Ligipääsuhaldus

Kaitse ja turvalisus

Operatsioonisüsteemil tuleb:

Kaitse	Turvalisus
• kontrollida juurdepääsu programmide ja arvuti ressursside juurde ja tagada nende säilimine	• ära hoida illegaalne ligipääs süsteemile, andmete hävitamine ja rikkumine
• Andmete juhuslik leke valedele kasutajatele	• Andmete peitmine pahatahtlike kasutajate eest

Ohud

- Ohud ähvardavad mitmest kohast:
  - välised jõud;
    - tulekahjud, üleujutused, sõjad
  - süsteemi enda vead;
  - rakendusprogrammide probleemid;
    - vigased kettad, programmi vead
  - pahalased
    - troojalased, viirused, ussid
  - kasutajad.

Kaitse - eesmärgid

ressursside õige kasutamise kindlustamine	turvapoliitika seadmine
Juba alustades failisüsteemist (NTFS failisüsteem lubab ligipääsuõigusi)	turvareeglite määramiseks Windowsis: *Policy Editor*, (Group Policy Editor – gpedit.msc) *Security template* ja *Security Configuration and analysis* tööriistad (läbi MMC)

Operatsioonisüsteemi turvalisus

Eesmärgid	Ohud
Konfidentsiaalsus	**Andmete lekkimine**
Andmetele tohib ligi pääseda ainult selleks volitatud isikud.	Andmed on lekkinud kolmandatele isikutele.
Terviklikkus	**Andmete muutmine**
Andmed peavad säilima sellisena nagu nad loodi või autoriseeritud isikute poolt viimati muudeti.	Andmed on kustutatud/muudetud/rikutud kolmandate isikute/programmide poolt.
Käideldavus	**Teenuse tõkestus (Dos)**
Teenus/andmed peavad olema kättesaadavad nõutud kiirusel igal ajahetkel.	Nt Interneti veebilehekülg ei avane, kuna sama veebilehekülge tahavad miljonid kasutajad vaadata ja veebiserver on arvestanud tavapärase paari tuhande kasutaja üheaegse kasutusega.

Sissetungijad

- on üldiselt ühes järgmistest kategooriatest:
  - juhuslikud piilujad;
  - süsteemisisesed nuuskurid;
  - rahaahned pahategijad;
  - spionaaž

Kasutajate autentimine

- on esimeseks astmeks süsteemi turvalisuse tagamisel.
- Autentimine peab tegema kindlaks kas isik on see, keda ta ennast väidab olevat:
  - midagi, mis kasutaja teab (parool);
  - midagi, mis kasutajal on;
  - midagi, mis kasutaja on.

Paroolipõhine autentimine

LOGIN: bah

PASSWORD: rUigam

SUCCSESSFUL LOGIN (a)

LOGIN: liina

INVALID LOGIN NAME

LOGIN: (b)

(a) Edukas logimiskatse.

(b) Viga peale nime sisestamist.

(c) Viga peale nime ja parooli sisestamist.

LOGIN: blaah

PASSWORD: p6ssapossa

INVALID LOGIN

LOGIN: (c)

Autentimine

- füüsilist objekti kasutades:
  - magnetkaardid;
  - kiipkaardid
- biomeetriline autentimine:
  - silma võrkkest;
  - sõrmejälg;
  - sõrmepikkus;
  - DNA;
  - hääletuvastus; ...

Riski vähendamine:

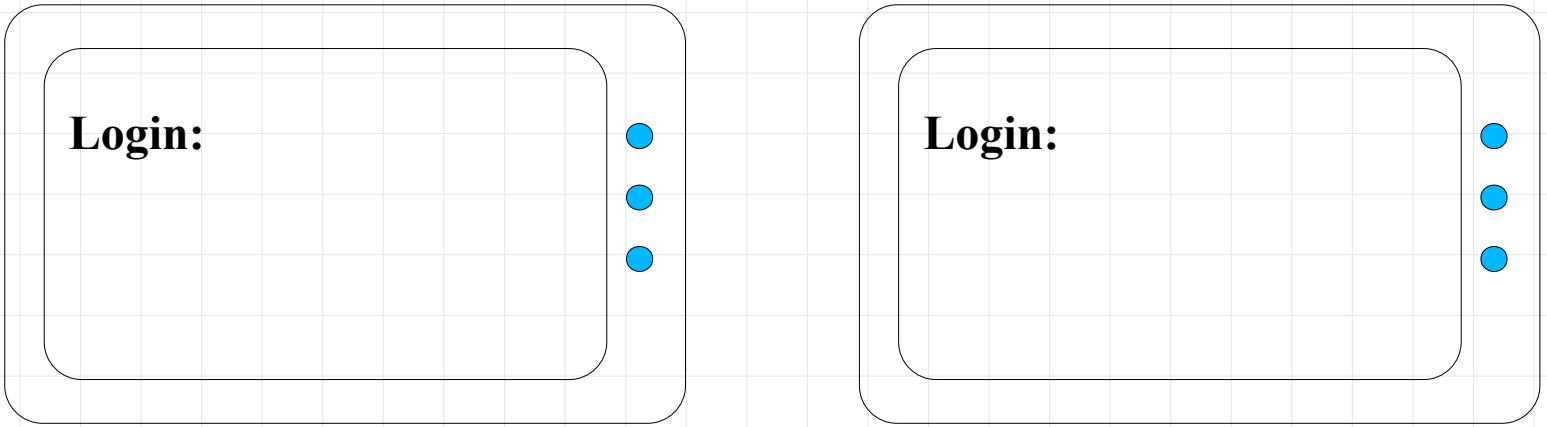
- süsteemi sisselogimise aja piiramine;
- logimiskatsete arvu piiramine;
- andmebaas kõigist logimiskatsetest;
- lõks lihtsa nime-parooli kombinatsiooniga
  - niipea, kui kasutaja end sisse logib, teavitatakse sellest süsteemihaldureid

Programsed ohud

Trooja hobused:

- on vabalt saadavad programmid;
  - sisaldavad koodi/funktsionaalsust, mis on mõeldud kasutajale kahju tegemiseks;
  - kasutaja laeb ise vabatahtlikult endale troojahobusega rikastatud tarkvara ja kasutab seda teadmata, et lisaks see tarkvara korjab ka nt kasutaja paroole ja edastab need Internetti.
- mingi utiliidi asendamine ohvri arvutis:
  - meelitatakse kasutajat seda utiliiti kasutama.

Meldimine



(a) (b)

(a) korrektne meldimisaken

(b) võltsing*

* visuaalne erinevus originaali ja võltsingu vahel puudub.

Salauksed

```
while(TRUE){
        printf(kasutajanimi: ");
        get_string(nimi);
        printf("parool: ");
        get_string(parool);
        enable_echoing();
        v = check_validity(nimi,parool);
        if (v) break;
}
execute_shell(nimi);
```

(a) normaalne kood

```
while(TRUE){
        printf(kasutajanimi: ");
        get_string(nimi);
        printf("parool: ");
        get_string(parool);
        enable_echoing();
        v = check_validity(nimi,parool);
        if (v||strcmp(nimi,"blah")==0) break;
}
execute_shell(nimi);
```

(b) salauksega kood

Jälgimine

- Väljastpoolt tuleva rünnete avastamiseks on vaja süsteemi jälgida:
  - näiteks: valesti sisestatud paroolide sagedus süsteemis;
- Auditi logi
  - seal on kirjas, iga tegevuse aeg ja objektid millal mingi kasutaja objekte kasutab;
- Oma süsteemist turvaaukude otsimine

Krüpteerimine

- tundlikud andmed vajavad salastamist:
  - kasutame krüpteerimist;
- Krüpteerimisalgoritmid:
  - avaliku võtmega
  - salajase võtmega
- Uuemates operatsioonisüsteemides on vahendid krüpteerimiseks juba vaikimisi olemas.
  - Kui krüptimisvõtmed jms kaovad, siis andmeid lugeda ei ole võimalik.

Failide krüptimine

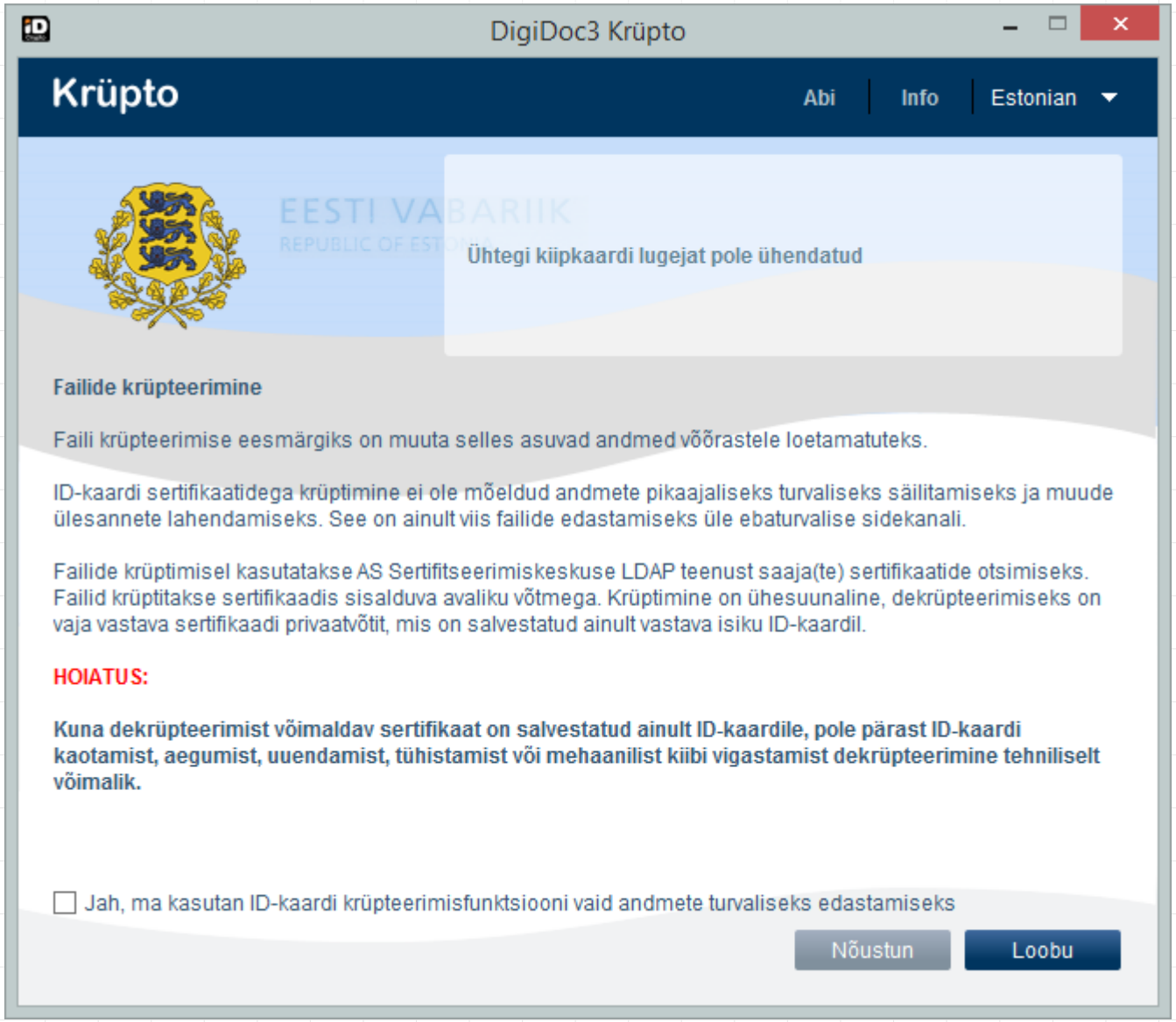
- VeraCrypt
  - Windows, Linux, OS X
  - Truecrypti edukaim järglane
  - https://veracrypt.codeplex.com/
- 7-zip
  - Windows, mitteametlikult ka Linuxi ja OSX jaoks
  - http://www.7-zip.org/
- Bitlocker (Windows 8 Pro ja enterprise)

Failide krüpteerimine

Digidoc3 krüpto

Krüpteerimiseks kasutatakse kasutaja ID-kaarti.

Nagu programm ise ütleb, ei ole mõeldud andmete pikaajaliseks säilitamiseks, kuna ID-kaardi vahetusega ei ole enam andmeid võimalik lahtikrüptida.



Süsteemi ohud

- Viirus on programm, mis teeb endast koopiaid:
  - lisades oma koodi muu programmi külge;
  - võib teha kurja.
- Uss on protsess, mis käivitab endast uusi koopiaid:
  - eesmärgiks on süsteemi jõudluse vähendamine
- Teenuse tõkestus DoS (*Denial of Services*):
  - serverid koormatakse üle suure päringute hulgaga.

Viiruse eesmärgid:

- Väljapressimine;
- Teenuse tõkestus viiruse töö vältel;
- Riistvara kahjustamine;
- Konkurendi arvutis:
  - kahju tegemine;
  - spionaaž;
  - valeandmete sisestamine.

Viiruse töö põhimõte

- Võib olla kirjutatud assembleris
  - Tänapäeval ka kõrgema taseme programmeerimiskeeltes
- Lisatakse teise programmi
  - spetsiaalse utiliidi „dropperi“ abil
- Aktiveerub programmi käivitamisel
  - nakatab teisi programme
  - lisaks nakatumisele täidab ka oma „ülesannet“
- Viirused on platvormispetsiifilised

Viiruste levimine

- Veeb, FTP, ..
- Kopeerimise järel:
  - nakatab failid kõvakettal;
  - võib üritada nakatada lokaalvõrku;
- Manusena e-maili küljes:
  - kasutab kasutaja aadressiraamatud edasiseks levimiseks.

Viirusetõrje

- Terviklikkuse kontroll;
- käitumise kontroll;
- viiruste vältimine:
  - hea operatsioonisüsteem;
  - installeerida ainult usaldusväärset tarkvara;
  - kasutada antiviirusprogrammi (sagedased uuendused);
  - ei tohi käivitada suvalisi manuseid;
  - sagedane varukoopiate tegemine.

Kui viirus on sisse pääsenud?

- Kuidas aru saada:
  - süsteem ei toimi nii, nagu vaja;
  - võrguliiklus on suurenenud
  - viirusetõrje programm ütleb nii.
- Viiruse rünnakule vastamine:
  - seisata arvuti;
  - teha puhtalt kettalt alglaadimine;
  - käivitada viirustõrje programm.

Näited viirustest

- Bad Brian – esimene viirus (1986)
- CIH.1003 – kirjutab üle arvuti kõvaketta ja võimaluse korral ka BIOS'i
- Värskeimad pahalased (Symantec jaotuse järgi):
  - Threat Explorer - Symantec
    http://www.symantec.com/norton/security_response/threatexplorer/index.jsp

Viirustest veel

- Kirjeldusi viiruste kohta ja ravi: antiviirusprogrammide tootjate kodulehtedel
  - www.symantec.com
  - www.mcafee.com
  - Www.avast.com
  - ...

Kodune ülesanne 6p

- Kursuse wikilehele on üles laetud (laetakse) krüptitud fail.
  - See sisaldab ülesandeid ja lahendamiseks vajalikke faile.

Kõik