Estonian Information Technology College

User management

Operating systems I800

Edmund Laugasson
edmund.laugasson@itcollege.ee

There has been used materials from Margus Ernits, Katrin Loodus when creating current slides.

Threats

- everyday use as regular user
  - even when you are the owner of your computer
  - also malware has same rights
  - avoid system damage (accidental deletion, possible malware
- have you been cleaned your friend’s computer?
- would you like to do that job also in future?

http://www.bordercomputers.co.uk/wp-content/uploads/2013/12/computer-virus-removal.jpg

Threats 2

- keeping secrets
  - when there comes out that one employee was not loyal
  - sold the secrets of the company
  - is it clear which information was accessible?
- minimal necessary rights
  - are annoying
  - are essential

http://1.bp.blogspot.com/-2vKcQeDIoOM/T-i5Tx-N04I/AAAAAAAAFXE/QjS2sW9HtPA/s1600/Permissions-Reset-Icon.png

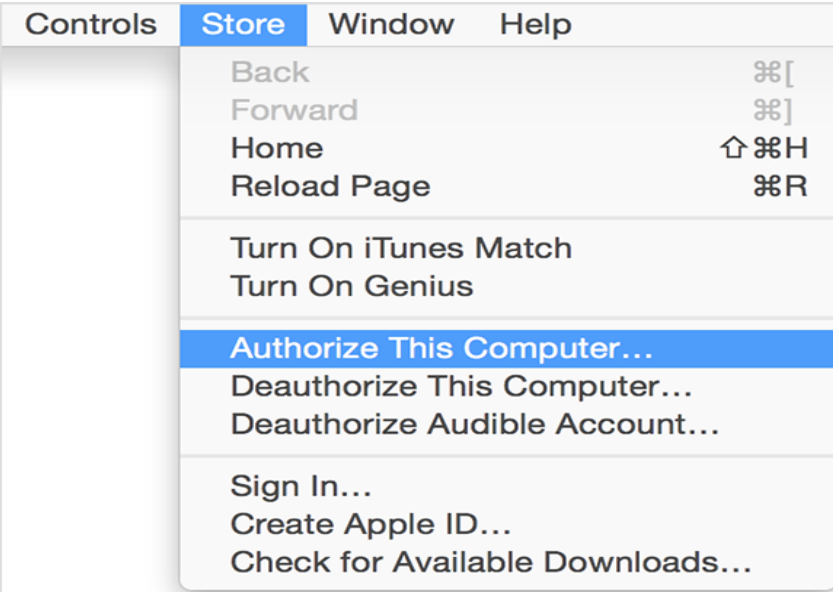
User management

- Changes in information system must leave its trace
  - who and when changed
  - people must be identified
- Modifications in information system data can be carried out only by authorized persons
  - user rights must be checked and regulated (access control managed)

Authentication and Authorization

- personal identification or *authentication*
- *authorization* – access control implementation

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

User

- users entering into information system will be identified
- ensure access only those resources that have been allowed for her/his role – this means: users will be authorized
- information system use and misuse will be watched - this means audited

Authentication

- is used:
  - something that user knows – passphrase (see next slide), PIN
  - something that user owns – smart card, magnetic card
  - something that is part of user – fingerprint and other biometric identification ways

https://upload.wikimedia.org/wikipedia/commons/thumb/8/8f/SecureID_token_new.JPG/220px-SecureID_token_new.JPG

Password -> passphrase

- the following requirements could (should) be met in case of user passphrase
  - must be hard to guess but easy to remember - for example, the total written sentence, including numbers and special characters but do not recommend the use of umlauts in Estonian language
  - length must be at least 8 characters, 20 and more suggested (up to 15-char MS Windows passwords can be cracked in less than 30 minutes) – this all depends on current computing power (see also quantum computers → DWaveSys)
  - should not contain dictionary words
  - should contain capital and small letters, numbers and also special signs
- passwords should not be shared with others (also management responsibility goes together!)
- instead of passwords there should be smart card, biometrics etc preferred
- whenever possible, use multilevel -, -factor authentication
- https://howsecureismypassword.net/ - sometimes useful to check current passwords security
- https://haveibeenpwned.com/ - what has been happened...

User in system

- In case of new user
  - user will be added into appropriate group or role
  - to user will be given password or smart card for identification
- user changes her/his role inside company
  - user will be removed from existing groups/roles
  - user will be added into new groups/roles

User leaves from company

- when user is leaving
  - access will be removed to information system resources
  - user data, also e-mail box will be archived
  - user e-mail will be redirected to another mailbox
  - sometimes user will be removed from system

Processes

- in company there must be written process for user rights sharing, changing, deleting
- thing just do not happen so that sysadmin will choose her-, himself the list of permissions that will be given to new user
- there must be an overview of users rights and roles

User roles

- users belong to roles, e.g.
  - engineer
  - product developer
  - administrator
  - etc
- roles are achieved often with groups
  - group engineers
  - etc
- every role has its own access rights into information system

User ID

- each user has her, his own ID
  - in UNIX-like systems (incl Linux) UID – user ID
    - e.g. 500
    - UID = 0 -> superuser
  - in MS Windows systems SID Security Identifier
    - e.g. S-1-5-21-domain_id-500
    - http://support.microsoft.com/kb/243330

User data

- in Linux-like systems there will be the following information held
  - user name
  - *password* and its *hash*
  - UID (User ID), GID (Group ID)
  - user's home folder (*/home/user*)
  - user's *shell* (usually default *shell*)
  - password and user expiration data

User data will be held

- users and groups data will be held in folders
- in UNIX-like systems (incl Linux, macOS)
  - /etc/passwd there will be held users
    user:x:UID:GID:name,,tel1,tel2:/home/user:/bin/bash
    http://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/
  - /etc/shadow – hash will be kept and account's expiration data (is not readable for everyone – why?)
    http://www.cyberciti.biz/faq/understanding-etcshadow-file/
  - /etc/group - groups
    http://www.cyberciti.biz/faq/understanding-etcgroup-file/
- AD Active Directory
  - Microsoft Windows systems
  - also UNIX-like systems (incl Linux) can authenticate
- multiple server systems
  - (Open)LDAP directory service

Groups

- user has primary group (in Ubuntu same as user name) and secondary groups
  - in Linux use command *id* to see currently logged in user
- e.g. there could be the primary group be users and secondary groups audio, video jne
- with group membership there will be regulated also the access to devices, folders etc
- configuration file: /etc/group
- each group has its own ID – group ID, GID

Central user database

- in large companies there are many servers
  - many of them are Unix ones
  - some also Windows servers
  - many workstations
- Problem: user should be kept in one system
- Solution: LDAP directory
  - as AD (Active Directory)
  - as LDAP+Kerberos
- only those apps should be deployed that support central user authentication
- when there is multiple folders needed to keep user’s data then try to automate data synchronization between folders

About ethics

- sysadmins have quite often access to many things
- you have user’s trust and big responsibility
- respect and protect user’s privacy
  - unencrypted backups can be often found from very strange places
- this (ethics) is something you cannot learn from current lecture

Adding user (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] **username**
- there is also *useradd* but do not suggest to use it (see *man useradd*)
- user profile will be taken from */etc/skel/* - designing this there will be possible new users create with preconfigured settings
- **example**
  - **adduser testuser**
  - http://askubuntu.com/questions/345974/what-is-the-difference-between-adduser-and-useradd

User management (Linux)

- change user password: **man passwd**
  - sysadmin will change other users password:
    - **passwd [user]**
  - (currently logged in) user will change her/his password:
    - **passwd**
- deleting user: **man userdel**
  - **userdel [options] user**
  - **userdel -r student –** will delete user and her, his home folder
  - to lock password without changing it: **passwd -l user**

User management (Linux) 2

- usermod [options] **user**
  - **-u UID**
  - **-g GID**
  - **-G groupA,groupB**
  - **-L locks user password**
  - **-U unlocks user password**
  - **-p password**
  - **-s shell**
  - **-l new username**
  - **-c coment**
  - can changed expiration
  - please see **man usermod**

User management (Linux) 3

- lock user (cannot log in even over SSH)
  - chage -E 0 <user> #set expiry to 01 Jan 1970
  - chage -l <user> #check user expiry information
- unlock user (can log in again, also over SSH)
  - chage -E -1 <user> #set expiry to never
- prohibit change password
  - passwd -l student
- unlock user student
  - usermod -U student
- allow change password:
  - passwd -u student

Groups (Linux)

- add group: **man addgroup**
  - **addgroup** [options] [--gid ID] **group**
- add user to group: **man adduser**
  - **adduser <user> <group>**
  - e.g. user *student1* will be added to group *students*
    - **adduser student1 students**

Information about user

- **id** (please see **man id**)

  id *<user name>*

- which groups user belongs to
  groups *<user name>*

  getent group *<user name>*

- *man groups*
- *man getent*

Information about users and groups

- list users
  getent passwd
- list groups

  getent group
- who is logged in and what is doing: **w**
  (more: *man w*)

Refences

- Kerberos protocol explanation
  http://learn-networking.com/network-security/how-kerberos-authentication-works
- OpenLDAP configuration example (in Estonian)
  http://wiki.itcollege.ee/index.php/OpenLDAP-i_seadistamine
- about w command (in Estonian):
  https://wiki.itcollege.ee/index.php/K%C3%A4sklus_w
- OpenLDAP in Ubuntu -
  https://help.ubuntu.com/lts/serverguide/openldap-server.html
- about w command (in English) -
  http://askubuntu.com/questions/283337/what-does-idle-time-output-from-w-command-tell

Questions?

Thank you for your attention!