User Management and Authentication

- Securing access to a computer
- Operating system boot process
- Login
- Creating and deleting users
- Changing user information
- Group management
- Setting limits
- Authentication

Securing Access (1)

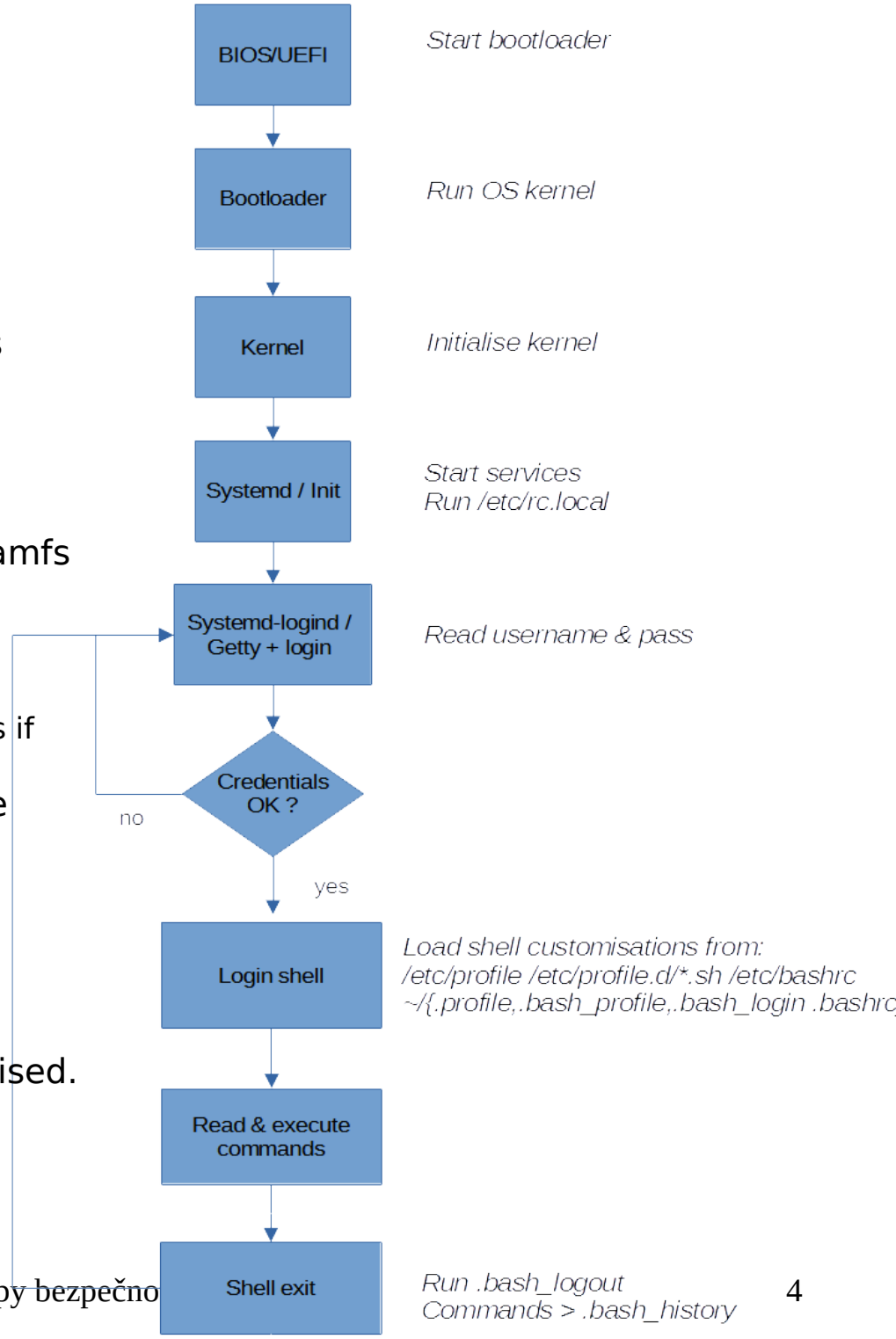
- Physical security
  - Control physical access to machine (also disks and other media).
- Boot medium
  - Set password to BIOS / UEFI, disable booting from removable media
  - When booting from removable media, it is possible to gain access to the filesystem (if not encrypted),
    - Set bootloader password (/boot/grub/grub.conf: password),
    - Change root password.

Securing Access (2)

- Bootloader
  - allows passing parameters to the kernel, e.g. “runlevel”,
  - allows gaining administrator (root) access using “single-user mode” / changing the boot process,
  - set bootloader password
- Root password
  - Root has all privileges in the system.
- Disk encryption
- Securing network, administration interfaces (ILO…)
- Updates,...

Boot Process

- After powering on, BIOS/UEFI loads and executes bootloader.
  - BIOS: loaded from boot sector (MBR).
  - UEFI: loaded from EFI System Partition (ESP).
- Bootloader loads into memory and executes OS kernel (can also load other parts, e.g. initrd/initramfs image).
- Bootloader passes kernel (boot) parameters.
  - e.g. location of the filesystem / (root), runlevel, ...
  - Can be changed during boot (with sufficient privileges if necessary).
- Kernel loads necessary modules, mounts root file system (r/o).
- After initialisation, kernel executes init system.
  - In Linux commonly SysV init (/sbin/init) or systemd.
- Init system loads services and userspace tools, mounts filesystems, and shows a login prompt.
- After successful login, user environment is initialised.



Runlevel

- Current mode of the operating system.
- 7 modes, defined in */etc/inittab* and RC scripts (*/etc/rc[0-6].d*)
  - 0: Halt
  - 1: single-user mode
  - 2 - 4: multi-user mode, text with network
  - 5: multi-user mode, graphical with network
  - 6: reboot
- Switching runlevels - *runlevel, telinit*
- Systemd uses *Systemd targets* instead of “runlevels”.
  - e.g. *multi-user.target* – activates system in multi-user text mode..
  - functionality of “runelvels” for backwards compatibility.

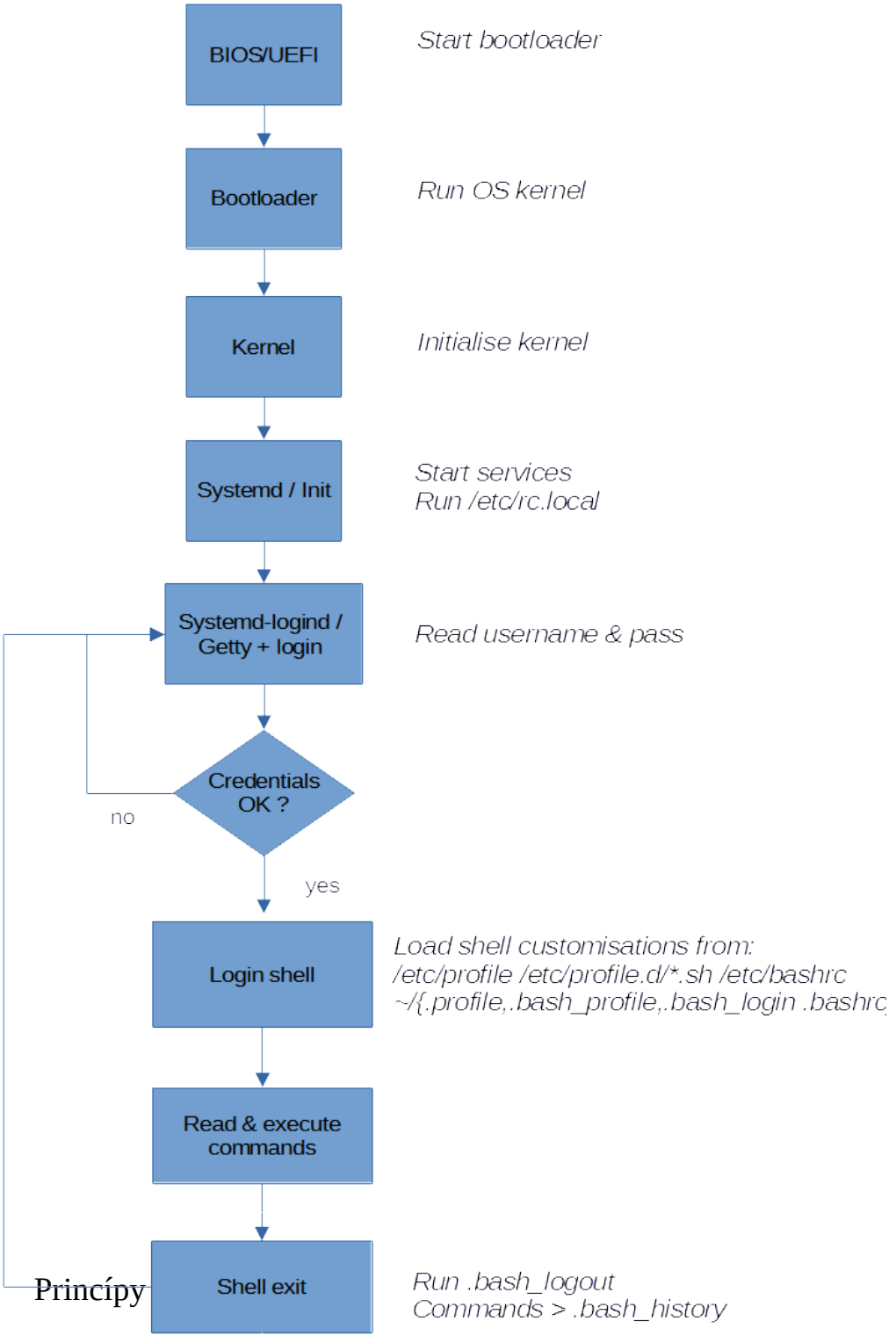
Single-user mode

- Provides only one text console for administrator (root).
- Services (daemons) are not started.
- Does not allow login for normal users.
- Only for maintenance, repairs, configuration.
- Allows gaining exclusive access to the system (without root password), provided:
  - We have access to the console after restart,
  - Possibility to pass kernel boot parameters, e.g. “single” (knowledge of bootloader password).

User in Linux

- A user is someone who has privilege to use the system.
- Assigned a name - **username**.
- Identified by unique **UID.**
- Belongs to a group with unique **GID**.
- Authentication using **username** and **password** (typically).
- Shell is executed after login (command interpreter, e.g. */bin/bash*).

Logging to the terminal



User Database */etc/passwd*

- Colon-delimited fields
- **User name –** 1 – 32 characters
- **Password** – if equals “x”, password is saved as hash in */etc/shadow*
- **UID** – user ID, unique identifier
  - 0 – root,
  - 1-99 – default accounts,
  - 100 – 999 – system accounts (services),
- **GID** – group ID, user’s primary group
- **User information** – additional information
- **Home directory** – absolute path to a directory where the user will end after login. If the directory does not exist, home directory = /.
- **Shell** – absolute path to a command or a command interpreter that will be executed after login (typically */bin/bash*).

Adding a user account

- Adding user with default settings
  - *useradd -m student* (“-m” – create home directory)
- List default settings
  - *useradd -D*
- Change default group
  - *useradd -D -g 4321*
- Testing the login
  - *su - student*

Deleting a user account

- Deleting a user account
  - *userdel student*
- Delete account including files in home
  - *userdel -r student*
- Search for all files belonging to the user
  - *find / -user student*
- Before deleting, it is necessary to end user’s processes

Adding / deleting a group

- Adding a group
  - *groupadd students*
  - *-g gid – specify GID*
  - *-r – create system group*
- Deleting a group
  - *groupdel students*

Adding / deleting manually

- Beware of the correct syntax!
- Users
  - *vipw, vipw -s*
- Groups
  - *vigr, vigr -s*
- Home directory
  - *cp -r /etc/skel/* /home/user/*
- Verify file integrity
  - *pwck, grpck*

Changing a user account

- Change account: *usermod student* (man usermod)
- Change information: *chfn student*
- Change login shellu: *chsh student*
- Change password: *passwd* (for other user only root)
- Change account validity: *chage student*
- Lock account: *passwd -l student*

Limiting login

- Enable login only for root
  - */etc/nologin* – if file exists and is readable
- Set a disallowed shell
  - */bin/false*
  - */sbin/nologin*
  - */usr/sbin/nologin*
- List of allowed: */etc/shells*

User limits (1)

- */etc/security/limits.conf*
- Syntax: <*domain*> <*type*> <*item*> <*value*>
- Domain can be username, groupname, * (default settings)
- Types of limits:
  - *soft* – user can change
  - *hard* – hard limits, user cannot exceed or change
- Check limits:
  - *ulimit -a*

User limits (2)

- *core* – setting size of a core file (KB),
- *fsize* – maximum file size (KB),
- *memlock* – maximum allocated memory (KB),
- *nofile* – maximum number of open files (KB),
- *cpu* – maximum CPU time (KB),
- *nproc* – maximum number of processes (KB).

Linux PAM

- Pluggable Authentification Modules – set of libraries that allows an administrators to set how applications will authenticate the users.
- Respective modules are located in */libs/security*
- Configuration files for applications: */etc/pam.d/**
  - e.g. for sshd: */etc/pam.d/sshd*
- Syntax: <*control*> <*module*> <*arguments*>
- Auxiliary tools are available in modern distros.
  - *authconfig, authselect*

PAM Example

- Authentication to the system using passwords - */etc/pam.d/system-auth*
- “Credit” system (user can get credit for using a special character and set a shorter password).
  password requisite pam_pwquality.so try_first_pass local_users_only retry=3 minlen=14 dcredit=1 ocredit=2 difok=3 authtok_type=
- Using negative credit for requiring a minimum nuber of respective characters.
- Beware of the correct syntax!

su vs. sudo

- su – “switch user”
  - primarily for switching to other user
  - asks for password of the user that we want to switch to
  - *su – user2*
  - configuration using PAM
- sudo – “switch user and do”
  - primarily for executing a command as another user
  - asks for password of the user running sudo
  - *sudo -u user2 id*
  - configuration in file */etc/sudoers*

References

- man command
- https://linux.die.net/
- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/installation_guide/ch-boot-init-shutdown
- https://www.digitalocean.com/community/tutorials/how-to-configure-a-linux-service-to-start-automatically-after-a-crash-or-reboot-part-1-practical-examples