmed

- Linux laadsetes süsteemides hoitakse kasutaja kohta järgnevaid andmeid
  - kasutajanimi
  - salasõna (*password*) ja selle räsi (*hash*)
  - **UID (User ID), GID (Group ID)**
  - kasutaja kodukataloog (*/home/kasutaja*)
  - kasutaja *shell* (vaikimisi kasutatav *shell*)
  - parooli ja kasutaja aegumise andmed



# Kasutajate andmed hoitakse

- Kasutajate ja gruppide andmed hoitakse kataloogides
- UNIXilaadsetes (sh Linuxis, Mac OS'is)
  - */etc/passwd* hoitakse kasutajad  
kasutaja:x:UID:GID:nimi,,tel1,tel2:/home/kodu:/bin/bash  
<http://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/>
  - */etc/shadow* – hoitakse salasõna räsi (*hash*) ja konto/salasõna aegumise andmeid jne, **pole kõigile loetav – miks?**  
<http://www.cyberciti.biz/faq/understanding-etcshadow-file/>
  - */etc/group* grupid  
<http://www.cyberciti.biz/faq/understanding-etcgroup-file/>
- *AD Active Directory*
  - Microsoft Windows süsteemides
  - ka UNIXilaadsed (sh Linux) suudavad kasutada (isikut tuvastada)
- Mitme serveriga süsteemid
  - (Open)LDAP kataloogiteenus



## Rühmad (grupid)

- Kasutajal on primaarne rühm (Ubuntu sama nimega kui kasutaja) ja sekundaarsed rühmad
  - Linuxis vaata käsuga *id* hetkel sisseloginud kasutaja kohta
- Näiteks võib kasutaja **primaarne rühm** olla *users* ja sekundaarsed rühmad *audio*, *video* jne
- rühmakuuluvusega reguleeritakse ka ligipääsu seadmetele, kataloogidele jne
- */etc/group*
- Igal grupil on oma ID ehk **GID**





# Keskne kasutajate baas

- Suurfirmades on palju servereid
  - mitmed Unix serverid
  - mitmed Windows serverid
  - palju tööjaamu
- Probleem: kasutaja oleks vaja hoida ühes süsteemis
- Lahendus: LDAP kataloog
  - AD kujul
  - LDAP+Kerberos kujul
- juurutada on vaja neid rakendusi, mis toetavad keskset kasutajate baasi
- kui on vaja mitut kataloogi kasutajate andmete hoidmiseks, siis proovida nendevahelist sünkroniseerimist automatiseerida



## Eetikast

- Süsteemiadministraatoritel on tihti juurdepääs paljudele asjadele;
- Teil on kasutajate usaldus ja suur vastutus;
- Austage ja kaitske kasutaja privaatsust;
  - Krüpteerimata varukoopiaid võib tihti leida kõige kummalisematest kohtadest;
- See on midagi, mida siin loengus selgeks ei saa.

# Kasutajate lisamine (Linux)

- `adduser [options] [--home DIR] [--shell|-s SHELL] [--no-create-home] [--uid ID] [--firs-tuid ID] [--lastuid ID] [--ingroup GROUP | --gid ID] [--disabled-password] [--disabled-login] [--gecos GECOS] [--add_extra_groups] kasutajanimi`
- on olemas ka *useradd* ent ei soovita seda kasutada (vt man useradd)
- kasutajaprofiil võetakse */etc/skel/* - seda kujundades on võimalik uusi kasutajaid luua soovitud seadistustega.
- Näide
  - *adduser testkasutaja*
  - [https://wiki.itcollege.ee/index.php/Adduser\\_%26\\_useradd](https://wiki.itcollege.ee/index.php/Adduser_%26_useradd)



## Kasutajate haldus (Linux)

- Kasutaja salasõna muutmine: *man passwd*
  - administraator muudab teiste kasutajate salasõnu:
    - *passwd [kasutaja]*
  - (hetkel sisseloginud) kasutaja muudab oma salasõna:
    - *passwd*
- Kasutaja kustutamine: *man userdel*
  - *userdel [options] kasutaja*
  - *userdel -r student* – kustutab kasutaja student ja tema kodukataloogi
  - salasõna muutmise lukustamiseks (ei lukusta kasutajat): *passwd -l kasutaja*

# Kasutajate haldus (Linux) 2

- `usermod [options] kasutaja`
  - **-u UID**
  - **-g GID**
  - **-G rühmA,rühmB**
  - **-L lukustab kasutaja salasõna**
  - **-U lubab kasutana salasõna**
  - **-p salasõna**
  - **-s shell**
  - **-l uus kasutajanimi**
  - **-c kommentaar**
  - saab muuta ka aegumist
  - **vt `man usermod`**



## Kasutajate haldus (Linux) 3

- Paneme kasutaja lukku
  - **usermod -L <kasutaja>**
  - **usermod -L *student***
- keelame salasõna muutmise
  - **passwd -l *student***
- Teeme kasutaja *student* lukust lahti
  - **usermod -U *student***
- lubame salasõna muutmise:
  - **passwd -u *student***



## Rühmad (Linux)

- Rühma lisamine: **man addgroup**
  - **addgroup** [options] [--gid ID] **grupp**
- Kasutaja lisamine rühma: **man adduser**
  - **adduser** <kasutaja> <grupp>
  - Näiteks järgmine korraldus lisab kasutaja *student1* rühma *students*
    - **adduser student1 students**



## Teave kasutaja kohta

- Kasutaja kohta saab teavet korraldusega **id** (vt **man id**)  
**id** <*kasutajanimi*>
- Kuhu rühma kasutaja kuulub  
**groups** <*kasutajanimi*>  
**getent group** <*kasutajanimi*>
- *man groups*
- *man getent*





## Teave kasutajate ja gruppide kohta

- Kasutajate nimekirja kuvamine  
**getent passwd**
- Gruppide nimekirja kuvamine  
**getent group**
- Kes on hetkel masinasse sisse loginud ja mida teeb: **w**  
(lisateave *man w*)



## Viiteid

- Kerberos protokoll lahtiseletus  
<http://learn-networking.com/network-security/how-kerberos-authentication-works>
- OpenLDAP seadistamise näide  
[http://wiki.itcollege.ee/index.php/OpenLDAP-i\\_seadistamine](http://wiki.itcollege.ee/index.php/OpenLDAP-i_seadistamine)
- Kes on arvutisse loginud ja mida teeb:  
[https://wiki.itcollege.ee/index.php/K%C3%A4sklus\\_w](https://wiki.itcollege.ee/index.php/K%C3%A4sklus_w)
- OSadmin kasutajate haldamise spikker  
[https://wiki.itcollege.ee/index.php/OSadmin\\_spikker#2.\\_KASUTAJATE\\_HALDAMINE](https://wiki.itcollege.ee/index.php/OSadmin_spikker#2._KASUTAJATE_HALDAMINE)

# Küsimused? Tänan tähelepanu eest!



IT KOLLEDŽ  
TALLINNA TEHNIKAÜLIKOOL



**TALTECH IT KOLLEDŽ**

**Raja 4C, 12616 Tallinn**

**tel +372 628 5800**

**info@itcollege.ee**

**<https://taltech.ee/itcollege>**



IT KOLLEDŽ  
TALLINNA TEHNIKAÜLIKOO

## Kasutajate haldamine

Operatsioonisüsteemid ja nende haldamine ICA0001

Edmund Laugasson

[edmund.laugasson@taltech.ee](mailto:edmund.laugasson@taltech.ee)

[https://wiki.itcollege.ee/index.php/User:Edmund#eesti\\_keeles](https://wiki.itcollege.ee/index.php/User:Edmund#eesti_keeles)

Käesoleva dokumendi paljundamine, edasiandmine ja/või muutmise on sätestatud ühega järgnevatest litsentsidest kasutaja valikut:  
\* GNU Vaba Dokumentatsiooni Litsentsi versioon 1.2 või uuem  
\* Creative Commons'i Autorile viitamine + Jagamine samadel tingimustel 4.0 litsents (CC BY-SA)

1 / 27

























































# Küsimused? Täna tähelepanu eest!



IT KOLLEDŽ  
TALLINNA TEHNIKAÜLIKOO



**TALTECH IT KOLLEDŽ**

**Raja 4C, 12616 Tallinn**

**tel +372 628 5800**

**info@itcollege.ee**

**<https://taltech.ee/itcollege>**