

Käyttöjärjestelmät II

TIETOTURVA

Ch 16 [Stal 05]

Suojaus (security)

n **Salakirjoitus**

App 16A [Stal 05]

n **Uhat**

- u turvallisuusuhat
- u pahantahtoiset ohjelmat
- u tunkeutujat

Ch 16 [Stal 05]

n **Suojaus**

- u suojausympäristöt
- u virustorjunta
- u luotettu järjestelmä

Luento 11

n **UNIX: suojaus (Ch 10.7 [Tane 01])**

Luento 12

n **W2K: suojaus (Ch 11.8 [Tane 01])**

Käyttöjärjestelmät II

Salakirjoitus

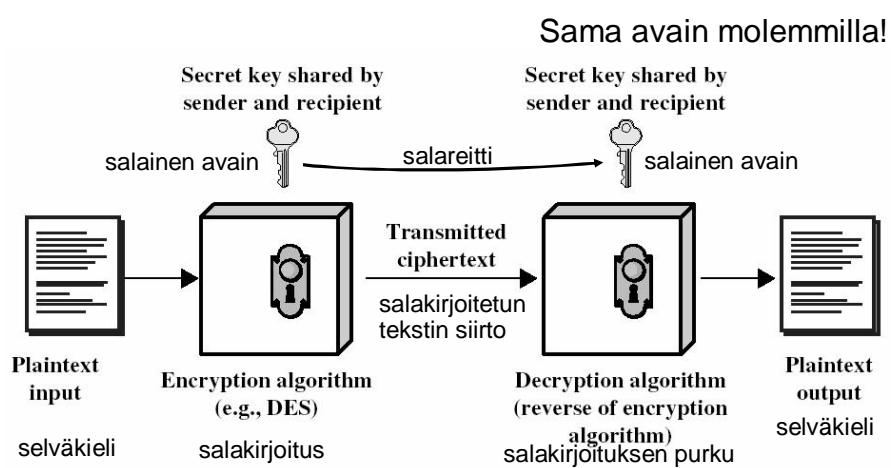
Appendix 16A [Stal 05]

KJ-II K2006 / Auvo Häkkinen - Teemu Kerola

24.4.2006

3

Perinteinen, symmetrinen salaus



(Fig 16.14 [Stal 05])

KJ-II K2006 / Auvo Häkkinen - Teemu Kerola

24.4.2006

4

DES: Data Encryption Standard

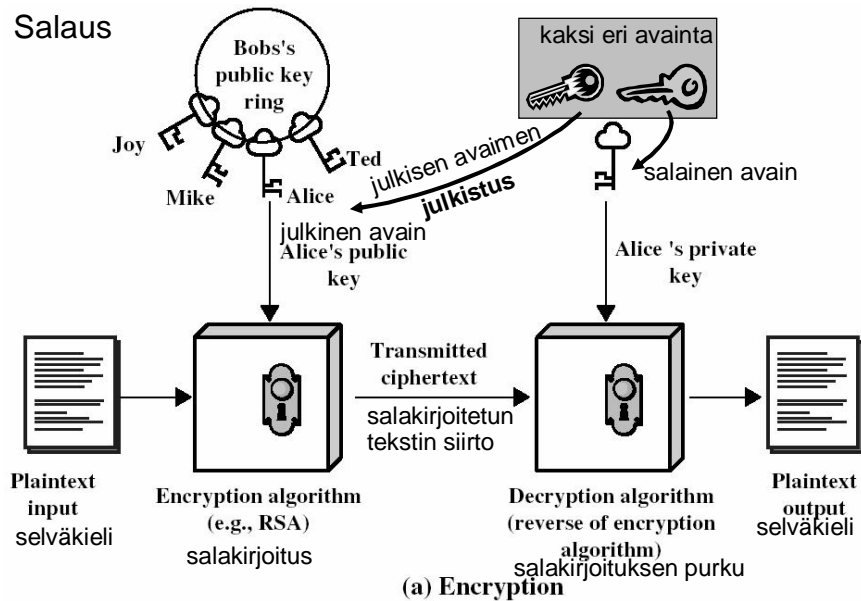
- n **Symmetrinen: sama avain molemmissa**
 - u perustuu Lucifer algoritmiin (Horst Feistel, IBM), 1977
- n **Avain 56 bittiä (plus 8 pariteettibittiä)**
 - u kryptaus 64 bitin lohkoissa
- n **Iteroi lohkolle 16 kertaa bittiopeeraatioita**
 - u eri kierroksella alkuperäisen avaimen eri 48 bittiä avaimena
 - u kierrosten välillä
 - F sekoita bittien järjestystä
 - F korvaa bittikuvioita toisilla
- n **Pystytty murtamaan erikoislaitteistolla**
 - u brute-force, muutama tunti
- n **Triple DEA**
 - u käyttää kolmea DES-avainta (168b + 24 pariteettibittiä)
 - u kolme peräkkäistä DES'iä (encrypt-decrypt-encrypt)

AES – Advanced Encryption Standard

- n **DES seuraaja, Rijndael lohkosalaaja** [click](#)
 - u Joan Daemen & Vincent Rijmen (Belgia), 2000
- n **eri kokoisia avaimia: 128b, 192b, 256b**
- n **lohkon koko 128b**
- n **eri moodeja**
 - u nopeampi vai suojatumpi?
- n **piirteitä**
 - u "alkuluku" polynomit (irreducible polynomials)
 - u polynomien kertolasku
 - u alkuperäistä avainta laajennetaan ja siitä johdetaan dynaamisesti vaihtuvat avaintilat, joista johdetaan kussakin vaiheessa käytettävä avain

Julkisen avaimen salakirjoitusmenetelmä

Saltaus



(a) Encryption

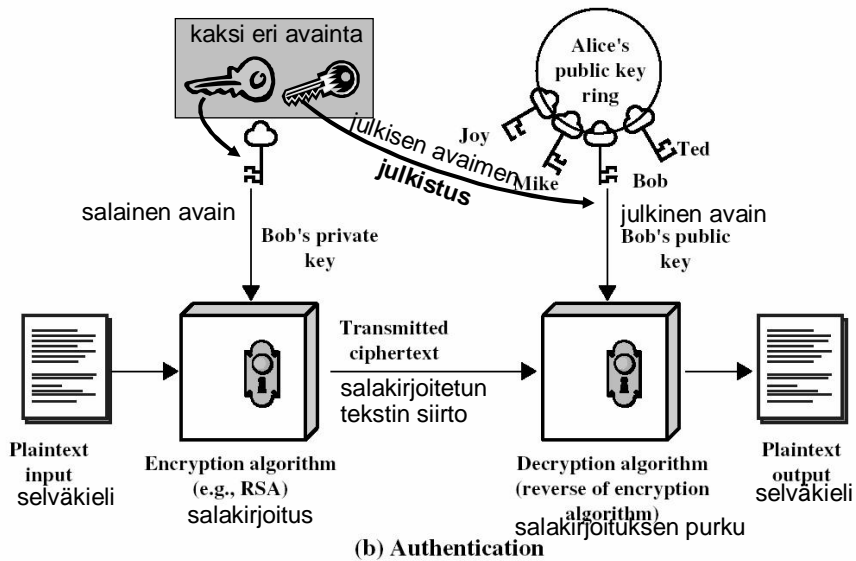
(Fig 16.15 (a) [Stal 05])

KJ-II K2006 / Auvo Häkkinen - Teemu Kerola

24.4.2006

7

Autentikointi julkisen avaimen menetelmällä



(b) Authentication

(Fig 16.15 (b) [Stal 05])

KJ-II K2006 / Auvo Häkkinen - Teemu Kerola

24.4.2006

8

Julkisen avaimen salakirjoitus

- n **Perustuu matemaattisiin funktioihin, ei bittitason operaatioihin**
 - u Diffie Hellman 1976
 - u moduloaritmetiikka, laskennallisesti erittäin vaikeaa ilman avaimia
 - u perustuu hyvin pitkiin (300 numeroa?) alkulukuihin ja aikaavievään polynomiaaliseen (*siis ei NP-täydelliseen*) tekijöihinjako-ongelmaan
- n **Asymmetrinen: kaksi avainta**
 - u julkinen publ: kryptaa tällä
 - u salainen secr: pura tällä $\text{plain} = \text{Decrypt}_{\text{secr}} (\text{Crypt}_{\text{publ}} (\text{plain}))$
- n **Voi tehdä myös toisin päin**
 - u salainen secr: kryptaa tällä
 - u julkinen publ: pura tällä $\text{plain} = \text{Decrypt}_{\text{publ}} (\text{Crypt}_{\text{secr}} (\text{plain}))$
- n **RSA-algoritmi**
 - u Rivest, Shamir, Adleman 1977 Lisää tietoja Tietoturvakurssilla
 - u samoja avainpareja voi käyttää kummin päin vain!
 - u käytetään nyt melkein kaikkialla avainten jakeluun

Käyttöjärjestelmät II

Turvallisuusuhat

Turvallisuustarpeet

Fig 16.1 [Stal 05]

- n **Suojattu pääsy tietoon** protection
 - u kellä pääsy mihin tietoon muistissa
- n **Kontrolloitu järjestelmän käyttö** user authentication
 - u kuka käyttää järjestelmää eli käyttäjän tunnistus
- n **Suojattu tiedon siirto järjestelmien välillä**
 - u verkkoyhteyksien suojaus network security
- n **Suojattu tiedostojen käyttö** file security
 - u kellä pääsy mihin tietoon tiedostojärjestelmässä

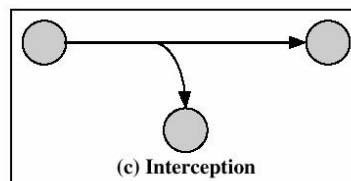
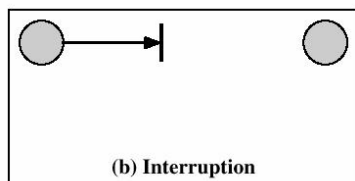
Turvallisuusvaatimuksia

- n **Luottamuksellisuus (confidentiality, secrecy)**
 - u tietoa saa lukea vain ne, joilla siihen lupa
 - u ei välttämättä tietoa edes tiedon olemassaolosta
- n **Eheys, koskemattomuus (integrity)**
 - u tietoa saa tuottaa/muuttaa vain ne, joilla siihen lupa
- n **Saatavuus (availability)**
 - u tieto oltava saatavilla käyttötarkoituksen mukaisesti
- n **Oikeaksi todentaminen (authenticity)**
 - u tiedon käyttäjä pystyttävä todentamaan siksi,
joka väittää olevansa
 - ⊞ kuka on? mitä tietää? mitä omistaa?

Uhkia

DoS – denial of service

- n **Häirintä, pysäyttäminen, "ilkivalta" (interruption)**
 - u tiedon tuhoaminen tai saatavuuden estäminen
 - u esim. kovalevy tuhottu, tietoliikennelinja katkaistu, tiedostojärjestelmä kytketty toiminnasta

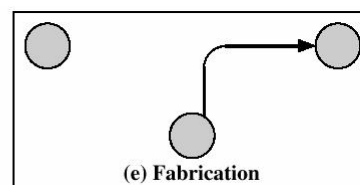
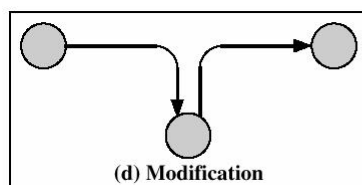


(Fig 16.2 [Stal 05])

- n **Sieppaus (interception)**
 - u luottamuksellisen liikenteen salakuuntelu
 - u kopiointi

Uhkia

- n **Muuntelu, "peukalointi" (modification)**
 - u tiedon korvaaminen muutetulla tiedolla
 - u esim. ohjelman toimintaa / datatiedostoa muutettu, sanomien väärentäminen



(Fig 16.2 [Stal 05])

- n **Valmistus, "satuilu" (fabrication)**
 - u järjestelmän tietojen muuttaminen, jotta saadaan haluttu (luvaton) toiminta
 - u esim. tekaistut tietueet, tunnukset, sanomat

Suojattavaa ja uhkia

Tbl 16.1 [Stal 05]

n Laitteisto

- u haavoittuvin osa tietokonejärjestelmää
 - F saatavuus, luottamuksellisuus, eheys, oikeaksi todentaminen
- u vaikea käyttää automaattisia turvajärjestelyjä
 - F lukitut konehuoneet, piilotetut kaapelitot
 - F pääsynvalvonta

n Ohjelmisto

- u haavoitettavana saatavuus: tuhottu, muutettu
- u tietoturva ylläpitohenkilökunnan vastuulla
- u osa automatisoitavissa
 - F varmuuskopiot
 - F tarkistussummat

Suojattavaa ja uhkia

Tbl 16.1 [Stal 05]

n Data

- u haavoitettavana
 - F saatavuus
 - F luottamuksellisuus
 - F eheys
- u ylläpito käyttäjien vastuulla
 - F oltava käyttöoikeuksia
- u tärkeä tieto voi olla analysoitavissa muita tietoja yhdistelemällä, vaikkei itse tietoon pääse suoraan käsiksi

Passiiviset hyökkäykset (kuuntelu)

Fig 16.3 [Stal 05]

- n **Luottamuksellisuus rikkoontuu, eheys ei rikkoudu**
- n **Tietoliikenneyhteydet, -verkko**
 - u salakuuntelu, tarkkailu, vuotaminen julkisuuteen (release of contents)
 - u puhelut, sähköposti, tiedostojensiirto
 - u salaus, salakirjoitus
 - F silti analysoitavissa (traffic analysis)

Aktiiviset hyökkäykset

- n **Tiedon eheys rikkoontuu**
- n **Tietoliikenneyhteydet, -verkko**
 - u lähettäjä teeskentelee olevansa joku muu (masquerade) Fig 16.4 (a) [Stal 05]
 - u virheellinen toisto (replay) Fig 16.4 (b) [Stal 05]
 - u viivyttäminen, muuttaminen, uudelleenjärjestely (modification of msg contents) Fig 16.4 (c) [Stal 05]
 - u käytön esto (DoS = denial of service) Fig 16.4 (d) [Stal 05]
 - F ylikuormitus, yhteyksien sabotointi
 - F yritetään havaita ja toipua nopeasti

Käyttöjärjestelmät II

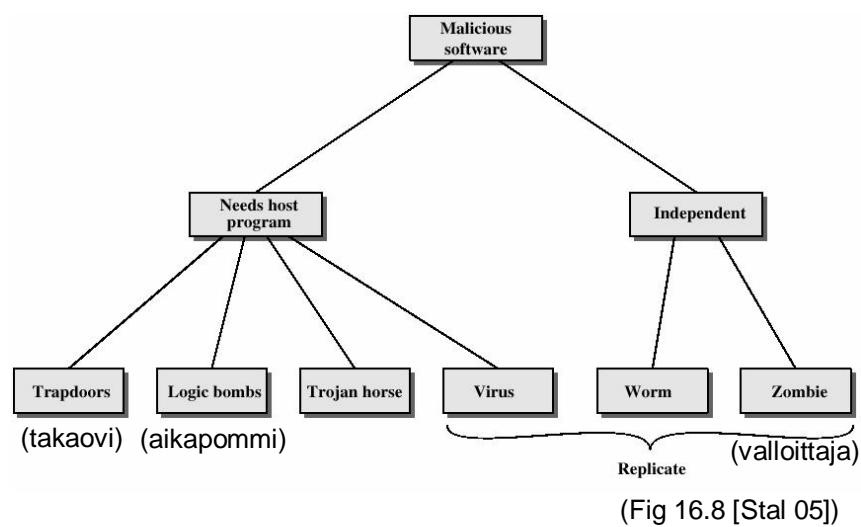
Pahantahtoiset ohjelmat (Malicious software)

KJ-II K2006 / Auvo Häkkinen - Teemu Kerola

24.4.2006

19

Luokittelua



KJ-II K2006 / Auvo Häkkinen - Teemu Kerola

24.4.2006

20

Takaovi (salaovi, trap door)

Fig 16.8 [Stal 05]

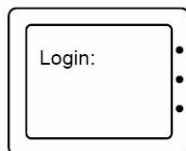
- n **Ohjelmoijan / testaajan oikopolku sopivaan kohtaan koodia**
 - u ko. haaraan pääsee ei-julkisella näppäilyllä
 - u välttää kaikenmaailman hidastavat alustukset ja salasanat Fig 9-10 [Tane 01]
 - u esim. takaa eteenpäin pääsyn, vaikka testaus muuten jumittaisi
 - F laillinen käyttö, joka "unohtunut" koodiin
- n **Mukamas "tietoturvapäivitys", mutta sisältääkin heikennystä / takaoven lisäämisen...**
 - u päivitys vain luotettavalta taholta

```
while (TRUE) {
    printf("login: ");
    get_string(name);
    disable_echoing( );
    printf("password: ");
    get_string(password);
    enable_echoing( );
    v = check_validity(name, password);
    if (v) break;
}
execute_shell(name);
(a)
```

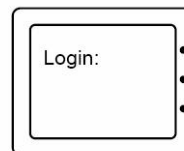
```
while (TRUE) {
    printf("login: ");
    get_string(name);
    disable_echoing( );
    printf("password: ");
    get_string(password);
    enable_echoing( );
    v = check_validity(name, password);
    if (v || strcmp(name, "zzzzz") == 0) break;
}
execute_shell(name);
(b)
```

Fig. 9-10. (a) Normal code. (b) Code with a trap door inserted.

[Tane 01]



(a)



(b)

Fig. 9-9. (a) Correct login screen. (b) Phony login screen.

Looginen pommi (aikapommi, logic bomb)

Fig 16.8 [Stal 05]

- n **Ohjelmassa koodinpätkä, joka suoritetaan, kun tietyt ehdot täyttyvät**
 - u joku tiedosto olemassa / puuttuu
 - u tietty viikonpäivä
 - u tietty käyttäjä
 - u tietylle käyttäjälle ei maksettu palkkaa 2 kk:een
- n **Kiristys ... vai ”konsulttipalkkio”**
 - u poista pommi
 - u laita uusi, parempi tilalle?

Troijan hevonen

- n **Hyödyllinen (tai siltä näyttävä) ohjelma, joka ajettaessa tekee muutakin kuin leipätyötään**
 - u hävittää tiedostoja
 - u antaa muille oikeuksia
- n **Houkuttele laillinen käyttäjä ajamaan ohjelmaa**
 - u hänen oikeuksillaan pahanteko onnistuu
 - anna käyttäjälle Pahis tai käyttäjän Pahis ohjelmalle P super-user oikeudet
- n **Ei näy välttämättä lähdekoodissa**
 - u kääntäjää, kirjastoa peukaloitu?
 - u muutos vain binäärissä?
- n **Login spoofing**
 - u CTR-ALT-DEL toimiva lääke

Fig 9-9 [Tane 01]

Puskurin ylivuoto (buffer overflow)

- n Koodissa vakiopituinen taulukko
- n Indeksiä tai merkkijonon pituutta ei tarkisteta
- n Talletus muuttaa tietoa muualla
 - u esim. aliohjelmasta paluusoite

Fig 9-11 [Tane 01]

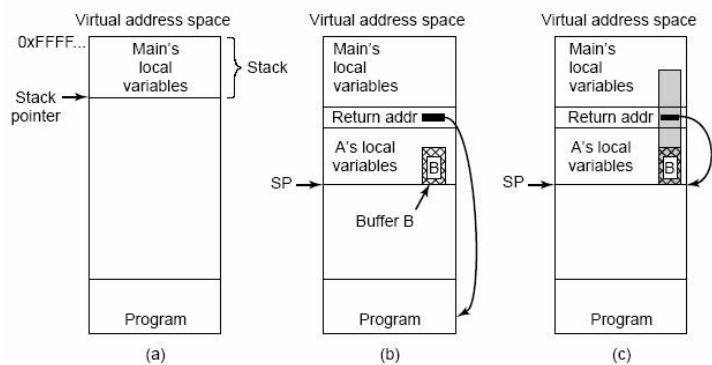


Fig. 9-11. (a) Situation when the main program is running. (b) After the procedure A has been called. (c) Buffer overflow shown in gray.

[Tane 01]

Virus

- n **Upotettu ”kohdetiedostoon” (Troijan hevonen)**
 - u peli, työkalu, kuva, artikkeli
 - u **dropper** – viruksen upotustyökalu
 - u kohdekäyttäjä kopioi sen itselleen
- n **Odottaa, kunnes kohdetiedosto aktivoidaan**
 - u käynnistyy aina tai joskus (looginen pommi)
- n **Saastuta kone pysyvämmiin**
 - u upota virus muihin tiedostoihin
- n **Suorita payload**
 - u harmiton viesti
 - u tuhoisa toiminta (esim. tuhoa BIOS)

Viruksen elinkaari

- n **Lepovaihe (dormant)**
 - u se vaan olla möllöttää
 - u katselee almanakkaa, tarkkailee levyn täyttöastetta...
- n **Lisääntymisvaihe (propagation)**
 - u kloonautuu muihin ohjelmiin ja tietyille levyalueille
- n **Laukaisuvaihe (triggering)**
 - u herkistyy toimimaan
 - u almanakka oikealla sivulla, kopioitunut riittävän monta kertaa, tms.
- n **Suoritusvaihe (execution)**
 - u tekee ilkeämieliset tempunsa

Mato

- n **Käyttää verkkoa levitäkseen koneesta toiseen**
 - u leviää itsestään ilman käyttäjän myötävaikutusta
 - u harmiton, tuhoisa tai tuottava payload
- n **Sähköposti**
 - u mato postittaa itseään osoitelistasta löytyville
 - u mato postittaa harkittua roskapostia osoitelistasta löytyville
 - ⌘ roskapostiin reagoidaan → **madon tekijä saa rahaa**
- n **Etäkomentojen suorittaminen**
 - u mato suorittaa itsensä löytämissään etäkoneissa
- n **Etäistuntojen hyödyntäminen**
 - u mato ottaa istunnon etäkoneeseen ja käyttää normaaleja komentoja leviämiseen
- n **Viisas mato ei leviä jo mahdolliseen koneeseen**
- n **Viisas mato piiloutuu normaalinnäköiseksi (nimiseksi) prosessiksi**

Zombie valloittaa koneen

- n **Asettuu uhriksi valittuihin koneisiin ja laukaisee sieltä käsin 'ikävät' toiminnot**
- n **Ei laukea polun alkupään koneissa**
 - u syntypaikan jäljittäminen vaikeaa
- n **Kun laukeaa, monistuu eksponentiaalisesti**
 - u valloittaa CPU-kapasiteetin
 - u täyttää muistin
 - u täyttää levytilan
- n **Distributed DoS – Distributed Denial of Service**
 - u zombiet pommittavat uhria esim. SYN-sanomilla
 - ⌘ kolmivaiheinen kättely pulmallinen
 - u saturoi web-palvelimen tuhansilta koneilta

Virustyyppejä

- n **Loinen (parasitic)**
 - u kun saastunut ohjelma ajetaan, tutkii levyn ja tarttuu muihin ohjelmiin
- n **Muistiresidentti**
 - u hengailee keskusmuistissa muistiresidentin ohjelman osana
 - F ei löydy levyskannauksella
 - u tarttuu kaikkiin suoritettaviin ohjelmiin
- n **Käynnistyslohkovirus (boot sector)**
 - u tarttuu järjestelmän käynnistyslohkoon
 - u pääsee muistiin heti, kun järjestelmä käynnistetään

Virustyyppejä

- n **Stealth, ”salamyhkäinen”**
 - u yrittää piiloutua virustorjuntaohjelmilta
 - F saastunut ohjelman ei näytä muuttuneen
 - F sieppaa esim. levypyynnön ja näyttää epäilijälle alkuperäisen tiedoston
- n **Polymorfinen** Fig 9-17 [Tane 01]
 - u yrittää piiloutua virustorjuntaohjelmilta
 - F muuttaa itseään jokaisella käynnistyskerralla
 - F salakirjoittaa / purkaa itseään eri avaimin
 - u muuttunut virus toiminnaltaan aiemman kaltainen, mutta bittikuviot (sormenjäljet) erilaisia
 - u mutation engine sober.f click

MOV A,R1	MOV A,R1	MOV A,R1	MOV A,R1	MOV A,R1
ADD B,R1	NOP	ADD #0,R1	OR R1,R1	TST R1
ADD C,R1	ADD B,R1	ADD B,R1	ADD B,R1	ADD C,R1
SUB #4,R1	NOP	OR R1,R1	MOV R1,R5	MOV R1,R5
MOV R1,X	ADD C,R1	ADD C,R1	ADD C,R1	ADD B,R1
	NOP	SHL #0,R1	SHL R1,0	CMP R2,R5
	SUB #4,R1	SUB #4,R1	SUB #4,R1	SUB #4,R1
	NOP	JMP .+1	ADD R5,R5	JMP .+1
	MOV R1,X	MOV R1,X	MOV R1,X	MOV R1,X
			MOV R5,Y	MOV R5,Y
(a)	(b)	(c)	(d)	(e)

Fig. 9-17. Examples of a polymorphic virus.

[Tane 01]

Virustyyppejä

[LoveLetter](#) [click](#)

n Makrovirukset

- u MS-Word ja MS-Excel suorittavat makrokomentoja käynnistyessään (oletus)
 - F automaattisen toiminnon voi kääntää pois
- u sotkevat / hävittävät dokumentteja
- u kopioituvat dokumentteihin
- u leviää helposti lähettämällä asiakirja sähköpostitse
 - F "I love you" viidessä tunnissa maailman ympäri
 - F ["Slammer" mato löysi lähes kaikki haavoittuvat koneet maailmalla 10 minuutissa (25.1.2003)]
- u vuosi 2001 ennätysellisen vilkas virusvuosi
 - F n. 100 tartuntaa 1000 tietokonetta kohden

F-Secure 2005: "Vuoden toisella puoliskolla virusten määrän kasvu jatkui hälyttävällä tahdilla. Määrä nousi vuoden loppuun mennessä ennennäkemättömälle tasolle, 110.000 viruksesta 150.000 virukseen."

[F-Secure 2005](#) [click](#)

Käyttöjärjestelmät II

Tunkeutujat

Tunkeutujat (intruders)

n Kasvava ongelma

- u vieraan tunnuksen käyttö masquerader
- u oman tunnuksen väärinkäyttö misfeasor
- u salattu käyttö clandestine user
 - F hommaa root-oikeudet, piilota jäljet

n Asiakas/palvelija ympäristö

- u ei enää keskuskoneympäristössä
- u verkon kautta tulevat yhteydenotot

n Krakkerit saavat oppia ja välineitä muilta

- u se verkko...

Miten sisään yritetään?

- n **Arvaa / kokeile salasanoja**
 - u standarditunnuksia + oletussalasana / ei salasanaa
 - u järjestelmällisesti lyhyitä salasanoja
 - u käytä apuna järjestelmän sanastoa tai jotain muuta valmista "top100"-listaa
 - u käytä käyttäjään liittyviä tietoja
 - ⊞ puh., nimet, seinällä olevat sanat, ...
- n **Käytä Troijan hevosta**
 - u hyötyohjelma, joka myös kokoaa käyttäjätietoa
- n **Salakuuntele verkkoa**
 - u tunnus/salasana voi olla selväkielisenä

Identiteetin kalastelu (phishing)

- n **Identiteettivarkaus**
- n **Huijaus**
 - u ei virus, ei mato
- n **Uskottava väärennetty sähköposti**
 - u sisältää linkin väärennetylle kotisivulle
 - u käyttäjä validoi itsensä ja "päivittää" tietonsa
 - u validointitietojen avulla hyökkääjällä käyttäjän identiteettitiedot, tunnukset, salasanat, jne

Phishing [click](#)

Käyttöjärjestelmät II

Suojautuminen (protection)

eli

Miten uhkia torjutaan?

Suojaustasoja

- n **Ei suojausta, mutta**
 - u haavoittuvat prosessit ajetaan erillään muista
- n **Eristäminen**
 - u kukin prosessi toimii itsenäisesti
 - u ei yhteiskäyttöä tai kommunikointia muiden kanssa
- n **Kaikki tai ei mitään julkiseksi**
 - u omistaja antaa resurssin julkiseen jakeluun tai pitää yksityisenä
- n **Rajoitettu (kiinteä) yhteiskäyttö**
 - u käyttöoikeus tietyillä käyttäjillä tiettyihin resursseihin
 - u KJ tarkistaa käyttöoikeuden resurssia käytettäessä
 - F ainakin silloin, kun käyttö alkaa

Suojaustasoja (jatkuu)

- n **Dynaaminen käyttöoikeuksien hallinta**
 - u (omistaja) voi muuttaa
- n **Käyttöoikeuksien/tavan rajoittaminen**
 - u käyttöoikeuden lisäksi voidaan määritellä myös käyttötapa
 - F esim. käyttäjä saa tilastollisia tunnuslukuja, mutta ei näe yksittäisiä arvoja
 - F tilastolliset tunnusluvut saa vain jos
 - populaatio > 3?
 - populaatio > 10?
 - populaatio > 100?

Muistinsuojaus

- n **Moniajojärjestelmä**
 - u muistissa useiden käyttäjien prosesseja
 - u saavat viitata vain hallitusti muistiin
 - F eivät saa luvatta viitata toisten data-alueelle
 - F eivät saa vaihtaa toisten funktioita toisiksi
- n **Toteutus: virtuaalimuisti**
 - u osittain laitteistolla, osittain KJ:ssa
- n **Yhteiskäyttö**
 - u sivu/segmentti esiintyy useassa sivu/segmenttitaulussa
 - u toteutus helpompi segmentoinnissa
 - F oma segmentti yhteiskäyttöalueelle

Käyttäjän tunnistus

- n **Käyttöoikeus vain rekisteröidyillä käyttäjillä**
 - u käyttäjätunnus ja salasana
- n **Vieraille voi olla guest / visitor tunnuksia**
 - u rajoitetut oikeudet
- n **Rekisteröinnin jälkeen tunnus mukana käyttäjän prosessien PCB:ssä**
 - u oikeuksien tarkistaminen
 - u prosessien oikeudet perustuvat käyttäjän identiteettiin
 - F yleensä tämä ei riitä!

Käyttöoikeudet

- n **Kuka saa käyttää ja mitä?**
- n **Peruslähtökohta**
 - u käyttäjän tunnistus (**user**)
 - u toimialue (suojausympäristö, **domain**)
 - F mitä resursseja ja miten tähän suojausympäristöön kuuluva käyttäjä tai muu subjekti (**subject, principal**) saa käyttää
- n **Pääsymatriisi**
 - u rivi: toimialue (domain) Fig 16.5 (a) [Stal 05]
 - u sarake: resurssi, objekti (object)
 - u alkio: toimialueen subjektin käyttöoikeus resurssiin
 - F domain on myös objekti! Fig 9-24 [Tane 01]

		Object										
		File1	File2	File3	File4	File5	File6	Printer1	Plotter2	Domain1	Domain2	Domain3
Domain	1	Read	Read Write								Enter	
	2			Read	Read Write Execute	Read Write		Write				
	3						Read Write Execute	Write	Write			

Fig. 9-24. A protection matrix with domains as objects. [Tane 01]

Käyttöoikeudet

- n **Käyttöoikeudet käyttäjän yhteydessä (mitä käytetään?)**
 - u käyttäjäprofiili Fig 16.5 (c) [Stal 05]
 - u valtakirjalistat (capability lists), väärentämättömät
- n **Käyttöoikeudet kohteen yhteydessä (kuka käyttää?)**
 - u kohde: data, ohjelma Fig 16.5 (b) [Stal 05]
 - u pääsyylistat (ACL, access control list)
 - u yleisempi, helpompi toteuttaa
 - F tieto vain yhdessä kohdassa
- n **Molemmat**
 - u vain pääsymatriisiin ei-tyhjät alkiot
- n **KJ tarkistaa oikeudet käytön yhteydessä**
 - u esim. vertaa PCB:ssä olevaa uid+gid paria tiedoston attribuutteihin talletettuun uid+gid pariin

Käyttöoikeuspolitiikat

- n **DAC – discretionary access control** harkinnanvarainen
 - u tiedon omistaja päättää, kuka siihen pääsee käsiksi ja miten
 - u käyttäjä voi dynaamisesti muuttaa omistamiensa tietojen (tiedostojen) pääsyoikeuksia
 - F vaikutus alkaa ... milloin? poista lukuoikeus?
 - u normaali yksityiskäyttö
- n **MAC – mandatory access control** pakollinen
 - u keskitetty politiikka, joka oletusarvoisesti määrittelee kuka pääsee käsiksi mihin tietoon ja miten
 - u käyttäjä ei voi muuttaa pääsyoikeuksia
 - u luokitellun tiedon käyttöympäristöt

Hyvä salasana

- n **Koneen generoima**
 - u vaikeampi arvata
 - u vaikeampi muistaa → paperille?
- n **Käyttäjän valitsema**
 - u hylkää liian lyhyet ja helpohkosti arvattavat
 - u järjestelmä voi laajentaa, salaisella 'suolalla' Fig 16.6 [Stal 05]
 - F sama salasana ei näytä samanlaiselta kryptattuna
 - F salasana käytännössä pitenee
 - F brute-force hyökkäys hidastuu (suola salainen tai ainakin kaikilla erilainen)
- n **Järjestelmä yrittää itse aktiivisesti arvata salasanan**
 - u vaihdettava, jos osoittautui liian helpoksi
 - u hakkeri voi tehdä tätä kopioimallaan passwd-tiedostolla
 - F login-yritysten rajoittaminen ei hidasteena
 - F "suolaus" on hyvä hidaste
 - F passwd-tiedosto suojatulle muistialueelle olisi hyvä idea

Tunkeilijan huomaaminen

- n **Tunkeilijaa vaikeaa estää vaikeuttamatta samalla normaalia käyttöä**
- n **Tunnuksen käyttöprofiili muuttuu yllättäen**
 - u aamu-uninen Arskako töissä kello 5?
 - u eikö Villen pitäisi olla lomalla?
- n **Tilastollinen poikkeama**
 - u kerää perustietoa laillisten käyttäjien tyypillisestä kuormasta tietyn jakson ajan
 - u vertaa uutta jaksoa perusjaksoon
 - u mikä on normaalia? mikä poikkeavaa?
- n **Mitä on automatisoitavissa?**

Tunkeilijan huomaaminen

- n **Sääntöpohjainen eksperttijärjestelmä**
 - u perussäännöstö normaalille käytölle
 - F eri yrityksissä/kulttuureissa erilaista
 - u mikä on normaalia? mikä poikkeavaa?
- n **KJ tarjoaa perusvälineet**
 - u kirjaa tietoa käyttäjän login-ajosta, CPU-ajasta jne.
 - u loki- ja historiatiedostot
- n **Omat räätälöinnit parempia**
 - u tunkeilija tuntee perus-KJ:n
- n **Erillinen audit-järjestelmä**
 - u kerää tunkeilijan huomaamisessa tarvittavaa tietoa
- n **Ansät**
 - u *user* guest, *password* guest → login OK, soita poliisille
- n **Kuka on tunkeilija? Kuka tuntee nykyisen lain?**

Käyttöjärjestelmät II

Virustorjunta

Virustorjunta

- n **Havaitse - tunnista**
 - u virustorjuntaohjelmalla
 - u vertaile ohjelmien pituuksia ja tarkistussummia
 - u etsi viruksen sormenjäljet
 - u muistiresidentti virusskanneri huomaa, kun virus yrittää tehdä työtänsä
- n **Hävitä**
 - u käynnistä järjestelmä puhtaalta kirjoitussuojatulta levykkeeltä / CD:ltä (vältä käynnistyslohkovirukset)
 - u aja virustorjuntaohjelma
 - F ajantasainen virustietokanta – ikä max 2 tuntia?
 - u joskus ohjelmia asennettava uudestaan

Generic Decryption Scanner

- n **Polymorfiset virusten etsintään**
- n **Tutki ohjelma ensin GD-skannerilla**
 - u CPU-emulaattori
 - u viruksien "sormenjälkien" tunnistin
 - u ohjausmoduuli
- n **Emulaattori tulkitsee ohjelmaa käsky kerrallaan**
- n **"Sormenjälkitunnistus" selaa koodin aika-ajoin**
 - u jos virus löytyy, ei koodia päästetä todelliseen suoritukseen
- n **Ongelma:**
 - u kauanko ajettava, ennen kuin virus purettu?
 - u ei saa hidastaa tarpeettomasti ohjelmien käynnistystä

Digital Immune System (IBM)

Fig 16.9 [Stal 05]

- n **Kussakin koneessa 'viritelty' virustorjunta**
 - u tunnetut: normaali virustorjunta
 - u uudet: etsi epäilyttäviä piirteitä (heuristiikka)
- n **Lähetä epäilyttävät ohjelmat tarkemmin tutkittavaksi immuuniin koneeseen**
 - u emulointi, monitorointi
 - u jos virus, kirjaa sormenjäljet, kehitä lääkkeet
- n **Tunnisteet ja lääkkeet automaattisesti muille koneille**
 - u nopeammin kuin virus itse leviäisi

Firewalls

(palomuri)

n Packet-filtering firewall

(pakettifiltteri)

- u look at packet header info
- u accept/reject packet based on rules
 - F accept from this domain, reject for know bad guy

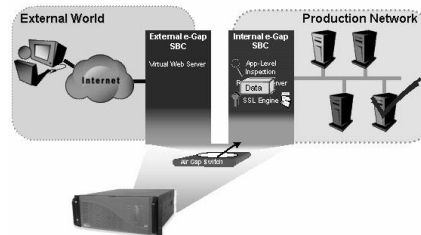
n Application-level gateway

(sovellustason yhdyskäytävä)

- u look at data in packet
- u scan for viruses, etc

n Air-gap technology (ilmarako)

- u create "empty space" firewall
- u two servers, memory bank in middle
 - F memory bank has no OS,
 - F memory bank connected to max one server at a time
- u E.g., e-Gap Systems (Whale Communications)



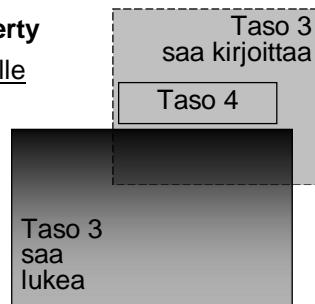
<http://www.whalecommunications.com>

Käyttöjärjestelmät II

Luotettu järjestelmä (trusted system)

Multilevel Security

- n **Tieto luokitellaan tärkeyden mukaan**
 - u unclassified, confidential, secret, top secret
- n **Käyttäjälle määritelty 'luottamustaso'**
- n **No-read-up eli simple security property**
 - u kukin saa nähdä vain omalle tai sen alapuoliselle tasolle luokiteltua tietoa
- n **No-write-down eli *-property eli star-property**
 - u tietoa saa tuottaa vain omalle tai ylemmälle tasolle
 - u tietoa saa 'vuotaa' alemmille tasoille vain, jos siihen on saatu erikseen lupa
- n **Esimerkki MAC-suojauksesta**
 - u Mandatory Access Control



Reference Monitor

Fig 16.10 [Stal 05]

- n **Säätää/laillistaa käyttäjien (subject) pääsyä kohteisiin (object) kumpiinkin liitettyjen attribuuttien mukaisesti**
- n **Security kernel database**
 - u käyttäjien pääsyoikeudet, liikkumavara
 - u kohteiden käyttöoikeudet, luokittelutasot
- n **Pakottaa noudattamaan säännöstöä**
 - u MAC: no-read-up, no-write-down
- n **Toteutus laitteistossa ja KJ:ssa**
 - u pelkkä ohjelmallinen toteutus liian hidasta
 - u "viittausvalvoja", tarkkain (reference monitor)
 - F jatkuvaan seurantaan tarkoitettu laite

Reference Monitor -politiikka

n Ominaisuudet

- u täydellinen sääntöjen noudattaminen (**mediation**)
 - F säännöt tarkistetaan jokaisella viitteellä, ei pelkästään esim. tiedostoa avattaessa
- u eristäminen (**isolation**)
 - F sekä monitor että tietokanta suojattu täysin luvattomilta muuttajilta
- u verifioitavuus (**verifiability**)
 - F monitorin **oikeellisuus pitää pystyä osoittamaan** matemaattisesti

n Jos verifioitavissa, sallitaan käyttää termiä luotettu järjestelmä (trusted system)

- u aika paljon vaadittu ...

Reference Monitor

n Audit-file

- u tärkeät tietoturvaan liittyvät tapahtumat rekisteröidään
 - F muutokset tietokantaan eli oikeuksiin
 - F login ja logout -tapahtumat
 - F tietoturvan rikkomisyrietykset

n Tutkittavissa jälkikäteen

- u jos rikosta ei voi estää, niin toivottavasti ...
 - F se voidaan edes myöhemmin havaita ja
 - F pahatekijä saadaan kiinni
 - kiinnijäämisen pelko on viisauden alku

Audit: tarkastus, arviointi, tilintarkastus

Esimerkki

n **Troijan hevonen ja normaalit käyttöoikeudet**

- u Alice vokottelee Bobin ajamaan ohjelmansa
 - F lukee Bobin yksityistä tietoa [Fig 16.11 (a, b) [Stal 05]]
 - F luo tiedoston, jonka Alice voi lukea, mutta Bob ei

n **Troijan hevonen ja luotettu järjestelmä**

- u Tasot: arkaluonteinen (harmaa), julkinen (valkea)
- u Bob tasolla, jolla oikeus arkaluonteiseen tietoon
- u Alice tasolla julkinen [Fig 16.11 (c, d) [Stal 05]]
- u Kun Bob suorittaa Alicen ohjelman, se ei voi kirjoittaa Bobin tasoa alemmalle tasolle (*-property)

Æ **suojaustaso tässä tärkeämpi kuin käyttöoikeudet !**

OpenBSD

(www.openbsd.org)

n **Unix project to create most secure UNIX**

- u try to be the #1 most secure operating system

n **Default setup**

- u very secure system
- u proactive security, integrated cryptography
- u every source file analyzed by core team
- u continuous development
- u no break in
- u have almost no external communications at all

n **Enable better, user-friendly communication**

- u not so easy, need good understanding of system
- u what if maintenance by inexperienced administrators?

Kertauskysymyksiä

- n **Miten tiedostojen käyttöoikeudet tavallisimmin määritellään?**
- n **Miten ja milloin oikeudet tarkistetaan?**
- n **Miten valtakirjat ja pääsyylistat eroavat toisistaan?**
- n **Reference Monitorin idea**