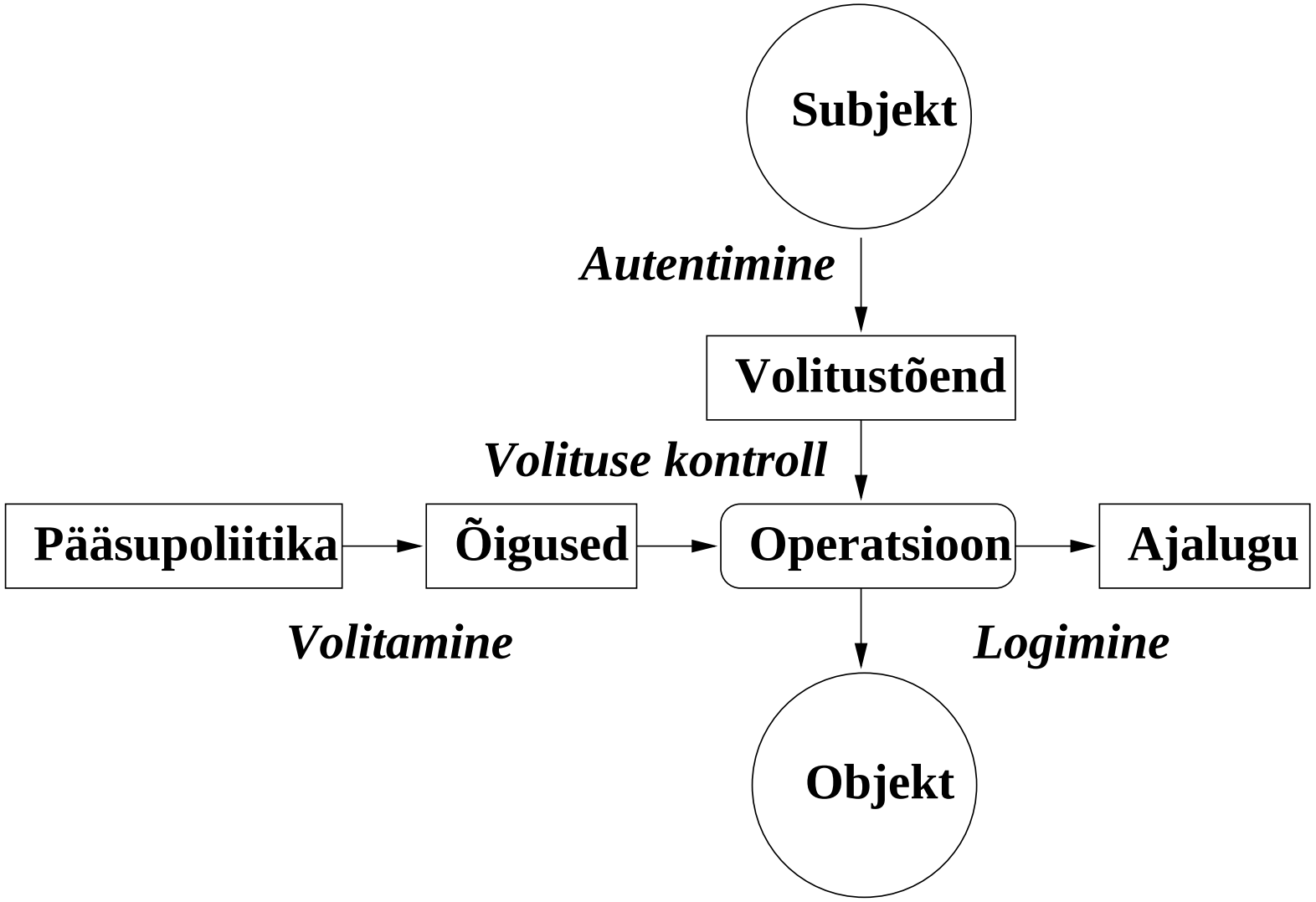
Autentimine

- Mitmekasutajasüsteemid
- Autentimismeetodid
- Autentimisprotsess
- Paroolid
- Biomeetrilised tõendid
- Elektroonilised volitustõendid
- Paroolkaitse näide: Unix
- Võrguautentimissüsteemid
- *Single sign-on*

Mitmekasutajasüsteemid

- Probleem:
  - Hulk kaitstavaid objekte (failid, kirjed, kataloogid, seadmed, . . .)
  - Hulk juurdepääsu omada võivaid subjekte (inimesed, protsessid, . . .)
- $\Rightarrow$ Vaja kasutajaid eristada
- Autentimine vs. identifitseerimine

Juurdepääsu kontroll



Autentimismeetodid

- Teadmuspõhised
  - Luku kombinatsioon
  - Parool
  - PIN-kood
  - Krüptovõti
  - Isikuandmed
  - ...

Autentimismeetodid

- Esemelised
  - Luku võti
  - Magnet- või kiipkaart
  - Infrapunamärk
- Biomeetrilised
  - Sõrmejälg
  - Silma iiris
  - Hääl
  - DNA

Autentimisprotsess

- Ühepoolne
- Kahepoolne
- Kolmepoolne
  - Vahendusrežiimis
  - *On-line*-režiimis
  - *Off-line*-režiimis

Paroolid

- Entroopia — parooli tugevuse mõõt
- Ründed:
  - Paroolide ära arvamine
    - Kogemusele tuginedes
    - Kõigi paroolide proovimise teel
    - Sõnastikurünne
    - Pöördkodeerimine
  - Õige parooli hankimine
  - Paroolkaitsest mööda hiilimine

Elektroonilised volitustõendid

- Magnetkaart
  - Vesimärgiga
  - Kahekihiline
  - Wiegandi kaart
  - Pääsudiskett :-)
- Kiipkaart, kiiplipik
  - Mälukaart (kaitsega ja kaitseta)
  - Turvaloogikaga mälukaart
  - Protsessorkaart
  - Võib olla kontaktivaba
- Pultkaart
- Raadiosageduslikud tõendid (RFID)

Biomeetrilised tõendid

- Anatoomilised
  - Sõrmejälg
  - Sõrme kuju
  - Nahapoorid
  - Käelaba
  - Käe veenid
  - Silma võrkkest
  - Silma vikerkest
  - Nägu

Biomeetrilised tõendid

- Käitumuslikud
  - Allkiri
  - Kõne
  - Tippimisrütm
- Muud
  - Lõhn
  - DNA struktuur

Paroolkaitse näide — Unix

- Parooli seadmisel genereeritakse juhuarv ("sool", 2 tähte)
- Parool koos soolaga räsitakse, meelde jäetakse sool ja räsi
- Kontrollil räsitakse kontrollitav parool samamoodi
- Uuemal ajal kasutatakse ka muid algoritme, MD5 räsi näiteks
- Algselt oli räsi kõigile näha (`/etc/passwd`), see lihtsustas ründeid
- Praegusel ajal kaitstakse räsisid muust kasutajainfost paremini (`/etc/shadow`)
- Autentimisinfo koosneb kolmest failist (eelnevad ja `/etc/group` grupikuuluvuste jaoks)
- Gruppidel paroole reeglina pole (on olnud)

Paroolkaitse näide — Windows NT

- Mitu eri meetodit, vaatleme NTLM (*NT/Lan Manager*) ja NTLMv2
- Andmebaasis (SAM) hoitakse räsisid (kumbki 16 baiti)
- NTLM: parool 14 baiti (2x7), suurtähtedeks, kummastki poolest DES võti, krüptitakse fikseeritud string
- NTLMv2: parool konverteeritakse Unicode'i, rakendatakse MD4 räsifunktsiooni
- Kaugautentimisel piisab räsist (Unixi puhul on algne parool vajalik)

NIS

- NIS — *Network Information System*, tuntud ka YP (*Yellow Pages*) nime all
- Sun'i vana süsteem `passwd`, `shadow`, `group` jms tabelite üle võrgu kasutamiseks
- Domeen — sama autentimisinfot kasutavate masinate hulk
- Domeenis oli primaarne server ja sekundaarsed
- Andmete muutmine käis peaserveris, sekundaarsed hoidsid koopiat ja jagasid seda
- Kliendid esitasid üle võrgu serverile `getpwent()` jms päringuid
- Protokollid kasutavad kaugprotseduure (SunRPC)
- Turvalisust eriti polnudki

NIS+

- NIS edasiarendus (sisuliselt hoopis uus süsteem)
- Domeenid on hierarhilised
- Igal domeenil on endiselt primaarne ja sekundaarsed serverid
- Alamdomeenidel on võimalik erinev administratiivne alluvus
- Lisatud turvalisus!
- Domeenide hierarhias ja tabelites saab kehtestada juurdepääsuõigusi
- Endiselt saab kasutada lisaks süsteemsetele ka kasutaja defineeritud tabeleid

NIS+ tööpõhimõte

- Kasutatakse turvalisi kaugprotseduure (Secure RPC) — krüptimise ja iga päringu autentimisega
- Krüptimiseks DES, autentimiseks Diffie-Hellmanni võtmevahetus
- Kliendid tunnevad serverit ja server kliente (hostivõtmete abil)
- Kasutaja logib klientmasinasse sisse nime ja parooliga
- Kasutajal on ka NIS+ parool (enamasti sama, mis harilik parool)
- NIS+ paroolist tuletatakse DES võti (≤ 40 bitti entroopiat)
- Avalikust NIS+ tabelist saadakse oma Diffie-Hellmanni võtme krüptitud salajane osa
- See krüptitakse lahti ning selle abil saadakse juurdepääs NIS+ serverile (saab oma parooli vahetada jms)

Kerberos

- Korraliku krüptoga võrgus autentimise süsteem
- Süsteemis on kliendid (kasutajad ja programmid) ning teenused
- Kliente ja teenuseid kokku nimetatakse osapoolteks (*principal*)
- Osapooltele antakse nimed järgmisel kujul:
  `nimi[/täpsustus]@piirkond`.
  Näiteks `mroos@UT.EE`, `mroos/nuuskur@UT.EE`
- Täpsustusega nimi on sõltumatu ilma täpsustuseta samast nimest
- Kliendid kasutavad enda teenustele autentimiseks pileteid (*ticket*)
- On olemas spetsiaalne esmane pilet teiste piletite saamiseks — piletite hankimise pilet (TGT — *Ticket Granting Ticket*)

Kerberose tööpõhimõte

- Klient logib Kerberos-süsteemi parooliga sisse
- Saadab võtmejaotuskeskusele (KDC — *Key Distribution Center*) päringu
- KDC saadab talle tema parooliga krüptitud piletite hankimise pileti
- Klient tahab logida masinasse `math.ut.ee`, selleks vajab ta piletit osapoolele `host/math.ut.ee@UT.EE`
- Klient küsib selle pileti TGT abil võtmejaotuskeskuselt ja esitab selle `math.ut.ee`-le enda autentimiseks
- `math.ut.ee` kontrollib seda võtmejaotuskeskusest
- Klient säilitab oma pileteid kuni väljalogimiseni või nende aegumiseni, et ei peaks kogu aeg küsimas käima

Klassikaline NT domeen

- Windowsi võrk, kus on üks ühtne kasutajatebaas
- Klientmasinates võib olla ka kohalikke kasutajaid
- Domeeni kasutajatebaas on domeenikontrolleris (*Domain Controller*)
- Saab teha sekundaarseid domeenikontrollereid, kuid muutmine käib ikka primaarselt kontrollerilt
- Mitme domeeni vahele saab lisada ühesuunalise usaldussuhte (*trust*)
- Klient saab Netlogon-teenuse kaudu omale SID'id DC käest
- Võrguteenusele esitatakse kliendi õigused ning teenus saab nende abil kliendina esineda

NT domeen koos Kerberosega

- Kasutusel alates Windows 2000
- Domeen on Kerberose piirkond
- Kerberose TGT-le lisab KDC NT-spetsiifilise laienduse turvainfoga (SID'id) ja signeerib selle
- TGT seest kopeeritakse see info harilike piletite sisse
- Autentimine toimub Kerberosega, teenused saavad NT kasutajainfo piletite laiendusest
- Ühilduvuse huvides toetatakse vaikimisi ka NTLM autentimist

Unixi Kerberose ja Windowsi Kerberose ühilduvus

- Windows NT Kerberos on pooleldi ühilduv Unixi Kerberosega:
  - Ainult nimel baseeruv autentimine toimib mõlemas suunas
  - Unixi KDC-d NT domeenikontrollerina kasutada ei saa (puudub NT kasutajainfo)
  - Saab kasutada piirkondade vahelist usaldamist: kasutajad on Unixi Kerberose piirkonnas, NT piirkonnas olev KDC lisab NT kasutajainfo

Active Directory

- Windows 2000 domeenide infot jagatakse *Active Directory* abil
- Hierarhiline domeenide süsteem
- Seotud Interneti (DNS) masinanimedega
- *Active Directory* on realiseeritud LDAP kataloogi baasil
- 3 sorti usaldust domeenide vahel:
  - Kahesuunaline transitiivne usaldus
  - Ühesuunaline usaldus (mitte transitiivne, nagu NT4)
  - Ristusaldus — domeenipuus otseteede tekitamine kiiruse huvides

Muud hajusad autentimissüsteemid

- LDAP kataloogi kasutajainfo levitamiseks võib kasutada *Active Directoryst* sõltumatult ka näiteks Unixi kasutajainfo levitamiseks
- LDAP kataloge (ka *Active Directory* sees) saab replitseerida — jõudluse ja töökindluse huvides
- NDS — *Netware Directory Services*
- PAM ja NSS kui autentimise programne liides

Single sign-on

- *Single sign-on* — kasutaja logib sisse korra oma töökohalt ja saab kasutada kõiki talle lubatud ressursse ilma edasise autentimiseta
- Realiseeritav näiteks parooli mällu jätmise, NTLM autentimise või Kerberose abil
- Hea:
  - Mugav
  - Paremini tsentraalselt hallatav (kui süsteemi tuntakse)
- Halb:
  - Vähem turvalisem
  - Keerulisem süsteem $\Rightarrow$ vigu rohkem
  - Keerulisem süsteem $\Rightarrow$ raskem aru saada, et õigesti konfigureerida