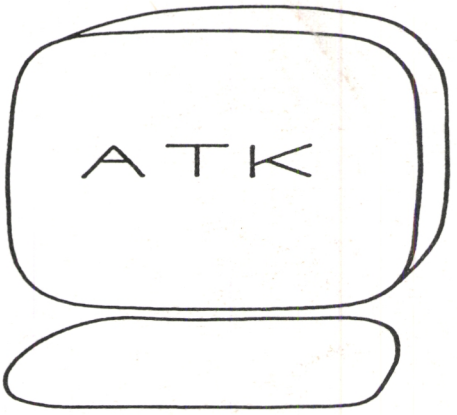
METSÄNTUTKIMUSLAITOKSEN
TIEDONANTOJA 254

Matemaattinen osasto

TURVALLISUUSNÄKÖKOHDISTA JA SUOJAUKSISTA METSÄNTUTKIMUSLAITOKSEN ATK-JÄRJESTELMISSÄ

Kari Lehto



Helsinki 1987

Helsinki 1987. Valtion painatuskeskus

Metsäntutkimuslaitoksen tiedonantoja 254

TURVALLISUUSNÄKÖKOHDISTA JA SUOJAUKSISTA METSÄNTUTKIMUSLAITOKSEN ATK-JÄRJESTELMISSÄ

Kari Lehto

Helsinki 1987

ISBN 951-40-0856-1
ISSN 0358-4283

Valtion painatuskeskus 1987

ALKUSANAT

Tietokone on tehokas laite, oli se sitten iso keskustietokone tai pieni mikrotietokone. Olemme tulleet siitä riippuviksi monissa tutkimus-, kehitys- ja rutiinitöissä. Mutta tehokkuudella on kääntöpuolensa: tietokoneella voidaan tehokkaasti tehdä vahinkoa, joko vahingossa tai tahallisesti. Myös laitteistohäiriöt saattavat aiheuttaa suurta haittaa toiminnalle. Menetykset mitataan joskus suoraan rahassa, joskus ne merkitsevät päiviä tai viikkoja kestäneen työn uudelleen tekemistä.

Monet tietokoneen ja sen muistivälineiden väärinkäytökset voidaan estää järjestelmän vastuuhenkilön ja käyttäjien yhteistyöllä. Käyttäjien puolelta tärkeintä on salasanojen kunnollinen ylläpito ja tiedostojen suojaaminen. Kokemus on osoittanut, ettei pyrkimys estää väärinkäytökset ole turhaa vainoharhaisuutta (edes valtion tutkimuslaitoksissa).

Suunnitelmallisella toiminnalla voidaan vähentää myös muita vahinkoja tai ainakin niiden vaikutuksia. Varmuuskopiointi, tietolevykkeiden oikea käsittely ja dokumentointi ovat tästä esimerkkejä.

Tämän julkaisun tarkoituksena on olla johdatus atk-turvallisuuden laaja-alaiseen aihepiiriin sekä esittää ne atk-turvallisuuden perusasiat, jotka jokaisen Metsäntutkimuslaitoksessa tietokonetta käyttävän tulee tuntea ja ottaa käytännössä huomioon. Keskus- ja mikrotietokoneisiin liittyvien yleisten näkökohtien lisäksi julkaisussa on keskitytty erikoisesti VAX/VMS-käyttöjärjestelmän salasanahallintaan ja tiedostosuojaukseen. Tarkoituksena ei ole ollut tarjota kattavaa kuvausta aihepiiristä eikä käsitellä tiedonhallinnan käytännön järjestelyjen erityiskysymyksiä.

Luvut 1, 2.1, 2.6, 3, 4 ja 5.1 on tarkoittu jokaiselle Metsäntutkimuslaitoksen tietokonekäyttäjälle. Mikrotietokoneiden käyttäjien on lisäksi hyvä tutustua lukuihin 2.4, 2.5 ja 7. Näissä luvuissa on esitetty tarpeellinen perustietous atk-turvallisuudesta ja tiedostosuojauksista sekä mikrotietokoneiden ja levykkeiden hoidosta. Muut luvut sisältävät lisämateriaalia, johon jokaisen käyttäjän ei ole välttämätöntä tutustua. Ne voi lukea myöhemmin tarpeen tai kiinnostuksen mukaan.

Henkilöille, jotka eivät itse käytä tietokonetta mutta ovat kiinnostuneet atk-turvallisuudesta (esimerkiksi esimiesaseman vuoksi), suositellaan lukuja 1, 2 ja 3. Nämä luvut tarjoavat yleiskuvauksen ongelma-alueesta, toimintamenetelmistä sekä eri käyttäjien ja käyttäjäryhmien tehtävistä.

SISÄLLYSLUETTELO

1 JOHDANTO

Atk-turvallisuuteen liittyvät asiat ovat tällä vuosikymmenellä tulleet entistä ajankohtaisemmiksi. Tähän ovat vaikuttaneet muun muassa seuraavat seikat:

- Tietokoneiden käyttö on lisääntynyt niin julkishallinnon piirissä kuin liikeyrityksissäkin. Suuria tietojärjestelmiä ja -rekistereitä on rakennettu, ja tietoliikenneyhteydet ovat laajentuneet. Pankit ovat siirtymässä ajantasaisiin järjestelmiin, joihin voidaan olla yhteydessä eri konttoreista ja joissakin tapauksissa kotitietokoneistakin käsin.

- Yhä useammat rutiinitoiminnat virastoissa ja yrityksissä on siirretty kokonaan tietokoneella hoidettaviksi. Myös suunnittelumenetelmiä on automatisoitu. Näin on saavutettu kiistattomia etuja, mutta työskentely on samalla tullut riippuvaksi tietokonelaitteiden ja -ohjelmien toimivuudesta sekä monista tietojen hallintaan liittyvistä tekijöistä.

- Arkaluontoisia aineistoja säilytetään yhä enemmän tietokoneen muistivälineillä. Esimerkkeinä voidaan mainita erilaiset henkilörekisterit sekä aineistot, jotka sisältävät yritysten liikesalaisuuksia.

- Kotitietokoneiden yleistyminen sekä nuorison kasvanut atk-harrastus todennäköisesti lisäävät puhelinlinjojen kautta tapahtuvia tunkeutumisyrityksiä tietokonejärjestelmiin.

Atk-väärinkäytöksistä on silloin tällöin kerrottu lehtien palstoilla. Kuitenkin vain pieni osa selville saaduista väärinkäytöksistä julkistetaan, sillä yritykset (etenkin pankit ja vakuutuslaitokset) pelkäävät menettävänsä maineensa ja yleisön luottamuksen, jos niiden atk-järjestel-

mien puutteellisuus ja haavoittuvuus tulevat julki. Yritykset todennäköisesti nuolevat usein itse haavansa ja rankaisevat väärinkäyttäjää yksityisesti (esim. erottamisella), mikäli hän kuuluu omaan henkilökuntaan.

Tietotekniikan käyttöön liittyneet vakavat häiriöt ja rikokset yhdistetään yleensä suuriin tietojärjestelmiin, jotka eivät ole tavallisen kansalaisen ulottuvilla. Usein luullaan, ettei vastaavia tapauksia voi esiintyä mini- tai mikrotietokonetta käytettäessä. Kuitenkin henkilökohtaisten tietokoneiden suorituskyky on nykyään sama tai suurempi kuin mitä keskitettyihin konehuoneisiin sijoitettujen suurten tietokoneiden suorituskyky oli kymmenisen vuotta sitten. Sekä isolla että pienellä tietokoneella voidaan sekunnissa tuhota vuosien työ vahingossa tai tahallaan.

Itse asiassa pieni tietokone tai sen levykkeet on paljon helpompi varastaa kuin suurikokoinen, suljettuun konehuoneeseen sijoitettu tietokone. Pienellä henkilökohtaisella tietokoneella ei myöskään ole ympärillään sitä suojaavaa psykologista kehää, joka ainakin ennen verhosi suuria, mystisiä "sähköaivoja". Se rinnastetaan ennemminkin videoihin ja konttorikoneisiin.

Minkälaisia atk-väärinkäytöksiä sitten voi tutkimuslaitoksessa esiintyä? Ensinnäkin on muistettava, että tietokoneaika, muistikapasiteetti ja yleiset ohjelmistot ovat laitoksen omaisuutta eivätkä julkisia resursseja. Niitä saa käyttää vain siihen oikeutettu henkilö, ja hänkin vain tavalla, joka vastaa hänen työtehtäviään laitoksessa. Kiellettyä on luonnollisesti laitoksen resurssien käyttö työntekijän omiin liiketoimiin.

Tietokoneresurssien luvattoman käytön lisäksi atk-väärinkäytöksiksi voidaan katsoa ilman erityistä lupaa tapahtuva ohjelmistojen ja luottamuksellista tietoa sisältävien tie-

dostojen kopiointi omiin tai ulkopuolisten henkilöiden tarkoituksiin. Myös toisen käyttäjän tiedostojen muuttaminen ja tuhoaminen kuuluvat samaan kategoriaan. Tiedostojen muuttamisessa voi kyseeseen tulla vahinko tai pahanilkisyys, ehkä myös hyötymistarkoituksessa tehty petos. Varsinkin ulkopuoliset systeemiin tunkeutujat voivat aiheuttaa paljon vahinkoa tahallaan tai taitamattomuuttaan.

Luottamuksellisten tietojen "vuotaminen" ulos valtion laitoksesta voi merkittävästi vahingoittaa laitoksen mainetta sekä haitata tutkimus- ja palvelutehtävien suorittamista jatkossa. Esimerkiksi Metsäntutkimuslaitos kerää yrityksiltä ja eri organisaatioilta paljon tietoja, joita sellaisenaan ei ole tarkoitettu julkisuuteen tai asiattomille.

Tietojenkäsittelytoiminnalle voi varsinaisten väärinkäytösten lisäksi aiheutua haittaa myös esimerkiksi varmuuskopioinnin laiminlyömisestä, levykkeiden ja magneettinauhojen huolimattomasta käsittelystä ja säilytyksestä sekä tietojärjestelmien dokumentoinnin puutteellisuudesta. Viimeksi mainitun tekijän sisältämä riski on erityisen huomattava silloin, kun ainoastaan yksi henkilö tuntee dokumentoimattoman järjestelmän. Onhan nimittäin aina mahdollista, että kyseinen henkilö ei yllättäen enää olisikaan käytettävissä (vaihtaa työpaikkaa, tulee työkyvyttömäksi, kuolee).

Kahdessa seuraavassa luvussa kuvataan atk-turvallisuuden osa-alueita ja käsitellään yksittäisten käyttäjien ja käyttäjäryhmien vastuuta suojauksista. Luvuissa 4, 5 ja 6 kerrotaan VAX/VMS-käyttöjärjestelmän suojausmenetelmistä, ja luvussa 7 keskitytään erityisesti mikrotietokoneisiin liittyviin turvallisuusseikkoihin.

2 ATK-TURVALLISUUDEN OSA-ALUEITA

Menetelmät tietokonejärjestelmän turvaamiseksi ja tiedostojen suojaamiseksi voidaan jakaa neljään luokkaan:

- laitteiden ja muistivälineiden fyysinen suojaus
- käyttöoikeuksien tarkistaminen
- tietojen koodaus salakielelle
- varautuminen vahinkoihin

Atk-turvallisuus laajassa merkityksessä sisältää myös käytön turvallisuuden, johon kuuluvat muun muassa

- yhteensopivuuden varmistaminen
- tiedotus, koulutus ja dokumentointi

Tässä luvussa kerrotaan pääpiirteittäin kuhunkin luokkaan kuuluvista seikoista. Osa asioista soveltuu monen käyttäjän tietokonejärjestelmiin, osa henkilökohtaisiin tietokoneisiin ja osa molempiin. Henkilökohtaisten tietokoneiden turvallisuusnäkökohtia käsitellään lisää luvussa 7.

2.1 LAITTEIDEN JA MUISTIVÄLINEIDEN FYYSINEN SUOJAUS

Tietokonelaitteiden, levyasemien, levykkeiden ja magneettinauhojen fyysinen suojaus tulipaloa, varkautta, vahingontekoa yms. vastaan on tärkeä atk-turvallisuuden osa-alue. Ei tule kuitenkaan unohtaa, että myös paperilistat ovat muistivälineitä. Luottamuksellisia tietoja sisältävien paperidokumenttien jättäminen esille voi tehdä tyhjäksi kaikki muut turvatoimenpiteet.

Suuret ja keskisuuret tietokoneet sekä niiden levy- ja magneettinauha-asemat suojataan yleensä sijoittamalla ne erilliseen konehuoneeseen, johon pääsy on valvottua tai joka

ainakin on lukittu. Konehuonetta pyritään suojelemaan tulipalolta sekä savu- ja vesivahingoilta ja sen ilmankosteutta ja lämpötilaa valvotaan. Häiriötön sähkönsaanti yritetään myös turvata. Jos talossa on operaattori huolehtimassa magneettinauhapalveluista, ei konehuoneeseen pitäisi olla pääsyä muilla kuin operaattoreilla ja tietokonejärjestelmän toiminnasta huolehtivilla henkilöillä.

Lisääntyneet tiedonsiirtoyhteydet aiheuttavat omat ongelmansa. Periaatteessa televerkon salakuuntelu sekä verkkoon kytkeytyminen on mahdollista käyttäen hyväksi teknisiä apuvälineitä. Tärkein suojausmuoto on estää käsiksipääsy tilaajajohtoon ja erityisesti sen eri kytkentäpisteisiin (talojakamoon ja keskustiloihin).

Henkilökohtaisia tietokoneita ei tulisi sijoittaa pölyisiin tai tupakansavuisiin paikkoihin tai tiloihin, joihin ulkopuoliset pääsevät vapaasti ilman valvontaa. Jos niiden käyttötarkoitus sallii, ne pitäisi sijoittaa huoneisiin, jotka on mahdollista lukita. Ikkunan ääreen sijoittaminen ensimmäisessä kerroksessa ei ole suositeltavaa, ellei laitteita ole kiinnitetty siten, että siirtämiseen tarvitaan erityistoimia. Ei ole myöskään hyvä, että laite joutuu alttiiksi kuumalle auringonpaisteelle tai lämpöpatterin välittömään läheisyyteen.

Huoltohenkilökunnan henkilöllisyys tulisi aina todeta. Jollei ole mahdollisuutta valvoa mikrotietokoneen huoltoa, on sen ajaksi syytä poistaa luottamukselliset tiedot kiinteältä levyasemalta sekä sijoittaa tärkeimmät levykkeet lukittuun kaappiin tai toiseen huoneeseen. Näin huoltohenkilöstö ei joudu turhaan epäilyksen alle (tai kiusaukseen).

Magneettinauhat (ainakin tärkeimmät) tulisi säilyttää tulenkestävissä kaapeissa. Varsinaiset datakaapit on suunniteltu juuri magneettinauhoja varten ja ne suojaavat nauhoja yli +75°C:n lämpötilalta. Levykkeet tuhoutuvat kuitenkin jo

pienemmissä lämpötiloissa, joten niiden perusteelliseksi suojaamiseksi kuumuudelta ja savulta tulisi käyttää erityisiä diskettikaappeja. Kaappien ovet on muistettava pitää kiinni virka-ajan ulkopuolella. Jos katsotaan, että näin täydellinen levykkeiden suojaaminen ei ole tarpeen, voidaan käyttää levykkeitä varten suunniteltuja yksinkertaisia, lukittavia säilytyslaatikoita. Nämä laatikot suojaavat levykkeitä melko hyvin vesi- ja savuvahingoilta ja jossain määrin myös lämmöltä, mutta eivät varkaudelta. Niitä olisikin hyvä säilyttää lukitussa teräskaapissa.

2.2 KÄYTTÖOIKEUKSIEN TARKISTAMINEN

Käyttöoikeuksia tarkistetaan esimerkiksi silloin, kun henkilö yrittää ottaa yhteyden tietokoneeseen, kun hän haluaa suorittaa tiettyjä erityiskomentoja tai -ohjelmia tai kun hän haluaa käsitellä toisen käyttäjän tiedostoja. Näin pyritään huolehtimaan siitä, että käyttäjät eivät voi tehdä tietokoneella sellaista, mihin heillä ei ole oikeutta.

Pääsy käyttämään tietokonetta perustuu yleensä muistettaviin salasanoihin, joiden pohjalta muut käyttöoikeudet myönnetään. Tällainen suojausjärjestelmä sisältyy useimmissa tapauksissa kokonaan tietokoneen käyttöjärjestelmään, mutta jos käyttöjärjestelmän salasanahallinta ei ole riittävän hyvä, voidaan lisänä käyttää tietokoneen ja puhelinlinjojen väliin sijoitettavaa mikroprosessoriohjattua salasananhallintalaitetta (PPD, port protection device). Toinen mahdollisuus on "takaisinsoittolaite" (call-back device), joka pitää yllä listaa käyttäjätunnuksista, salasanoista ja niihin liittyvistä puhelinnumeroista. Kun puhelinlinjan välityksellä yhteyden ottanut soittaja on antanut hyväksyttävän tunnuksen ja salasanan, katkaisee laite yhteyden ja soittaa itse takaisin tunnusta vastaavaan puhelinnumeroon.

Käyttöoikeuksien tarkistaminen voi perustua joko siihen, kuka henkilö on, mitä hän osaa, mitä hän tietää (muistaa) tai mitä hän omistaa. Salasanajärjestelmä on tyypillinen esimerkki menetelmästä, joka pohjautuu siihen, mitä henkilö tietää. Osaamiseen perustuu esimerkiksi nimikirjoitus, joka yksinään käytettynä on epäluotettava tunnistusmenetelmä. Sormenjäljen tai puheäänen tunnistaminen ovat menetelmiä sen selvittämiseksi, kuka henkilö on. Tällaiset biometriset turvallisuusjärjestelmät ovat kuitenkin vielä liian kalliita käytettäviksi tavallisissa tietokonejärjestelmissä.

Salasanapohjaista järjestelmää voidaan kuitenkin melko helposti täydentää menetelmillä, jotka perustuvat siihen, mitä henkilö omistaa (toisin sanoen: mitä henkilöllä on mukanaan). Tunnetuin esimerkki lienee luottokortti. Tietokoneen käyttöön liittyvistä sovelluksista mainittakoon LazerLock-menetelmä, johon kuuluu ohjelmiston lisäksi jokaiselle käyttäjälle annettava television kaukosäädintä muistuttava laite. Kun käyttäjä on kirjoittanut käyttäjätunnuksensa ja salasanansa normaaliin tapaan, ilmestyy näyttöruudulle kaksi nopeasti välkkyvää kenttää, joiden sisältöä silmä ei pysty tulkitsemaan. LazerLock-laite suunnataan näitä kenttiä kohti, ja sen nelinumeroisesta näytöstä luetaan numerosarja, joka kirjoitetaan päätteelle.

Monet salasanapohjaiset käyttöjärjestelmät (kuten VAX/VMS versio 4) tarjoavat yksinäänkin hyvät mahdollisuudet tietokonejärjestelmän turvaamiseksi väärinkäytöksiltä. Tehokkuus riippuu käytännössä kuitenkin suuresti siitä, ovatko yksityiset käyttäjät riittävän motivoituneita huolehtimaan suojauksistaan ja salasanoistaan ja onko heillä tarpeeksi tietoja asiasta. Jos käyttäjät ovat yhteistyöhaluisia, ei yleensä ole tarpeen pitää käynnissä raskaita valvontaohjelmia, jotka hidastavat tietokoneen toimintaa.

Käyttöoikeuksien tarkistamisella pystytään parhaassa tapauksessa estämään ulkopuolisten tunkeutuminen järjestelmään sekä huolehtimaan siitä, että tavalliset käyttäjät

toimivat sallituissa puitteissa eivätkä haittaa toistensa työskentelyä. On kuitenkin henkilöitä, joihin käyttöoikeuksien tarkistaminen ei tehoa.

Tietokonejärjestelmän toiminnasta vastuussa olevalla henkilöllä on työnsä puolesta oltava täydet käyttöoikeudet järjestelmään. Yleensä tällainen henkilö pyritään löytämään oman talon sisältä, jolloin hänen luotettavuudestaan on jo jotain näyttöä. Ulkopuolelta näihin tehtäviin palkatulle henkilölle ei tulisi heti antaa tällaisia oikeuksia, vaan vasta esimerkiksi koulutus- ja perehdyttämisjakson jälkeen.

Alla kuvattu tietojen koodaaminen salakielelle tarjoaa keinon, jolla voidaan varmistaa, ettei edes järjestelmävastuuhenkilö pysty lukemaan arkaluonteista dataa. Tämä on vastuuhenkilön kannalta hyvä asia, sillä tällöin hänen ei tarvitse joutua aiheettoman epäilyksen uhriksi.

2.3 TIETOJEN KOODAAMINEN SALAKIELELLE

Salausalgoritmien tutkiminen ja testaaminen on viime vuosina muodostunut nopeasti kasvavaksi sovelletun matematiikan osa-alueeksi. Pääsyynä atk-kryptologian kehittämiseen on lisääntynyt tiedonsiirto, sillä laajaa tietoliikenneverkkoa on mahdotonta suojata fyysisesti. Passiivisen linjasieppauksen (salakuuntelun) lisäksi pyritään estämään myös aktiivinen sieppaus (sanoman muuttaminen) kehittämällä menetelmiä sanoman oikeaperäisyyden varmistamiseksi.

Luottamuksellisten tietojen koodaaminen salakielisiksi voi olla paikallaan myös niissä tapauksissa, joissa tiedonsiirtoa yhden rakennuksen ulkopuolelle ei esiinny. Koska salakielen selvittäminen ei riipu tietokonejärjestelmän käyttöoikeuksista, voi tiedoista vastuussa oleva henkilö tällöin paremmin luottaa tietojen salassapysymiseen.

Jotta kunnollinen salausavainten hallinta ja suurten tietomäärien koodaaminen salakielisiksi olisivat käytännössä mahdollisia, tarvitaan kansainvälisiä standardeja salausalgoritmeistä ja näiden mukaisesti koodaavia tehokkaita mikropiirejä. Vaikka jotain onkin jo tehty, on standardointi ja piirikehittely vielä kesken. Suomessa lienee nykyään mahdollista saada salauspiirejä joihinkin mikrotietokoneisiin, mutta VAX-tietokoneille niitä ei ainakaan Euroopassa ole tällä hetkellä yleisesti saatavilla.

2.4 VARAUTUMINEN VAHINKOIHIN

Tärkein ja tunnetuin keino vahinkojen varalle on säännöllinen varmuuskopiointi. Monen käyttäjän tietokonejärjestelmissä tämä asia on yleensä järjestyksessä. Sen sijaan henkilökohtaisten tietokoneiden levykkeiden varmuuskopiointi riippuu käyttäjästä ja on normaalisti epäsäännöllistä, vaikka levykkeiden tuhoutuminen tai lukukelvottomiksi tuleminen on melko tavallista. Luvussa 7 käsitellään lähemmin varmuuskopiointia mikrotietokoneiden yhteydessä.

Oli tietokone suuri tai pieni, varmuuskopioiden kunnollisesta säilytyksestä on huolehdittava. Tärkeimmät kopiot tulisi säilyttää data- tai diskettikaapeissa. Muiden säilytykseen riittää lukittu teräskaappi, jonka sisällä levykkeet ovat omissa säilytyslaatikoissaan. Varmuuskopioita ei pitäisi säilyttää samassa huoneessa kuin alkuperäisiä tietoja sisältäviä muistivälineitä.

Etukäteen on syytä miettiä, miten pitäisi menetellä vahingon (esimerkiksi tulipalon, vesivahingon tai vakavamman laitevian) sattuessa. Millä tavalla laite pitää peittää tai siirtää kuiviin tiloihin? Mistä varmuuskopiot löydetään? Kuinka kauan voidaan olla ilman tietokonetta? Tarvitaanko joissakin tilanteissa varalaitetta ja miten sen saa?

Vastaavasti on myös järkevää varautua tilanteeseen, että joku henkilö ei enää yllättäen ole käytettävissä. Riittävällä ja oikein suunnatulla koulutuksella ja dokumentoinnilla voidaan turvata se, etteivät tärkeät toiminnat ole yhden henkilön varassa.

2.5 YHTEENSOPIVUUDEN VARMISTAMINEN

Laitekirjavuutta kannattaa välttää. Yhteensopivuus on varmistettava erityisen huolellisesti silloin, jos uusi laite on eri merkkiä kuin vanhat. Huomiota on kiinnitettävä varsinkin tiedostojen ja ohjelmien siirtoon laitteesta toiseen sekä siihen, että samaa ohjelmaa voidaan ajaa eri koneilla.

Ulkopuolisen toimittajan myymiin ohjelmiin ei kannata tehdä itse muutoksia (mikäli se edes on mahdollista), jos aikoo ostaa toimittajan uudet ohjelmaversiot. Seurauksena olisi parhaassakin tapauksessa jatkuvaa korjailua aina uuden version ilmestyessä. Mahdollinen yhteensopivuuden puute voi myös pakottaa vanhojen datatiedostojen konvertointiin.

2.6 TIEDOTUS, KOULUTUS JA DOKUMENTOINTI

Yhä useammat henkilöt, joilla ei ole minkäänlaista atk-alan pohjakoulutusta, joutuvat nykyään työskentelemään mikrotietokoneilla tai tietokonepäätteillä. Monet tuntevat ainakin aluksi tietokoneen käytön epämukavaksi ja stressaavaksi, sillä riittämätön koulutus ja epätäydelliset ohjeet aiheuttavat epävarmuutta oikeiden toimintojen ja komentojen valitsemisessa. Yleistä on pelko, että vahingossa tulee tuhonneeksi tiedostoja tai tyhjentäneeksi levykkeitä, ja tällaisia vahinkoja todella melko usein sattuu.

Koulutuksesta ja käyttöohjeista saadut tiedot auttavat käyttämään oikeita komentoja ja pienentävät virhetoimintojen määrää. Oikein suunnitellut ohjelmat johtavat samaan tulokseen. Ne opastavat tarvittaessa käyttäjää eivätkä suostu tekemään mitään peruuttamatonta yhden komennon perusteella kysymättä ensin varmistusta.

Tiedotuksella on oma tärkeä osuutensa huolehdittaessa siitä, että käyttäjät tietävät, mitä voi tehdä ja mitä ei, eivätkä turhaan ihmettele, jos jokin ennen onnistunut toimenpide ei enää onnistukaan. Tiedot oleellisista muutoksista laitteissa, käyttöjärjestelmissä, ohjelmissa tai datatiedostoissa olisi ilmoitettava kaikille niille, joiden työhön kyseisillä muutoksilla saattaa olla vaikutusta. Ilmoitukset muutoksista tulisi tehdä etukäteen.

Uusista yleiskäyttöisistä ohjelmista pitäisi tiedottaa viimeistään käyttöönoton yhteydessä. Jos ohjelma tulee muuttamaan aikaisempia käsittelyrutiineja, on siitä ja sen mukanaan tuomista muutoksista kerrottava mahdollisimman aikaisessa vaiheessa ja varattava riittävästi aikaa koulutukseen ja siirtymävaiheeseen.

Dokumentointia tarvitaan ainakin kahdella tasolla. Ensimmäinen taso on kokonainen informaatiojärjestelmä, jonka sisältämät toiminnat ja toimintojen väliset yhteydet on kuvattava ja dokumentoitava. Informaatiojärjestelmän eri osien toiminnat kuvataan tarkemmin käyttöohjeissa. Nämä osat voivat olla valmiina ostettuja, teetettyjä tai itse tehtyjä ohjelmia. Tällä tasolla ei ohjelmien sisäiseen rakenteeseen puututa, pääpaino on ohjelmien suorittamissa tehtävissä suuremman kokonaisuuden osana.

Toisen dokumentointia kaipaavan tason muodostavat itse tehdyt ohjelmat. Jos on mahdollista, että ohjelmalla on nyt tai tulevaisuudessa muitakin käyttäjiä kuin ohjelman suunnittelija itse ja mahdollisesti joku hänen kollegansa, tu-

lisi ohjelmasta tehdä dokumentti, josta käyvät ilmi ainakin ohjelman tarkoitus, suunnittelija, valmistumispäivä, käyttöohjeet, käsiteltävät tiedostot, tehdyt oletukset ja tulosten tulkinta. Mikrotietokoneelle tehdyn ohjelman dokumentista tulisi selvitä, millä levykkeillä ohjelmatiedosto ja tarvittavat datatiedostot sijaitsevat.

Koska usein käy niin, että joku toinen joutuu joskus tekemään muutoksia ohjelmaan, tulisi myös ohjelman päärakenne dokumentoida (tietorakenteet, aliohjelmat, kutsukaaviot) ja itse ohjelmateksti varustaa riittävin kommentein. Lähdekielinen listaus on hyvä liittää dokumentin liitteeksi.

3 VASTUU ATK-TURVALLISUUDESTA

Ryhdyttäessä pohtimaan tarvittavia suojaustoimenpiteitä monen käyttäjän tietokonejärjestelmässä sekä määrittämään eri käyttäjien tai käyttäjäryhmien vastuuta suojauksista, on ensin paikallaan arvioida turvallisuusvaatimusten taso.

Erilaiset tietokoneenkäyttöympäristöt voidaan turvallisuusvaatimusten mukaisesti jakaa karkeasti matalan, keskimääräisen ja korkean turvallisuustason ympäristöiksi. Näitä voidaan luonnehtia seuraavasti:

Matalan turvallisuustason ympäristössä ei pidetä tiedostosuojausta tarpeellisena, vaan luotetaan siihen, ettei kukaan tahallaan tai vahingossa haittaa toisten työskentelyä. Käyttäjätunnuksen saaneilla on yleensä mahdollisuus lukea ja muuttaa toisten käyttäjien tiedostoja ja sähköistä postia. Useimmat tällaiset ympäristöt eivät toivo ulkopuolisia tunkeutujia, mutta niiden suojautumismahdollisuudet ovat puutteelliset, jos järjestelmään voidaan olla yhteydessä puhelinlinjoja pitkin.

Keskimääräisen turvallisuustason ympäristössä ei käyttäjä pääse käsittelemään toisten tiedostoja ilman erikseen myönnettyjä oikeuksia. Poikkeuksena tästä saattavat olla vapaammat käsittelyoikeudet tiettyjen käyttäjäryhmien sisällä. Käyttäjät pystyvät usein selaamaan toisten hakemistoluetteloita ja seuraamaan, minkä nimisiä ohjelmia järjestelmässä ajetaan.

Korkean turvallisuustason ympäristössä järjestelmä ei yhteyttä otettaessa esitä tervehdystä eikä kerro mitään itsestään. Käyttäjä pystyy käsittelemään omia tiedostojaan ja vain harvoja muita tiedostoja. Käyttäjä ei voi selata muiden hakemistoluetteloita eikä saa tietoja järjestelmässä kullakin hetkellä ajettavista ohjelmista tai

avoimista tiedostoista. Järjestelmä pitää kirjaa tärkeimpien tiedostojen käytöstä.

Matalan turvallisuustason käyttöympäristöjä ovat yleensä pienet (alle 30 käyttäjän) tutkimus- tai suunnittelukäytössä olevat tietokonejärjestelmät, joissa ei käsitellä hallinnollisia tietoja eikä luottamuksellisia tai vaikeasti korvattavia aineistoja. Useassa tapauksessa näihin järjestelmiin ei ole puhelinlinjayhteyksiä.

Edellisen perusteella Metsäntutkimuslaitos on luokiteltava ainakin keskimääräistä turvallisuustasoa vaativaksi ympäristöksi. Onhan laitoksessa noin 400 VAX-tietokoneiden käyttäjää, ja etäisyhteys voidaan ottaa sekä tavallista puhelinlinjaa, yleistä pakettiverkkoa että Decnet-tietoliikenneverkkoa käyttäen. Lisäksi laitoksessa käsitellään hallinnnollia tietoja, muita luottamuksellisia tietoja sekä monia tärkeitä tutkimusaineistoja. Lukuisat mikrotietokoneet asettavat myös omat turvallisuusvaatimuksensa.

Tarkastellaan nyt Metsäntutkimuslaitosta (METLA) keskimääräisen turvallisuustason vaativana käyttöympäristönä ja pyritään selvittämään atk-turvallisuuden kannalta tarvittavat vastuuhenkilöt sekä määrittämään käyttäjien velvollisuudet.

Käyttöpäällikkö

Matemaattinen osasto ylläpitää laitoksen VAX-tietokoneita ja valvoo niiden käyttöä. Jokaiselle VAX-tietokoneelle on määrätty järjestelmävastuuhenkilö eli käyttöpäällikkö (system manager) huolehtimaan laitteiston toiminnasta. Hänen ohellaan tai apunaan voi työskennellä henkilöitä, joilla on rajatut tehtävä-alueet tietokonejärjestelmän tai atk-turvallisuuden hoidossa ja jotka toimivat tarvittaessa hänen sijaisinaan.

Tämän henkilöryhmän tehtävien pääperiaate atk-turvallisuuden osalta on luoda riittävän turvallinen ja toimiva käyttöympäristö tinkimättä liikaa järjestelmän mahdollistamasta käyttäjäystävällisyydestä. Tehtäviin kuuluu muun muassa käyttäjätunnusten ja käyttöoikeuksien myöntäminen, kunnollisten systeemisalasanojen ylläpito, tietokoneen käytön ja käyttäjien valvonta (ettei luvattomia käyttäjiä esiinny), tiedostojen yleisen oletussuojauksen asettaminen, yleisen tietohakemiston ylimmistä tasoista huolehtiminen sekä tietoliikenneverkkojen suojaaminen (ja niitä vastaan suojautuminen) mahdollisuuksien mukaan.

Lisäksi kyseiset henkilöt jakavat käyttäjille tietoa tiedostojen suojaamisesta ja salasanoista huolehtimisesta ja antavat muutakin atk-turvallisuuteen liittyvää neuvontaa.

Atk-yhdyshenkilöt

Käyttäjätunnukset on ryhmitelty METLAn toimintayksiköiden (osastojen, tutkimussuuntien, toimistojen ja asemien) mukaan. Helsingin yliopiston käyttäjät muodostavat oman yksikkönsä. Henkilökohtaiset tunnukset liittyvät aina johonkin yksikköön. Kullakin toimintayksiköllä tulee olla atk-yhdyshenkilö, joka opastaa ja valvoo tietokoneen käyttöä yksikössä sekä toimii yksikön käyttäjien ja käyttöpäällikön välisenä yhdyssiteenä. Yksiköllä voi olla atk-yhdyshenkilö kutakin sen käyttämää VAX-tietokonetta kohti.

Atk-yhdyshenkilö opastaa käyttölupa-anomuksen teossa yksikköön tullutta uutta työntekijää, joka tulee työssään tarvitsemaan VAX-tietokonetta (anomusmenettelystä on erilliset ohjeet). Yhdyshenkilö huolehtii myös siitä, että uusi käyttäjä hankkii tietokoneen käytöstä perustiedot kirjallisuuden tai sopivan henkilön avulla. Perustietoihin kuuluu kunnollinen salasanasta huolehtiminen.

Jos atk-yhdyshenkilö huomaa leväperäisyyttä salasanojen käytössä (esim. etunimiä salasanoina, salasanan kirjoittamista paperille tai henkilökohtaisen salasanan kertomista toiselle henkilölle), on hänen neuvottava kyseisiä käyttäjiä ja kehotettava heitä muuttamaan salasanansa.

Atk-yhdyshenkilö voi saada (osaston tai tutkimussuunnan päällikön suostumuksella) ryhmätason erikoisoikeuksia. Hän voi tällöin esimerkiksi määritellä ryhmätason loogisia nimiä. Jos atk-yhdyshenkilön käyttäjätunnuksella on tällaisia oikeuksia, hänen on erityisesti pidettävä huolta, ettei kukaan muu pääse hänen tunnustaan käyttämään. Hänen tulee myös itse käyttää harkiten oikeuksiaan.

Laitevastuuhenkilöt

Laitoksen jokaisella osastolla tai tutkimussuunnalla tulisi olla laitevastuuhenkilö, joka pystyy tekemään yksinkertaisia vianmäärityksiä ja muuttamaan pääte- ja kirjoitinasetuksia. Tämä henkilö voi hyvin olla yksikön atk-yhdyshenkilö, mutta tämä ei ole välttämätöntä.

Jos yksikön työntekijä havaitsee atk-laitteessa vikaa tai tarvitsee erilaisia laiteasetuksia, hän kääntyy yksikön laitevastuuhenkilön puoleen. Laitevastuuhenkilö tutkii tilanteen ja korjaa asetukset. Jos kyseessä on varsinainen vika tai laitevastuuhenkilö ei muuten pysty asiaa hoitamaan, hän ottaa yhteyttä käyttöpäällikköön (tai erikseen sovittuun henkilöön).

Laitevastuuhenkilön tulee mahdollisuuksien mukaan pitää silmällä myös yksikön atk-laitteiden fyysistä turvallisuutta. Jos hän havaitsee selviä puutteita suojautumisessa varkautta tai vahinkoa (esim. tulipalo, vesivahinko) vastaan, hänen tulee pyrkiä vaikuttamaan niin, että

asian hyväksi tehdään jotain, jollei hän itse pysty tilannetta korjaamaan.

Ohjelmavastuuhenkilöt

Jokaisella yleiskäyttöisellä tietokoneohjelmalla tulee olla vastuuhenkilö, joka tuntee ohjelman toiminnan hyvin ja pysyttelee ajan tasalla ohjelman muutoksien suhteen. Laitoksessa tehtyyn ohjelmaan voi muutoksia tehdä vain vastuuhenkilö tai joku toinen hänen valvonnassaan. Vastuuhenkilö huolehtii siitä, että muutos dokumentoidaan. Mikrotietokoneohjelmien ollessa kyseessä henkilön tulee

- estää ohjelmistovarkaudet ja asiaton kopiointi sekä
- säilyttää viimeisimmät ohjelmaversiot turvallisesti ja huolehtia varmuuskopioinnista

Tietojärjestelmävastuuhenkilöt

Kutakin tietojärjestelmää kohti on nimettävä henkilö, jolla on kokonaisvastuu järjestelmän tietojen asianmukaisesta käsittelystä ja säilytyksestä. Henkilön tulee laatia tietojen käsittelyohjeet (mikäli sellaisia ei vielä ole) ja valvoa ohjeiden noudattamista. Ohjeiden pitäisi käsitellä ainakin seuraavia seikkoja:

- ketkä ovat oikeutettuja käyttämään järjestelmää
- miten tiedot tallennetaan; miten alkuperäiset (esim. paperilla olevat) tiedot säilytetään
- miten tallennettua aineistoa käsitellään
- miten varmuuskopiot säilytetään (jos järjestelmä on mikrotietokoneella)

Tavalliset käyttäjät

Tietokonejärjestelmän turvallisuus ja luvattoman käytön estäminen ovat viime kädessä kiinni tavallisesta käyttäjästä. Järjestelmän turvallisuus on yhtä vahva (tai heikko) kuin sen heikoin osa, ja heikoin osa on yleensä joko magneettinauhojen ja levykkeiden säilytys tai käyttäjä, joka ei välitä huolehtia salasanastaan.

Uuden käyttäjän tulee heti käyttäjätunnuksen saatuaan muuttaa salasanansa niin, ettei kukaan muu sitä tiedä. Käyttäjän pitää yleensäkin muuttaa salasanansa ainakin joka kolmas kuukausi, ja hänen velvollisuutensa on huolehtia siitä, että salasana on riittävän pitkä ja vaikea arvattavaksi tai kokeilemalla selvitettäväksi. Salasanan salassapysymisestä on huolehdittava hyvin (katso seuraavia lukuja). Jos käyttäjän hallintaan annetaan tiedostoja, joilla on merkitystä muillekin kuin hänelle itselleen, on hänen suojattava ne sopivalla tavalla.

Yksikön sisällä käyttäjillä on yleensä vähintään lukuoikeus toistensa tiedostoihin suojauksien ryhmäkenttien mukaisesti. Käyttäjä on vastuussa siitä, etteivät luvattomat henkilöt pääse hänen käyttäjätunnuksensa avulla käsiksi osaston tai tutkimussuunnan tiedostoihin. Käyttäjän on siksi huolehdittava salasanansa lisäksi myös siitä, ettei jätä yhteyttä päälle poistuessaan päätteen luota.

Jos käyttäjä huomaa, että hänen tiedostojaan puuttuu, uusia ja outoja tiedostoja on ilmestynyt, levykiintiötä on kulunut selittämättömästi, hänen käyttäjätunnuksensa on käytössä toisella päätteellä tai yhteydenoton alun Login Failures -ilmoitus ei täsmää käyttäjän omien yhteydenottovirheiden määrän kanssa, niin käyttäjän on hyvä ottaa yhteys käyttöpäällikköön asian selvittämiseksi.

Ryhmätunnusvastuuhenkilöt

Yleensä käyttäjätunnukset ovat henkilökohtaisia. Erikoistapauksissa voidaan muodostaa käyttäjätunnuksia, jotka on tarkoitettu usean henkilön käyttöön. Kullakin tällaisella ryhmätunnuksella tulee olla vastuuhenkilö, joka on käyttöpäällikön tiedossa.

Vain vastuuhenkilö saa kertoa tunnuksen salasanan sitä tarvitseville henkilöille. Vastuuhenkilön on pidettävä huolta siitä, että salasana vaihtuu ainakin silloin, kun joku sen tunteva eroaa laitoksen palveluksesta tai ei muuten enää tunnusta tarvitse.

Jos VAX-tietokonetta väärinkäytetään (esimerkiksi käytetään helposti arvattavaa salasanaa, salasana paljastetaan ulkopuoliselle, METLAn työntekijä käyttää tietokonetta muuhun kuin työhönsä liittyviin tehtäviin tai ulkopuolinen käyttäjä käyttää tietokonetta muuhun kuin käyttöluvassa mainittuihin tehtäviin), matemaattisella osastolla on oikeus peruuttaa henkilön käyttölupa määräajaksi tai pysyvästi.

Luvun lopuksi vielä varoittava esimerkki. Erityisesti nyt, kun Metsäntutkimuslaitos on liittynyt DATAPAK-pakettiverkkoon, on syytä huolehtia hyvin salasanoista. Jos esimerkiksi käyttäjä Matias Meikäläinen valitsee salasanakseen MATIAS, ei hänellä käytännöllisesti katsoen ole salasanaa ollenkaan. Jos sitten joku luvaton tunkeutuja onnistuu hänen tunnustaan käyttäen kuluttamaan aikaansa vaikkapa ulkomaisissa tietopankeissa, voidaan herra Meikäläistä pitää vastuussa (tai ainakin osavastuussa) laitokselle aiheutuneesta huomattavasta laskusta.

4 SALASANOJEN YLLÄPITO VAX/VMS-JÄRJESTELMÄSSÄ

4.1 SALASANAN VALITSEMINEN

Käyttöpäällikkö voi määrätä vähimmäispituuden salasanalle. Oletusasetusten mukainen minimipituus on kuusi merkkiä. Maksimipituus on 31 merkkiä, ja mahdolliset merkit ovat englantilaiset aakkoset A,...,Z (isoilla ja pienillä ei eroa), numerot 0,...,9 sekä alaviiva (_) ja dollari ($).

Käyttäjä, jolla on erityisoikeuksia tai tärkeitä tiedostoja, voi vaihtoehtona yhdelle pitkälle salasanalle käyttää kahta kohtuumittaista salasanaa. Yhteyttä otettaessa järjestelmä kysyy tällöin erikseen kummankin salasanan. Toisen salasanan voi ottaa käyttöön vain käyttöpäällikön avulla. Alkuasetuksen jälkeen käyttäjä voi muuttaa sitä itse. Jos järjestetään niin, että yksi henkilö tuntee ensimmäisen ja toinen henkilö toisen salasanan, saadaan valvottu käyttäjätunnus, joka vaatii kahden henkilön läsnäolon yhteydenotossa. Tavallisesti käyttäjälle riittää yksi salasana, kunhan se on kunnolla valittu.

Oleellista salasanassa on, että se ei saa olla arvattavissa eikä eri mahdollisuuksia kokeilevan ohjelman selvitettävissä. Salasanaksi ei tule valita etu- tai sukunimeä (ei edes takaperin kirjoitettuna), projektinimeä, puolison tai lapsen nimeä tai syntymäaikaa eikä mitään muutakaan termiä, joka liittyy käyttäjään tai hänen työhönsä tai harrastuksiinsa. Salasana ei myöskään saa olla minkään sanakirjan hakusanoja. Tekstinkäsittelyjärjestelmiin sisältyy toisinaan tällainen sanavarasto, jonka tunkeutuja voi kokeilemalla läpikäydä.

Hyvä salasana on noin 8-18 merkkiä pitkä ja sisältää usein myös numeroita. Muistamista silmälläpitäen voi salasanan valita esimerkiksi seuraavilla tavoilla:

a) Valitaan jokin tavallinen sana ja sijoitetaan kirjainten väliin numeroita. Esimerkiksi sana HAMPURI on sellaisenaan salasanaksi sopimaton, mutta HA2MPU8RI on kelvollinen salasana.

b) Kirjoitetaan useampi tavallinen sana yhteen (väliin voi sijoittaa myös numeroita) siten, että yhdistelmää ei löydy sanakirjoista eikä sitä ole muutenkaan helppo arvata. Tällaisen salasanan on syytä olla ainakin 10 merkkiä pitkä. Esimerkiksi KUUSSAKASVAAKOIRIA on melko hyvä salasana, kun taas MINUNSALASANA on esimerkki huonosta salasanasta.

c) Valitaan jokin kirjaimista ja numeroista muodostuva merkkijono sen perusteella, että sen näppäily muodostaa jonkinlaisen kuvion ("sormen koreografiaa"). Esimerkkinä olkoon vaikka TY6H5GFYT.

Käyttäjä voi antaa koneen ehdottaa salasanoja. Tämä tapahtuu komennolla SET PASSWORD/GENERATE. Kone ehdottaa viisi salasanaa ja näiden tavutuksen (muistamisen helpottamiseksi). Jokainen sana koostuu kirjaimista ja on 6-8 merkkiä pitkä. Jollei mikään ehdotuksista kelpaa, niin painamalla <RETURN> saa uudet ehdotukset. Painamalla <CTRL/Z> voi palata komentotasolle säilyttäen vanhan salasanan.

Jos käyttäjä haluaa tietokoneen ehdottavan esimerkiksi 8-10 merkin mittaisia salasanoja, voi edellä mainitussa komennossa käyttää tarkennetta /GENERATE=8.

Kun uudeksi salasanaksi valitaan jokin järjestelmän ehdottamista sanoista, ei ehdotusluetteloa tule jättää ruudulle näkyviin muiden luettavaksi. Paperille kirjoittavilla päätteillä tätä menetelmää ei ole syytä ollenkaan käyttää.

4.2 SALASANASTA HUOLEHTIMINEN

4.2.1 Salasanan salassapito

Koska VAX/VMS-järjestelmän suojaukset perustuvat salasanoihin, on näiden sanojen salassapito ensiarvoisen tärkeää. Salasanaa ei tule paljastaa kenellekään toiselle, eikä sitä myöskään pidä kirjoittaa paperille tai tiedostoon.

Jos käyttäjä ei käytä tunnustaan moneen kuukauteen (esimerkiksi matkan tai kenttätöiden vuoksi), on tietysti mahdollista, että hän tänä aikana unohtaa hyvin valitun salasanansa. Muistamista ei silti kannata helpottaa siten, että muuttaa salasanan yksinkertaiseksi (poissaolon aikana käyttäjätunnus on muutenkin tavallista suojattomampi).

Tällaisessa tapauksessa on perusteltua kirjoittaa salasana paperille. Paperilla tulee silloin olla vain pelkkä salasana (mieluummin hivenen muutettuna tai epätäydellisenä) eikä mitään tunnistetietoja, jotka paljastavat, mihin tietokoneeseen ja kehen käyttäjään sana liittyy. Paperi on parasta säilyttää lompakossa tai kotona varmassa paikassa. Kun käyttäjä ryhtyy taas käyttämään tunnustaan, tulee salasana muuttaa heti eikä uutta tule kirjata mihinkään.

Toinen mahdollinen menettely on pyytää käyttöpäällikköä laittamaan käyttäjätunnus "lukkoon" poissaolon ajaksi.

Yleensä kullakin käyttäjällä on oma käyttäjätunnuksensa, jonka salasanan vain hän tietää. Erikoistapauksessa yhdellä käyttäjällä voi olla kaksikin käyttäjätunnusta, mutta kutakin henkilökohtaista tunnusta kohti tulee olla vain yksi käyttäjä. Jos usea käyttäjä haluaa tehdä töitä samoilla tiedostoilla, voidaan tätä varten luoda projektunnuksia.

Poikkeuksen edellä sanotusta muodostavat sidotut käyttäjä-

tunnukset (captive accounts), joita voidaan luoda määrättyjen, rajoitettujen asioiden suorittamista varten ja jotka saattavat olla monen henkilön käytössä. Näiden tunnusten käyttäjä joko pysyy koko ajan tietyn ohjelman sisällä pääsemättä koskaan komentotasolle tai hän pystyy suorittamaan vain määrättyjä komentoja.

Jos käyttäjä kuitenkin jossakin äärimmäisessä erikoistapauksessa määrättyä tehtävää varten paljastaa salasanansa toiselle henkilölle (jolla on omakin käyttäjätunnus ja siis käyttöoikeus koneeseen), hänen ei pidä tehdä tätä niin, että joku kolmaskin saattaa kuulla sen. Salasanan kertomista puhelimitse tulee välttää. Käyttäjällä on vastuu siitä, mitä hänen tunnuksellaan tehdään. Hänen tulee oman etunsa vuoksi muuttaa salasanansa heti, kun tuo toinen ei sitä enää (ainakaan vähään aikaan) välttämättä tarvitse.

On mahdollista, että henkilö, joka tuntee salasanasi, voi mennä muuttamaan sen niin, ettet enää itse pääse omalle tunnuksellesi. Onneksi salasanan paljastaminen ei käytännöllisesti katsoen koskaan ole tarpeellista. Hakemistojen ja tiedostojen suojausten muuttaminen yleensä riittää.

Salasana tulee muuttaa heti, kun joku sen tunteva eroaa METLAn palveluksesta. Kenellekään laitoksen ulkopuoliselle salasanaa ei tule paljastaa, eikä myöskään niille laitoksen palveluksessa oleville, joilla ei ole omaa käyttölupaa.

4.2.2 Salasanan ajoittainen muuttaminen

Salasanan muuttaminen tapahtuu komennolla SET PASSWORD. Käyttöjärjestelmä tiedustelee ensin vanhan salasanan ja sen jälkeen uuden salasanan kahdesti. Jos näillä kahdella kerralla annetaan sama merkkijono, järjestelmä hyväksyy sen uudeksi salasanaksi. Jos merkkijonot ovat erilaiset tai käyttäjä painaa <CTRL/Z>, vanha salasana jää voimaan.

Nykyisillä asetuksilla käyttöjärjestelmä vaatii salasanan muuttamista vähintään kolmen kuukauden välein. On tärkeätä, että salasana todella muutetaan erilaiseksi, eikä välimuodon kautta takaisin entiselleen.

Viiden viimeisen päivän aikana ennen salasanan vanhenemista järjestelmä varoittaa ilmoituksella

WARNING---Your password expires on <päiväys>

Jos tänä aikana salasanaa ei muuteta (esim. loman tai matkan takia), on siihen vielä mahdollisuus seuraavan pääteyhteyden aikana. Tällöin järjestelmä ilmoittaa

WARNING---Your password has expired; update immediately
with SET PASSWORD !

Jos tämänkään yhteyden aikana salasanaa ei muuteta, järjestelmä lukitsee tunnuksen, ja käyttäjän on otettava yhteys käyttöpäällikköön.

Jos käyttäjällä on kaksi salasanaa, vanhenevat ne omia aikojaan. Ensimmäinen salasana muutetaan komennolla SET PASSWORD ja toinen komennolla SET PASSWORD/SECONDARY.

Jos käyttäjä haluaa poistaa toisen salasanan käytöstä, hän kirjoittaa viimeksi mainitun komennon ja antaa uuden salasanan kyselyyn vastaukseksi pelkän <RETURN>-napin painalluksen.

Salasanan muuttamiseen voi tietysti käyttää myös aikaisemmin mainittua automaattista salasanatuottamista. Tällöin esimerkiksi kaksoissalasanan jälkimmäisen osan muuttamiseen käytetään komentoa SET PASSWORD/SECONDARY/GENERATE.

Tiheämpi kuin kolmen kuukauden välein tapahtuva salasanan muuttaminen on tarpeen, jos tunnuksella on pääsy luottamuksellisiin aineistoihin. Lisäksi salasana tulee muuttaa he-

ti, jos on pienintäkin aihetta epäillä sen paljastuneen.

4.2.3 Salasanoja varastavat ohjelmat

Kun käyttäjä aloittaa työskentelyn päätteellä, jolla joku toinen on mahdollisesti ollut häntä ennen, ei hän yleensä voi tietää, onko aikaisempi yhteys todella katkaistu, vai onko päätteellä toiminnassa salasananoja varastava ohjelma tai komentoproseduuri. Tällainen ohjelma voi jäljitellä yhteyden päättymistä ja uuden aloittamista ryhtyen kyselemään käyttäjätunnusta ja salasanaa, eikä käyttäjä ehkä huomaa mitään tavallisuudesta poikkeavaa. Ohjelma kirjoittaa saamansa tiedot johonkin tiedostoon ja sitten esimerkiksi ilmoittaa "User authorization failure" katkaisten yhteyden.

Mahdollisia turvatoimenpiteitä tällaisia tapauksia vastaan on kolme:

a) Yhteydenoton alussa tulevien ilmoitusten "last interactive login" ja "number of login failures" tarkkailu.

   Salasanoja varastavan ohjelman antama ilmoitus "User authorization failure" ei kerro todellisesta yhteydenoton epäonnistumisesta. Jos käyttäjä saa tällaisen ilmoituksen, mutta järjestelmä ei ilmoita mistään "login failure" -tapauksesta uuden yhteydenoton alussa, käyttäjä on mahdollisesti joutunut salasanavarkauden uhriksi. Samaa voi epäillä myös, jos on varma, että antoi käyttäjätunnuksensa ja salasanansa oikein, mutta silti saa "User authorization failure" -ilmoituksen.

   Tällaisissa tapauksissa tulee salasana muuttaa välittömästi ja ilmoitaa tapahtuneesta käyttöpäällikölle.

b) Käyttäjä voi myös ottaa taktiikaksi antaa aina ensin väärän salasanan. Kun kone seuraavan kerran kysyy käyt-

täjätunnusta, on kysyjänä tällöin melko varmasti käyttöjärjestelmä itse. Silti ei pidä unohtaa tarkkailla a)-kohdassa mainittuja seikkoja.

c) Jos käyttäjän pääte on kiinteässä linjayhteydessä, hän voi keskustella käyttöpäällikön kanssa Secure Terminal Server -attribuutin liittämisestä päätteeseensä. Tällöin halutessaan ottaa yhteyden hän painaa <RETURN>-näppäimen sijasta jotakin muuta tiettyä näppäintä, jolloin päätteellä mahdollisesti käynnissä olevat prosessit katkeavat ennen käyttäjätunnuksen tiedustelua.

Yhtä tärkeää, kuin pitää salasana omana tietonaan, on muistaa sulkea pääteyhteys poistuessaan päätteen luota (jollei ole mahdollista lukita huoneen ovea). Salasanoja varastavan ohjelman tai muun vahingollisen ohjelman sisäänlatauksen voi suorittaa alle 10 sekunnissa. Käyttäjätunnuksen luvaton "lainaaja" voi myös lyhyessä ajassa tuhota tai kopioida tiedostoja sekä käyttää ryhmäoikeuksia hyväkseen.

Potentiaalisia vaaratekijöitä ovat myös toisten tekemät ohjelmat. Nämä voivat olla ns. Troijan hevosia, joiden sisälle on kätketty osa, joka tekee aivan muuta kuin mitä lahjoittaja tai myyjä on kertonut. Kannattaa pitäytyä tunnettujen ohjelmistotalojen tuotteissa, jollei muuten voi olla varma toimittajan luotettavuudesta.

5 TIEDOSTOJEN SUOJAAMINEN VAX/VMS-JÄRJESTELMÄSSÄ

5.1 STANDARDISUOJAUKSET

Jokaisella tiedostolla ja hakemistolla on oma suojauskoodinsa. Käyttäjät on siinä jaettu neljään luokkaan käyttäjänumeron (UIC, User Identification Code) perusteella:

SYSTEM (systeemi)	Järjestelmän ylläpitoon käytettävät käyttäjätunnukset (systeemitunnukset). Myös ne samaan yksikköön kuuluvat käyttäjät, joilla on täydet ryhmäoikeudet.
OWNER (omistaja)	Tiedoston omistaja (yleensä luoja).
GROUP (ryhmä)	Käyttäjät, jotka kuuluvat samaan toimintayksikköön.
WORLD (maailma)	Kaikki käyttäjät, myös edellämainitut.

Kun käyttäjä yrittää käsitellä jotakin tiedostoa, hän kuuluu ainakin luokkaan maailma ja mahdollisesti myös muihin luokkiin. Käyttäjä saa haluamansa käsittelyluvan tiedostoon (tai hakemistoon), jos hän kuuluu mihin tahansa sellaiseen luokkaan, jonka käyttäjille kyseinen lupa on suojauskoodissa myönnetty.

Käyttäjäluokille voidaan suojauskoodissa antaa halutut seuraavista neljästä oikeudesta: READ, WRITE, EXECUTE, DELETE. Oikeutta CONTROL ei voida antaa tai poistaa, vaan luokat systeemi ja omistaja saavat sen aina automaattisesti, kun taas luokat ryhmä ja maailma eivät voi saada sitä koskaan.

Edellämainituilla oikeuksilla on hieman eri merkitys levytiedostoille ja hakemistotiedostoille (tyyppi .DIR). Levytiedostoille merkitykset ovat seuraavat:

READ	oikeus lukea, tulostaa ja kopioida tiedosto
WRITE	oikeus kirjoittaa tiedostoon tai muuttaa sitä
EXECUTE	oikeus suorittaa tiedosto, joka sisältää suoritusvalmiin ohjelman (.EXE) tai DCL-komentoja (.COM)
DELETE	oikeus tuhota tiedosto
CONTROL	oikeus muuttaa tiedoston suojausta

Hakemistotiedostoille oikeudet DELETE ja CONTROL merkitsevät samaa, mutta READ, WRITE ja EXECUTE poikkeavat hieman:

READ	oikeus lukea ja listata hakemistotiedostoa tähtikonstruktioita käyttäen tai ilman
WRITE	oikeus lisätä ja poistaa tiedostoja sekä muuttaa niiden nimiä hakemistossa
EXECUTE	oikeus etsiä tiedosto hakemistosta sen koko nimeä käyttäen (ilman tähtikonstruktiota)

Jos siis johonkin hakemistoon on ainoastaan EXECUTE-oikeus, eivät komennot

```
$ DIRECTORY
$ DIRECTORY   ABC
```

toimi. Sen sijaan seuraava komento kyllä toimii

```
$ DIRECTORY   ABC.DAT
```

Sekä levytiedostoilla että hakemistotiedostoilla READ-oikeus sisältää myös EXECUTE-oikeuden. Lisäksi on huomattava, että pelkkä WRITE-oikeus ei riitä kirjoittamiseen; sen li-

säksi on oltava myös READ-oikeus.

Suojauskoodi muutetaan komennolla SET PROTECTION. Oikeudet on tällöin lyhennettävä yhden kirjaimen pituisiksi: R, W, E ja D. Käyttäjäluokat voidaan kirjoittaa täydellisinä tai lyhentää halutussa määrin. Eri oikeudet ja käyttäjäluokat voidaan mainita missä järjestyksessä tahansa. Esimerkiksi

```
$ SET PROTECTION=(S:RWED,OWN:ERDW,GROUP:R,W)  DATAFILE.DAT
```

Tämä esimerkkikomento antaa luokille systeemi ja maailma täydet oikeudet tiedostoon DATAFILE.DAT. Luokka ryhmä saa pelkästään lukuoikeuden, ja luokka maailma ei saa mitään oikeutta. Luokalta poistetaan siis oikeudet mainitsemalla luokan nimi ilman oikeuslistaa. Jos sen sijaan komennosta jätetään luokan nimi kokonaan pois, esimerkiksi

```
$ SET PROTECTION=(S:RWED, O:RWED, G:R)  DATAFILE.DAT
```

jäävät kyseisen luokan (maailma) oikeudet ennalleen. Kun luokan oikeuksia muutetaan, ei luokan vanhoista oikeuksista jää mitään "pesämunaksi", vaan vanhat korvataan kokonaan uudella oikeuslistalla.

Hakemistotiedoston suojaus muutetaan samalla komennolla ja aivan vastaavalla tavalla. Jos esimerkiksi käyttäjä haluaa hävittää oman tyhjän alihakemistonsa, on hänen ensin annettava itselleen DELETE-oikeus (jos sitä ei ennestään ole):

```
$ SET PROTECTION=(O:RWED)  ALIHAKEM.DIR
```

Tiedoston tai alihakemiston suojauskoodin voi katsoa komennolla

```
$ DIRECTORY/PROTECTION  ALIHAKEM.DIR
```

Luokkien järjestys on tällöin S, O, G ja W. Päähakemiston

(esim. [MATXX]) suojauksen näkee kirjoittamalla

```
$ DIRECTORY/PROTECTION [000000]MATXX
```

Tiedostojen oletussuojauksen saat selville kirjoittamalla komennon SHOW PROTECTION. Jos haluat muuttaa oletussuojauksen pysyvästi omalta osaltasi esimerkiksi sellaiseksi, että ryhmä saa vain EXECUTE-oikeuden ja maailma ei saa mitään oikeutta, sijoita LOGIN.COM-komentotiedostoosi komento

```
$ SET PROTECTION=(G:E,W)/DEFAULT
```

Sekä tiedostot että hakemistot tulee suojata sopivalla tavalla. Pelkästään jompien kumpien suojaaminen ei takaa, että tiedostot löytyvät tulevaisuudessa muuttumattomina hakemistosta. Näin on siksi, että ensinnäkin taitava ja tiedostohallintajärjestelmää tunteva ohjelmoija voi päästä käsiksi tiedostoon suoraan käyttämättä hakemistoa ja sen suojauksia. Toiseksi, jos suojataan pelkästään tiedosto, mutta ei hakemistoa (eli annetaan muille kirjoitusoikeus hakemistoon), joku toinen käyttäjä voi komennolla RENAME siirtää tiedostot omaan hakemistoonsa.

5.2 ACL-SUOJAUKSET

Jos tavallinen luokkajako (systeemi, omistaja, ryhmä, maailma) osoittautuu riittämättömäksi, voidaan tiedostoille ja hakemistoille määritellä standardisuojauskoodin lisäksi myös ACL-suojauslistoja (Access Control List). Kukin ACL-lista koostuu yhdestä tai useammasta lista-alkiosta eli ACE:stä (Access Control Entry), joilla suojaukset voi asettaa vaikkapa käyttäjäkohtaisesti.

ACL-suojauslistoja on syytä käyttää harkitusti ja säästeliäästi. Joissakin tapauksissa ne ovat todella tarpeellisia, mutta on muistettava, että useiden pitkien ACL-listojen läpikäyminen vie oman aikansa ja hidastaa toimintaa.

Lista-alkion perusosat ovat tunniste (IDENTIFIER) ja oikeuslista (ACCESS-lista). Tunniste kertoo, keitä käyttäjiä oikeuslistan oikeudet koskevat. Tunniste voi olla

a) UIC-tunniste, joita on kahta lajia:

   - käyttäjänumero (UIC-koodi) numeerisessa tai aakkosnumeerisessa muodossa, esim. [175,24], [175,*], [MAT], [MAT,MATXX] tai [MATXX]

   - käyttäjätunnusta tai ryhmätunnusta suoraan vastaava tunniste, esim. MATXX, MAT

b) yleinen tunniste, jonka käyttöpäällikkö on määritellyt systeemitasolla, esim. METSATILASTO tai SIHTEERIT

c) käyttöjärjestelmän määrittelemä tunniste: BATCH, NETWORK, INTERACTIVE, LOCAL, DIALUP ja REMOTE

Yleisiä tunnisteita käyttäen voidaan määritellä uusia ryhmiä, jotka eivät ole sidoksissa osastojakoon. Esimerkiksi tunniste SIHTEERIT voi tarkoittaa kaikkia osastosihteereitä, ja tunniste XYZ_PROJEKTI voi tarkoittaa kaikkia niitä, jotka työskentelevät projektissa XYZ.

Järjestelmän määrittelemät tunnisteet kuvaavat erilaisia prosesseja, joista käsin suojausten tarkistusjärjestelmälle on tullut tiedoston käsittelypyyntö:

tunniste	käsittelypyynnön lähde
BATCH	eräajoprosessi
NETWORK	DECnet-verkon etäissolmun käyn-

	nistämä paikallinen prosessi
INTERACTIVE	vuorovaikutteinen prosessi
LOCAL	käyttäjä paikallisella päätteellä
DIALUP	käyttäjä modeemipäätteellä
REMOTE	käyttäjä, joka on ottanut yhteyden verkkoa ja SET HOST -komentoa käyttäen

Näistä kuudesta tunnisteesta vain yhtä voi käyttää yhdessä lista-alkiossa. Niitä voi muuten liittää vapaasti muihin tunnisteisiin plus-merkillä (+).

Oikeuslistassa on mahdollista nimetä seuraavat oikeudet: READ, WRITE, EXECUTE, DELETE, CONTROL ja NONE. Viimeksi mainittu kieltää nimenomaisesti kaikki oikeudet. Oikeudet liitetään plus-merkillä (+) toisiinsa ja ne voidaan halutaessa lyhentää.

Seuraavassa on esimerkkejä tiedostojen lista-alkioista:

a) (IDENTIFIER=[175,40],ACCESS=READ+WRITE)

Tämä ACE antaa käyttäjälle [175,40] luku- ja kirjoitusoikeuden kyseessä olevaan tiedostoon.

b) (IDENTIFIER=MATXX+BATCH,ACCESS=READ)

Tämä ACE antaa käyttäjän MATXX eräajotöille lukuoikeuden tiedostoon.

c) (IDENTIFIER=DIALUP,ACCESS=NONE)

Kyseinen lista-alkio kieltää kaikki oikeudet tiedostoon kaikilta niiltä käyttäjiltä, jotka ovat yhteydessä keskuskoneeseen puhelinlinjan ja modeemin välityksellä.

d) (IDENTIFIER=XYZ_PROJEKTI,OPTIONS=PROTECTED,ACCESS=READ)

Yllä olevaan lista-alkioon sisältyvä valinnainen lisämääre PROTECTED merkitsee, että kyseistä ACE:tä ei voi hävittää komennolla, jonka tehtävä on poistaa koko ACL yhdellä kertaa (esim. $ SET ACL/DELETE file-name). On käytettävä yksilöidympää komentoa, kuten esimerkiksi

```
$ SET ACL/ACL=(IDENTIFIER=XYZ_PROJEKTI,-
_$ OPTIONS=PROTECTED)/DELETE  file-name
```

Muita mahdollisia lisämääreitä ovat NOPROPAGATE ja NONE. Jos tiedostosta tehdään uusi versio, niin tiedoston ACL-suojauslista siirtyy myös tälle uudelle tiedostolle lukuunottamatta niitä lista-alkioita, joissa on määritelty NOPROPAGATE.

ACL-suojauslistoja voidaan määritellä myös hakemistotiedostoille (tyyppi .DIR). Edelliset esimerkit lista-alkioista sopivat myös hakemistotiedostoille, mutta näille on mahdollista määritellä myös seuraavanlaisia alkioita:

e) (DEFAULT_PROTECTION,S:RWED,O:RWED)

Tämä ACE on toisen tyyppinen kuin edellä esitetyt. Se määrää kyseessä olevaan hakemistoon luotavien uusien tiedostojen oletussuojauksen tavallista luokkajakoa (S, O, G, W) käyttäen.

f) (IDENTIFIER=MAT,OPTIONS=DEFAULT,ACCESS=READ+EXECUTE)

Lisämäärettä DEFAULT voidaan käyttää vain hakemistotiedostoille. Se merkitsee, että kyseinen lista-alkio (DEFAULT-määre poistettuna) liitetään jokaiseen uuteen tiedostoon, joka luodaan kyseiseen hakemistoon.

Oletetaan esimerkin vuoksi, että yleinen oletussuojaus on (S:RWED,O:RWED,GR:RE,W:E) ja hakemiston ALIHAK.DIR tiedostojen oletussuojaukseksi halutaan nyt (S:RWED,O:RWED,G:E,W) sillä lisäyksellä, että käyttäjä MAAXYZ saa aina lukuoikeuden. Tällöin sijoitetaan hakemistotiedoston ALIHAK.DIR suojauslistaan seuraavat kaksi ACE:tä:

```
(DEFAULT_PROTECTION,S:RWED,O:RWED,G:E,W)
(IDENTIFIER=MAAXYZ,OPTIONS=DEFAULT,ACCESS=READ)
```

Kun levytiedoston tai hakemistotiedoston suojauslistaa laaditaan, on kiinnitettävä erityistä huomiota siihen, mihin järjestykseen lista-alkiot sijoitetaan. Tiedostoon liittyvän käsittelypyynnön saatuaan käyttöjärjestelmä alkaa käydä lista-alkioita läpi suojauslistan alusta alkaen siihen saakka, kunnes löytää ensimmäisen lista-alkion, jonka tunniste on yhteensopiva käsittelypyyntöä anovan prosessin kanssa. Tästä alkiosta löytyvä oikeuslista otetaan huomioon, ja muita alkioita ei enää tarkasteta. Siksi on yksittäisiin käyttäjiin liittyvien lista-alkioiden syytä sijaita ennen sellaisia, jotka liittyvät käyttäjäryhmiin. Yksittäiset henkilöthän saattavat nimittäin kuulua myös kyseisiin ryhmiin. Seuraavassa on esimerkki tiedoston suojauslistasta:

```
(IDENTIFIER=[120,45], OPTIONS=PROTECTED,
     ACCESS=READ+WRITE+EXECUTE+DELETE+CONTROL)
(IDENTIFIER=P3_USERS, ACCESS=READ+WRITE+EXECUTE)
(IDENTIFIER=[120,*]+LOCAL, ACCESS=READ)
(IDENTIFIER=[*,*], ACCESS=NONE)
```

Virhe olisi esimerkiksi vaihtaa ensimmäisen ja kolmannen lista-alkion paikkoja. Tällöin käyttäjä [120,45] ei saisi paikallisilta päätteiltä käsin tiedostoon muuta kuin lukuoikeuden, vaikka tarkoitus on antaa kaikki oikeudet.

Mitenkä sitten ACL-suojauslistat liittyvät standardisuojauksiin? VAX/VMS-käyttöjärjestelmä tutkii suojaukset seuraavalla tavalla, kun käyttäjä haluaa käsitellä tiettyä tiedostoa:

a) Ensin tutkitaan ACL-suojauslista, jos sellainen on. Jos suojauslistan ensimmäinen sopiva lista-alkio sallii käsittelyn, niin lupa myönnetään eikä enempää testailla. Jos ensimmäinen sopiva lista-alkio nimenomaisesti kieltää käsittelyn, tutkii järjestelmä kuitenkin vielä tavallisen UIC-suojauskoodin SYSTEM ja OWNER -kentät, jotka lopullisesti ratkaisevat pääsyn.

b) Jos suojauslistan yksikään lista-alkio ei ota kantaa kyseiseen tapaukseen tai jos suojauslistaa ei ole, käytetään tavallista UIC-suojauskoodia asian selvittämiseksi.

c) Jos käsittelypyyntöön ei voida a) tai b) -kohdan perusteella suostua, tutkii järjestelmä vielä, onko käyttäjällä sellaista erityisoikeutta, jonka nojalla käsittelylupa voidaan kuitenkin myöntää.

Sitten onkin vielä syytä kertoa, miten suojauslistat käytännössä tehdään. Mahdollisia komentoja ovat muun muassa seuraavat:

```
$ SET ACL
$ SET FILE/ACL
$ SET DIRECTORY/ACL
```

Komento SET ACL soveltuu sekä levytiedostoille että hakemistotiedostoille, eikä muita kahta välttämättä tarvita.

Suojauslistan tekoon tai muuttamiseen voi käyttää myös ACL-editoria. Se käynnistyy komennoilla

```
$ EDIT/ACL      ABC.DAT
$ SET ACL/EDIT  ABC.DAT
```

Oletuksena on tällöin PROMPT-moodi. Tämä voi kuitenkin tuottaa aluksi hankaluuksia, joten viisainta saattaa olla lisätä edellisiin komentoihin tarkenne /MODE=NOPROMPT.

ACL-editori toimii ainakin VT-sarjan päätteillä. Kun on päässyt editorin sisään, voi <PF2>-näppäimellä hankkia lisäopastusta. Huomautettakoon tässä vain siitä, että painamalla <RETURN> voidaan lista-alkiota jatkaa seuraavalle riville. Kun lista-alkio on valmis, painetaan laskinnäppäimistön (keypad) nollaa tai <ENTER>-näppäintä, ennen kuin uusi lista-alkio aloitetaan uudelta riviltä. ACL-editorista poistutaan painamalla <CTRL/Z>.

Tarkastellaan sitten komentoa SET ACL esimerkkien valossa:

```
$ SET ACL/ACL=(IDENTIFIER=[123,45],ACCESS=READ+EXECUTE) -
_$ XY.DAT
```

Tätä komentoa voidaan käyttää sekä silloin, kun tiedostolla ABC.DAT ei ole ennestään ACL:ää, että silloin, kun sellainen jo on. Jälkimmäisessä tapauksessa uusi lista-alkio sijoitetaan suojauslistan alkuun.

Jos uusi lista-alkio halutaan sijoittaa listassa jo olevan alkion (IDENTIFIER=[150,55],ACCESS=READ+WRITE+EXECUTE) jälkeen, niin lisätään tarkenne /AFTER=(ace) :

```
$ SET ACL/ACL=(IDENTIFIER=[123,45],ACCESS=READ+EXECUTE)-
_$ /AFTER=(IDENTIFIER=[150,55])  ABC.DAT
```

Monta lista-alkiota voidaan luoda kerralla seuraavaan tapaan

```
$ SET ACL/ACL=((IDENTIFIER=[140,20],ACCESS=READ+WRITE), -
_$ (IDENTIFIER=[140,*],ACCESS=READ))  ABC.DAT
```

ja tiedoston ABC.DAT suojauslista voidaan kopioida tiedostolle BCD.DAT komennolla

```
$ SET ACL/LIKE=(OBJECT_NAME=ABC.DAT)  BCD.DAT
```

Suojauslistasta voidaan poistaa lista-alkio seuraavasti:

```
$ SET ACL/ACL=(IDENTIFIER=[150,50])/DELETE  ABC.DAT
```

Tällöin ei tarvitse kirjoittaa ACCESS-listaa näkyviin, mutta mahdollinen OPTIONS-lista on kirjoitettava. Samat säännöt pätevät myös edellä mainitulle /AFTER -tarkenteelle. Koko ACL-suojauslistan (lukuun ottamatta niitä lista-alkioita, jotka sisältävät PROTECTED-määreen) voi hävittää komennolla

```
$ SET ACL/DELETE  BCD.DAT
```

Suojauslistat saa näkyviin komennoilla

```
$ SHOW ACL  ABC.DAT
$ DIRECTORY/ACL  ABC.DAT
$ DIRECTORY/SECURITY  ABC.DAT
$ DIRECTORY/FULL  ABC.DAT
```

Tarkenne /SECURITY on sama kuin /ACL/OWNER/PROTECTION.

5.3 NIMEÄMINEN, TUHOAMINEN JA VARMUUSKOPIOINTI

Pyrittäessä luottamuksellisten aineistojen mahdollisimman hyvään suojaamiseen on syytä kiinnittää huomiota myös tiedosto- ja hakemistonimiin. Vaikka sellaiset nimet kuin PALKKA.LIS tai SECRET.DAT sisältävät työskentelyä helpottavaa informaatiota, ne kuitenkin kiinnittävät mahdollisen systeemimurtautujan huomiota. Silti vain erityistapauksissa kannattaa muuttaa tiedostonimet harhaanjohtaviksi, jottei normaalityölle aiheutuva haitta ylittäisi hyötyä.

DELETE ja PURGE -komentoja käytettäessä tiedostot eivät itse asiassa tuhoudu. Tiedostojen varaama levytila ainoastaan vapautuu muuhun käyttöön ja niiden sisällöt tuhoutuvat vasta, kun joku kirjoittaa niiden päälle uutta tietoa. On periaattessa mahdollista, että joku taitava ja viitseliäs henkilö pääsee siinä välissä lukemaan "hävittämääsi" aineistoa.

Jos haluataan, että käyttöjärjestelmä kirjoittaa "puppua" hävittetyn tiedoston paikalle, käytetään komentoja

```
$ DELETE/ERASE  SECRET.DAT;1
$ PURGE/ERASE   SECRET.LIS
```

Jos tiedostolle määritellään ERASE_ON_DELETE -attribuutti, on /ERASE -tarkenne automaattisesti voimassa, kun joskus kyseessä oleva tiedosto tuhotaan:

```
$ SET FILE/ERASE_ON_DELETE  SECRET.DAT
```

Huomautettakoon kuitenkin, että näitä ERASE-toimenpiteitä ei tule käyttää yleisesti vaan ainoastaan arkaluontoista aineistoa sisältäville tiedostoille tarvittaessa. Päällekirjoittaminen on nimittäin aikaa kuluttavaa, jos sitä teh-

dään suuressa mitassa. Riski, että joku ryhtyisi yrittämään lukea toisen käyttäjän vapauttamalle levytilalle jäänyttä dataa ja onnistuisi siinä, on melko pieni.

METLAn VAX-tietokoneilla tiedostojen varmuuskopiointi (backup) tapahtuu aamupäivisin seuraavan aikataulun mukaan:

Kukin levypakka kopioidaan täydellisesti kuuden viikon välein perjantaisin. Kolmen viimeisimmän täydellisen kopioinnin nauhat säilytetään, joten tietyllä hetkellä vanhimmat kopiot ovat 12-18 viikkoa vanhoja.

Muina perjantaina kopioidaan varmuusnauhoille ne tiedostot, jotka ovat muuttuneet edellisen perjantain jälkeen. Näitä nauhoja säilytetään kuusi viikkoa.

Muina työpäivinä varmuuskopioidaan ne tiedostot, jotka ovat muuttuneet edellisen työpäivän kopioinnin jälkeen. Nämä nauhat säilytetään yhden viikon.

Oletetaan esimerkin vuoksi, että luot uuden tiedoston tiistai-iltapäivällä. Jos et tämän jälkeen muuta tiedostoa ennen kuin vahingossa tuhoat sen, on sinulla seuraavat mahdollisuudet saada se takaisin:

Jos tuhoaminen tapahtuu ennen keskiviikkoaamun varmuuskopiointia, tiedostosta ei ole ehditty ottaa kopiota.

Jos tuhoaminen tapahtuu keskiviikkoiltapäivänä tai seuraavina päivinä, tiedosto löytyy keskiviikon varmuuskopiointinauhoilta seuraavaan keskiviikkoon saakka.

Jos tiedosto elää perjantain varmuuskopiointiin asti, on sen kopio tallessa ainakin kuusi viikkoa.

6 MAGNEETTINAUHOJEN SUOJAAMINEN VAX/VMS-JÄRJESTELMÄSSÄ

Tärkein toimenpide magneettinauhojen suojaamiseksi on huolehtia niiden fyysisestä turvallisuudesta. Tähän kuuluu ennen kaikkea varkauksien estäminen ja tulipalolta suojaaminen. Jos on mahdollista, että joku saa luvatta nauhan käsiinsä ja vie sen jollekin toiselle tietokoneelle, ei nauhaan merkityistä suojauskoodeista ole paljoakaan hyötyä.

VAX/VMS-käyttöjärjestelmässä magneettinauhojen suojaukset voidaan asettaa kahdella tavalla (edellyttäen, että nauhoissa on nimiö):

a) Magneettinauhat voidaan suojata UIC-pohjaisilla suojauskoodeilla. Vain VAX/VMS-järjestelmä tarkista nämä, muut käyttöjärjestelmät ohittavat ne. Koodit ovat nauhakohtaisia, tiedostoja ei voida erikseen suojata.

b) Suojaukset voidaan tehdä ANSI-standardien mukaisesti, kun nauhoja vaihdetaan VAX/VMS- ja muilla käyttöjärjestelmillä toimivien tietokoneiden kesken. Tällöin on mahdollista asettaa tiedostoille omat suojaukset.

Seuraavassa tarkastellaan vain kohdan a) mukaisia suojauksia. Niiden merkitys on lähinnä nauhan lukemisen tai päällekirjoittamisen estämisessä siinä tapauksessa, että nauha-asemaan vahingossa laitetaan väärä nauha.

Magneettinauhojen suojauskoodissa voidaan antaa oikeudet

READ	oikeus lukea ja kopioida nauhaa
WRITE	oikeus lisätä tiedostoja nauhalle

Lisäksi on olemassa CONTROL-oikeus (suojausten muutosoikeus), jonka myöntämisestä järjestelmä pitää huolen. Pelk-

kää kirjoitusoikeutta ilman lukuoikeutta ei voida myöntää, sillä WRITE-oikeus sisältää READ-oikeuden.

Käyttäjäluokat systeemi ja omistaja saavat aina automaattisesti oikeudet READ, WRITE ja CONTROL, eikä näitä oikeuksia voi kyseisiltä luokilta poistaa. Käyttäjäluokat ryhmä ja maailma eivät voi milloinkaan saada CONTROL-oikeutta. Näiden luokkien oletusoikeudet ovat READ ja WRITE.

Kun magneettinauha alustetaan ja sille luodaan nimiö komennolla INITIALIZE, voidaan luokkien ryhmä ja maailma oikeuksia kaventaa esimerkiksi seuraavasti:

```
$ INITIALIZE/DENSITY=1600/PROTECTION=(G:R,W) MTA1: TAPE3
```

Yleensä on syytä poistaa maailmalta oikeudet nauhaan.

METLAssa on magneettinauhojen käsittelyyn tehty komennot ALUSTA ja VARAA. Komennossa ALUSTA on oletussuojauksena (S:RW, O:RW, G:R, W). Suojausta voi muuttaa tarkenteella /PROTECTION. Jos halutaan esimerkiksi kieltää ryhmältä ja maailmalta kaikki oikeudet, kirjoitetaan

```
$  ALUSTA  TEST23/PROT=(G,W)  V458
```

Kun magneettinauha otetaan käsittelyyn pelkällä VARAA-komennolla, sitä voidaan vain lukea. Haluttaessa kirjoittaa nauhalle, on käytettävä komentoa VARAA/WRITE.

7 MIKROTIETOKONEET JA ATK-TURVALLISUUS

Luvussa 2 on jo osittain käsitelty mikrotietokoneita. Tässä luvussa annetaan täydentävää tietoa ja yksityiskohtaisempia ohjeita kertaamatta aikaisemmin esitettyjä asioita.

Laitteistoa sijoitettaessa tulee tutkia, onko vesivahinko seuraavassa kerroksessa mahdollinen. Kannattaa myös ottaa huomioon, ettei viherkasveja kastellessa tarvitsisi kurkoittaa laitteiston yli. Kun hyvä sijoituspaikka on löytynyt, huolehditaan laitteiston maadoituksesta ja vältetään sen siirtelyä sekä muuta tärinää. Herkästi palavia materiaaleja ei tule pitää hajallaan laitteen ympärillä.

Laitteisto tulee merkitä niin, että sen pystyy tunnistamaan varkaustapauksessa. Laitoksessa on oltava ajan tasalla oleva atk-laiterekisteri, johon merkitään laitteiden nimet, mallit ja valmistusnumerot (ja ehkä tunnistusmerkinnätkin).

Yleisimmät häiriöt mikrotietokoneiden käytössä aiheutuvat levykkeiden tai niiden sisältöjen tuhoutumisesta. Pahimmat viholliset ovat savu, pöly, korkea lämpötila (yli +50°C), staattinen sähkö, magneettikentät, nesteet, tahmeat aineet sekä mekaaniset vauriot (esim. naarmut). Tietoja saattaa kadota levykkeiltä myös sähköhäiriöiden takia.

Tulisi huolehtia siitä, ettei irrallisia levykkeitä ole esillä. Levykkeitä, joita ei parhaillaan käytetä koneessa, pitäisi säilyttää suojakoteloissaan säilytyslaatikossa.

Tupakansavu voi tehdä levykkeistä lukukelvottomia. Levykkeet eivät toimi, jos niiden päälle karistetaan tuhkaa tai sokeria tai kaadetaan kahvia. Levykkeet sietävät melko hyvin puhdasta vettä, mutta epäpuhtaudet vedessä voivat vahingoittaa niitä. Myös sormenjälki levykkeellä voi vaikeuttaa lukemista ja kirjoittamista.

Levykkeitä ei pidä sijoitaa sähköisten laitteiden (kuten radion, kaiuttimen tai kuvaruudun) päälle, ikkunalaudalle tai lämpöpatterin lähelle. Paperille, jonka alla on levyke, ei tietenkään tule kirjoittaa. Levykkeen etikettiin voi kirjoittaa vain huopakynällä, jos se on jo kiinnitetty levykkeeseen.

Luottamukselliset ja salattavat tiedot on hyvä tallettaa omille levykkeilleen ja säilyttää ne erillään muista.

Alla on muutamia neuvoja levykkeiden varmuuskopioinnista:

- Jos datatiedostoon tai ohjelmaan tehdään muutoksia, otetaan kopio sekä ennen muutoksia että niiden jälkeen. Erityisen tärkeistä ohjelmista ja tiedostoista on hyvä olla kaksi varmuuskopiota.

- Vaikka muutoksia ei tehtäisikään, otetaan silti säännöllisin väliajoin varmuuskopiot kaikista levykkeistä. Levykkeiden käyttöikä on rajallinen: vaikkei mitään ulkoista vahinkoa niille tapahtuisikaan, ne tulevat toimintakyvyttömiksi ennemmin tai myöhemmin (riippuen valmistajasta ja yksilöstä). Levykkeitä hankittaessa onkin järkevää kiinnittää huomiota myös laatuun eikä ainoastaan hintaan. Ilman keskusaukon vahvikerengasta myytävät levykkeet kannattaa jättää ostamatta.

- Tulisi pitää kirjaa siitä, milloin ja mitä on varmuuskopioinut ja missä kopiot ovat. Jos tallennetut tiedot on helppo saada myös muualta, voi kopioita säilyttää pelkästään erityisessä levykkeiden säilytyslaatikossa, jota pidetään lukitussa teräskaapissa eri huoneessa. Vaikeasti korvattavien tiedostojen ja ohjelmien kopiot on syytä säilyttää disketti- tai datakaapeissa.

- Jos jonkin levykkeen toiminnassa ilmenee virheitä ja päätetään turvautua varmuuskopioon, tulee ensin tarkistaa, että laitteisto toimii kunnolla testaamalla sitä toisilla (vähemmän tärkeillä) levykkeillä. Näin vältetään varmuuskopion tuhoutuminen. Jos kuitenkin on syytä epäillä levykkeen vahingoittuneen esimerkiksi savun tai lämmön johdosta, ei sitä kannata yrittää itse lukea, koska se voi pahentaa mahdollista vahinkoa. Asiantuntija voi arvioida tilanteen ja yrittää pelastaa talletetun tiedon mahdollisuuksien mukaan.

Jos mikrotietokoneeseen kuuluu kiinteä levyasema (kovalevy, umpilevy, "Winchester"), on tarpeen huolehtia myös sen varmuuskopioinnista. Suositeltavaa on kopioida kiinteän levyaseman tiedot VAX-tietokoneelle KERMIT-ohjelman avulla.

Kiinteä levyasema on hyvä järjestää hierarkiseksi siten, että päähakemisto sisältää lähinnä vain alihakemistojen nimet. Toiselle hakemistotasolla (ensimmäisellä alihakemistotasolla) voisi olla harvoin muuttuvat tiedostot kuten ohjelmat. Kolmannella hakemistotasolla olisivat muuttuvat tiedostot kuten data-aineistot ja työtiedostot. Koska varmuuskopiointi suoritetaan hakemistoittain, ei useimmiten tarvitse kopioida kuin kolmannen tason hakemistot. Päähakemiston ja toisen tason hakemistot voi kopioida harvemmin.

Samoin kuin levykkeet myös itse tietokone voi vahingoittua, jos se joutuu alttiiksi savulle, kosteudelle tai korkealle lämpötilalle. Esimerkiksi kostea piirikortti saattaa tuhoutua, kun jännite kytketään päälle. Tällaisissa tilanteissa ei itse kannata suorittaa koeajoja. Tarvittaessa tulee ottaa yhteyttä tietokoneen saneeraukseen perehtyneisiin henkilöihin esimerkiksi matemaattisen osaston kautta.

8 LISÄTIETOJA

Edeltävissä luvuissa on käsitelty salasanojen ylläpitoa sekä tiedostojen ja magneettinauhojen suojauksia VAX/VMS-käyttöjärjestelmässä. Joihinkin erityisohjelmistoihin liittyy kuitenkin oma suojausmenetelmänsä.

Esimerkiksi yleisessä tietohakemistossa (CDD) on omat suojauskoodinsa, joita käyttää myös kysely- ja raportointikieli DATATRIEVE. Tavalliset tiedostosuojaukset eivät tähän sovellu, sillä tietohakemisto muodostuu yhdestä tai useammasta isosta tiedostosta, joiden sisällä eri osat kuuluvat eri käyttäjille.

Samoin relaatiotietokantaohjelmistossa VAX Rdb/VMS on tietokantojen käyttöoikeuksien määrittämiseksi omat suojauslistansa, jotka muistuttavat ACL-suojauslistoja. Käyttöoikeuksien määrittämiseen ei tule käyttää varsinaisia tiedostosuojauksia eikä tietohakemistosuojauksia. Tietokantatiedostojen oletustiedostosuojaus antaa pääsyoikeudet vain SYSTEM-luokalle eli käytännössä tietokannan hallintajärjestelmälle, eikä tätä oletustiedostosuojausta yleensä tule muuttaa.

Tietohakemiston ja tietokantojen suojauksia on käsitelty ja tullaan käsittelemään näihin aiheisiin liittyvissä koulutustilaisuuksissa, joten niistä ei tässä julkaisussa lähemmin kerrota.

KIRJALLISUUTTA

Boulanger, J. & Kenealy, P. 1985. A look at LazerLock. Digital Review, March, 50-51.

Colbert, Mary 1986. Ports of entry. Digital Review, April, 71-77.

Delmage, Sherman H. 1985. No trespassing. Digital Review, March, 31-34.

Fegreus, Jack 1986. When jabberwocky makes sence. Digital Review, April, 65-68.

Guide to VAX/VMS system security, July 1985. Digital Equipment Corporation, Maynard, Massachusetts.

Kämäräinen, Kristiina 1986. Tehokas tiedonsuojaus. I.D.E.A. 2:26-28.

Lafauci, Richard 1985. Safe and sound. Digital Review, March, 81-82.

Ledell, Roman & Voutilainen 1985. Tietosuoja-opas mikrotietokoneiden käyttäjille. Amersoft & Proteva security.

Salomaa, Arto 1985. Tietosuojauksen kehittäminen. Matemaattisten aineiden aikakausikirja 4:283-291.

Schlosberg, Jeremy 1985. Out of site. Digital Review, March, 37-41.

Voipio, Raimo 1986. Tieto suojaan. Puhelin 1:24-25.

Zipp, Eric 1985. Security tips for VMS system managers. Digital Review, March, 43-47.

Zipp, Eric 1985. More security tips for VMS system managers. Digital Review, April, 85-88.

Zipp, E. & Shannon, T. C. 1986. Restricted access. Digital Review, April, 49-56.

LIITE: METLAN TIETOKONEIDEN KÄYTTÖEHDOT

Käyttöoikeus

Henkilö, jolla on työsuhde METLAan, on oikeutettu käyttämään laitoksen tietokoneita työssään. Mikrotietokoneita lukuunottamatta tietokoneiden käyttöä varten tarvitaan erityinen käyttölupa. Erikoisluvalla voidaan käyttöoikeus myöntää myös muille seuraavasti:

- Henkilö, joka on METLAn jonkin osaston ulkopuolinen tutkija, saa käyttää tietokoneita METLAan liittyvässä työssään.
- Helsingin yliopiston metsäalan tutkijoilla on oikeus käyttää Helsingin VAXia METLAn ja Helsingin yliopiston välisen atk-yhteistyösopimuksen puitteissa. METLAn tutkijoilla on saman sopimuksen mukaan oikeus käyttää yliopiston (keskus)tietokonetta.
- Muut (seuraavassa "ulkopuoliset"), kuten esim. laudaturtöitään tekevät opiskelijat, saavat töitä valvovan METLAn toimintayksikön päällikön luvalla käyttää METLAn tietokoneita käyttöluvassa määritellyissä tehtävissä.

Kukin toimintayksikkö on vastuussa siitä, että käyttöluvan hakija tarvitsee ja käyttää tietokoneita työtehtäviensä suorittamiseen ja siitä, että käyttötarpeen tai työsuhteen lakatessa myös käyttöoikeus päättyy.

Käyttöoikeuden valvonta

Matemaattinen osasto vastaa laitoksen yleisessä käytössä olevista tietokoneista ja valvoo niiden käyttöä. Jokaisella tietokoneella on henkilö, joka vastaa koneesta ja valvoo siihen liittyviä käyttölupia. Häntä kutsutaan seuraavassa laitteiston vastuuhenkilöksi. Käyttäjätunnukset on ryhmitelty METLAn toimintayksiköiden mukaan. Tunnus liittyy aina johonkin toimintayksikköön. Jokaiseen käyttäjätunnukseen liittyy salasana, jonka tarkoitus on varmistaa että tunnusta voi käyttää ainoastaan sen omistaja. Tunnuksen omistaja on velvollinen pitämään salasanansa omana tietonaan ja olemaan paljastamatta sitä muille.

Käyttäjäksi liittyminen

Kunkin tietokoneen käyttöä varten on matemaattiselta osastolta haettava HENKILÖKOHTAINEN käyttäjätunnus. Hakemus tehdään käyttölupalomakkeella, jonka saa toimintayksikön sihteeriltä. Tunnus on konekohtainen ja haet-

tava jokaiselle koneelle erikseen.

Käyttöluvan voimassaolo

Vakituisessa työsuhteessa METLAan oleville myönnetään jatkuva käyttöoikeus. Kaikilla muilla käyttölupa on määräaikainen:

- Määräaikaisessa työsuhteessa olevan henkilön käyttölupa on voimassa korkeintaan työsuhteen päättymispäivään asti.
- Muu käyttölupa on voimassa niin kauan kuin hakemuksessa ilmoitetaan, kuitenkin enintään kuusi kuukautta kerrallaan. Käyttölupaan voidaan hakea jatkoaikaa. Menettelytapa on tällöin sama kuin uutta tunnusta haettaessa.

Vanhentuneet käyttäjätunnukset poistetaan, mutta niiden tiedostot viedään sitä ennen magneettinauhalle.

Muutokset käyttölupaan

Työsuhteen päättyminen tai vakinaistuminen, henkilön siirtyminen toiseen toimintayksikköön tai työsuhteen keston muutos vaikuttavat myös käyttöoikeuteen. Tällöin muutoksesta on heti ilmoitettava matemaattiselle osastolle kirjallisesti käyttölupalomaketta käyttäen. Käyttäjätunnusta EI SAA SIIRTÄÄ henkilöltä toiselle. Sen sijaan uuden tunnuksen hakemisen yhteydessä toimintayksikkö voi ilmoittaa, että poistetun tai poistettavan tunnuksen tiedostot siirretään avattavalle uudelle tunnukselle.

Seuraamukset väärinkäytöstä

Jos VAXia käytetään lupaehtojen vastaisesti, siitä seuraa vähintään käyttöoikeuden menettäminen määräajaksi.

KÄYTTÖLUVAN HAKEMINEN

Joensuun tutkimusasema käyttää Joensuun yliopiston tietokonetta ja käyttöluvan hakeminen tapahtuu yliopiston noudattamien pelisääntöjen mukaan. METLAn hallinnassa olevilla koneilla lupaa haetaan seuraavasti:

Uuden käyttöluvan hakeminen

Käyttöluvan eli käyttäjätunnuksen hakija täyttää ja allekirjoittaa käyttölupalomakkeen annettujen ohjeiden mukaan. Sen jälkeen toimintayksikön päällikkö tarkistaa, että hakija täyttää käyttöoikeuden edellytykset ja että lomakkeen tiedot, kuten työsuhteen kestoaika, pitävät paikkansa, ja vahvistaa tämän allekirjoituksellaan. Jos kyseessä on ulkopuolinen käyttäjä, tarvitaan työtä valvovan yksikön päällikön allekirjoitus sekä selvitys käyttötarkoituksesta ja käyttötarpeen kestoajasta.

Hakemus lähetetään tietokoneen vastuuhenkilölle, joka luo käyttäjätunnuksen ja ottaa yhteyden tunnuksen hakijaan ja kertoo mm. millä salasanalla tunnusta ensimmäisen kerran voi käyttää. Tunnuksen omistaja ottaa yhteyden tietokoneeseen ja vaihtaa heti salasanan.

Käyttäjätunnuksen tietojen muuttaminen

Jos käyttäjän työsuhde muuttuu, jos ulkopuolinen käyttäjä hakee jatkoaikaa käyttöluvalleen, tai yleensä jos käyttöluvan hakemuksessa ilmoitettuja tietoja halutaan muuttaa, menetellään kuten uutta tunnusta haettaessa. Ulkopuolisilla käyttäjillä tarvitaan työtä valvovan yksikön päällikön allekirjoitus ja samanlainen selvitys, kuin uutta tunnusta haettaessa.

Käyttöluvan lopettaminen

Jos käyttäjätunnuksen omistajan työsuhde päättyy tai jos käyttölupaa ei enää tarvita, toimintayksikkö täyttää käyttölupalomakkeelle omistajan nimen, käyttäjätunnuksen, lopettamisen syyn sekä lopettamispäivämäärän ja lähettää lomakkeen tietokoneen vastuuhenkilölle. Näin ei kuitenkaan tarvitse tehdä mikäli kyseessä on määräpäivänä vanheneva määräaikainen käyttölupa.

METSÄNTUTKIMUSLAITOS

Matemaattinen osasto
Osoite: PL 37, 00381 HELSINKI (Kornetintie 8) ja
Unioninkatu 40 A, 00170 HELSINKI
Puhelin: (90) 556 276 ja
(90) 661 401

Pekkonen, Timo, vs. professori

Klippi, Lea, tutkimussihteeri

Menetelmät
Häkkinen, Risto, matemaatikko
Heinonen, Jaakko, tutkija (Joensuun tutkimusasema)
Linnilä, Kimmo, tutkija
Sievänen, Risto, tutkija

Atk
Pöntinen, Jukka, atk-päällikkö
Herrala-Ylinen, Helena, tutkija
Kaila, Erkki, tutkija (Rovaniemen tutkimusasema)
Kinnunen, Hilkka, tutkija (Rovaniemen tutkimusasema)
Mäkinen, Markku, tutkija
Salmi, Veli-Pekka, atk-suunnittelija
Snellman, Carl-Gustaf, tutkija
Granlund, Hilkka, pääoperaattori
Soimula, Maire, operaattori
Virtanen, Eija, tutkimusapulainen (Rovaniemen tutkimusasema)

Metsätilasto
Uusitalo, Matti, tutkija
Aarne, Martti, tutkija
Lehto, Kari, tutkija
Mäki-Simola, Elina, tutkija
Leppäkumpu, Tuula, toimistosihteeri
Kämäräinen, Paula, toimistosihteeri

Metsäverotus
Rauskala, Raimo, vanhempi tutkija
Kakkuri, Eero, tutkija
Kulju, Irma, toimistosihteeri
Mäkinen, Kaija, ohjelmoija

Sivulliset tutkijat
Hari, Pertti, dosentti
Heikinheimo, Lauri, emer. professori
Kallio, Markku, professori
Rytkönen, Antti, metsänhoitaja

Matemaattisella osastolla ilmestyneet Metsäntutkimuslaitoksen tiedonantoja -sarjan viimeisimmät julkaisut:

nro 88 Martti Aarne & Matti Uusitalo. Yksityisluontoisten metsien raakapuun kanto- ja hankintahinnat hakkuuvuoden 1982/83 alkupuoliskolla. 3 s. 1983.

nro 92 Martti Aarne. Markkinahakkuut 1.7. - 31.12.1982 ja kalenterivuonna 1982 piirimetsälautakuntien alueittain. 14 s. 1983.

nro 93 Eero Kakkuri. Ilomantsin luonnonsuojelualueiden taloudellinen merkitys puuntuotannolle ja matkailulle. 23 s. 1983.

nro 128 Raimo Rauskala. Kunnittaiset kantohinnat ja puukuutiometrin bruttoarvot hakkuuvuonna 1982/83. 38 s. 1984.

nro 149 Pertti Hari, Kullervo Kuusela, Pentti K. Räsänen, Risto Seppälä. Metsäntutkimukseen liittyvistä kehityssuunnista. 38 s. 1984.

nro 152 Eero Kakkuri. Yksityismetsänomistajien puun kasvatuksen kulut vuosina 1981 ja 1982. 17 s. 1984.

nro 157 Erkki Kaila ja Markku Taipale. Tutka-tiedonhallintaohjelmisto Tietokannan muodostus ja käyttö. 113 s. 1984.

nro 176 Raimo Rauskala. Forest taxation and roundwood supply in Finland. 12 s. 1985.

nro 183 Staffan Ringbom. Virkesproduktionens totala lönsamhet och dess mätning. 32 s. 1985.

nro 191 Raimo Rauskala. Kunnittaiset kantohinnat ja puukuutiometrin bruttoarvot hakkuuvuonna 1983/84. 44 s. 1985.

nro 194 Heinonen, J., Penttinen, A., Salminen, S., Tomppo, E. Spatiaalisen tilastotieteen soveltaminen metsäntutkimukseen. 129 s. 1985.

nro 223 Raimo Rauskala. Kunnittaiset kantohinnat ja puukuutiometrin bruttoarvot hakkuuvuonna 1984/85. 55 s. 1986.

nro 224 Eero Kakkuri. Puun hintojen vaihtelu kuntien sisällä hakkuuvuonna 1980/81. 22 s. 1986.

nro 240 Eero Kakkuri. Yksityismetsänomistajien puun kasvatuksen kulut vuosina 1983 ja 1984. 22 s. 1986.

ISBN 951-40-0856-1
ISSN 0358-4283