


LUENTO 21

Tietoturva

Ch 16 [Stal 05]

1



Suojaus (security)

- Salakirjoitus App 16A [Stal 05]
- Uhat Ch 16 [Stal 05]
 - turvallisuusuhat
 - pahantahtoiset ohjelmat
 - tunkeutujat
- Suojaus
 - suojausympäristöt
 - virustorjunta
 - luotettu järjestelmä

2

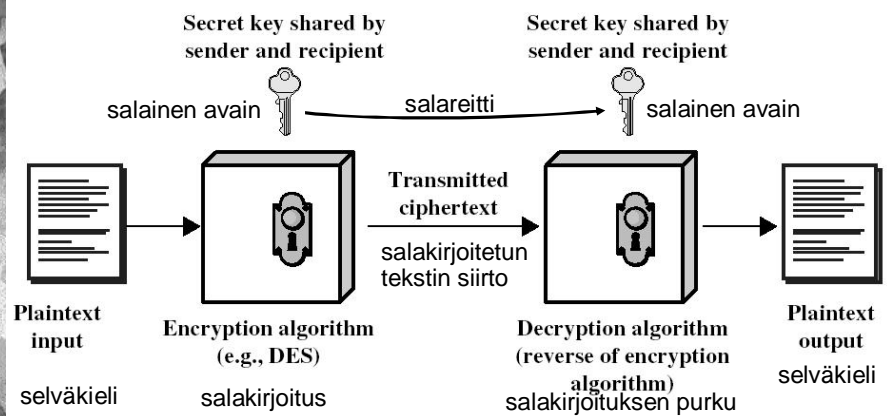
Salakirjoitus

Appendix 16A [Stal 05]

3

Perinteinen, symmetrinen salaus

Sama avain molemmilla!



(Fig 16.14 [Stal 05])

4

DES: Data Encryption Standard

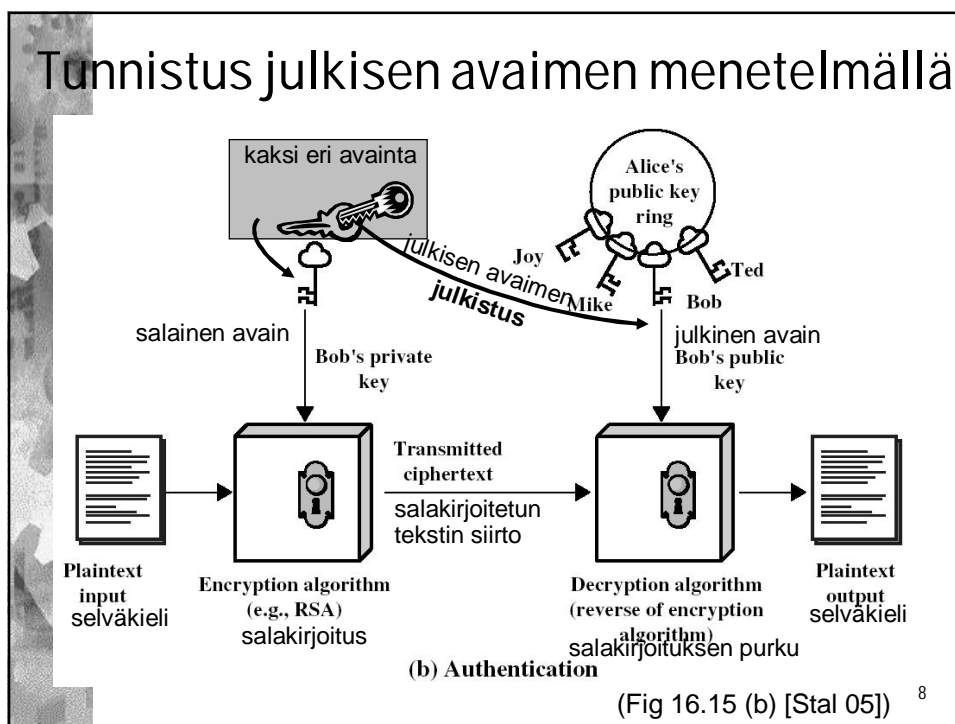
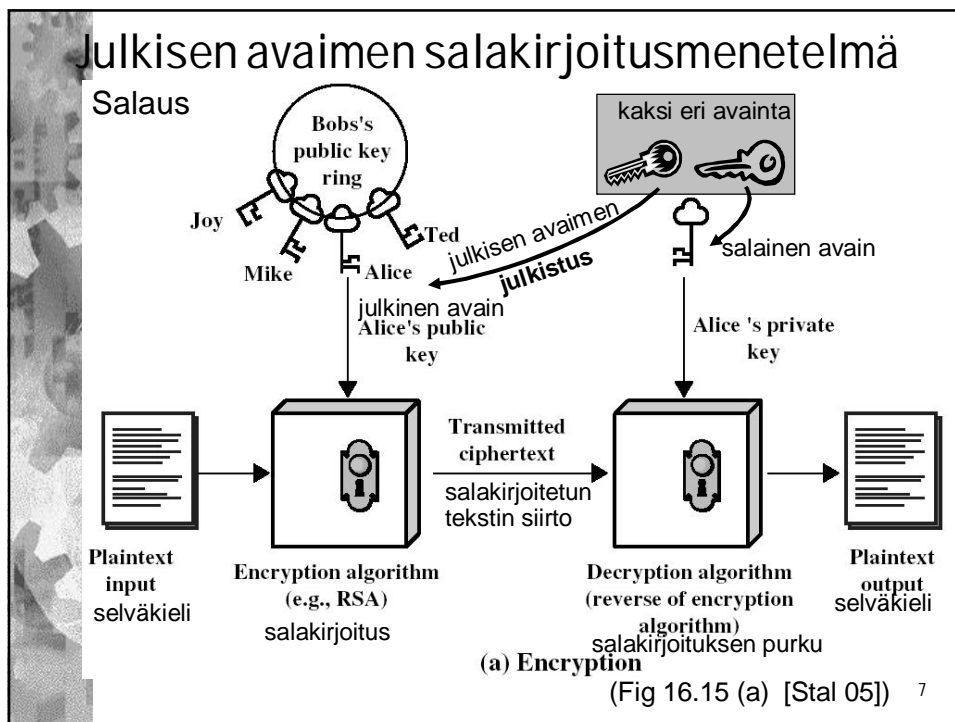
- Symmetrinen: sama avain molemmissa
 - perustuu Lucifer algoritmiin (Horst Feistel, IBM), 1977
- Avain 56 bittiä (plus 8 pariteettibittiä)
 - salaus 64 bitin lohkoissa
- Iteroi lohkolle 16 kertaa bittiopeatioita
 - eri kierroksella alkuperäisen avaimen eri 48 bittiä avaimena
 - kierrosten välillä
 -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

5

AES – Advanced Encryption Standard

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

6



Julkisen avaimen salakirjoitus

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

9

Turvallisuusuhat

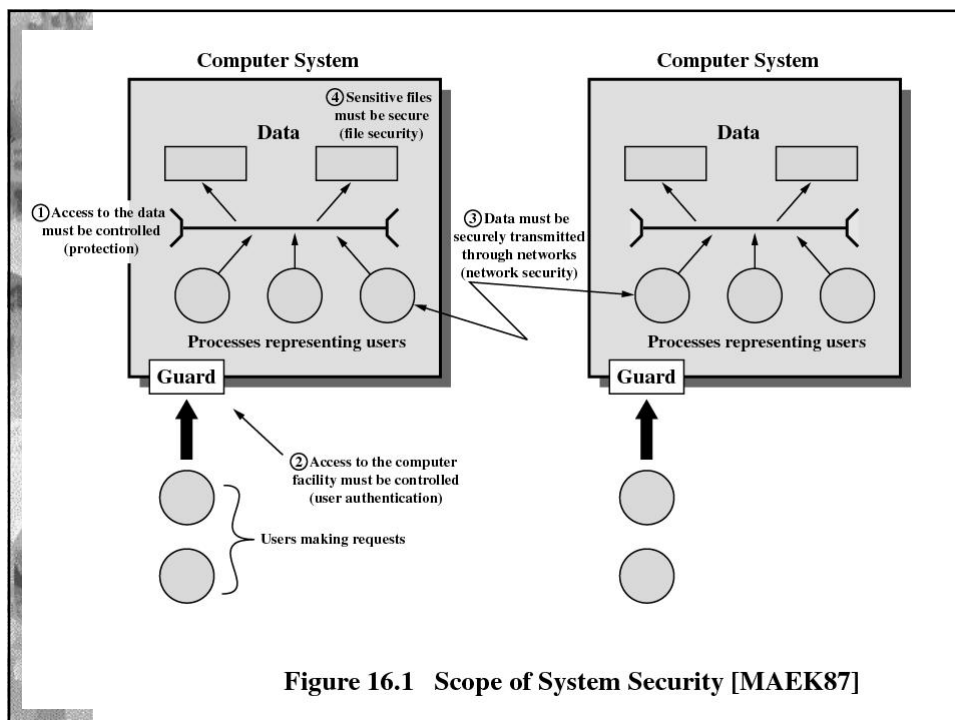
10

Turvallisuustarpeet

Fig 16.1 [Stal 05]

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

11



Turvallisuusvaatimuksia

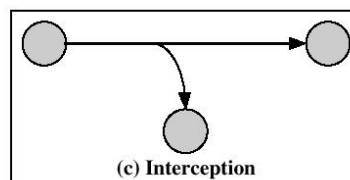
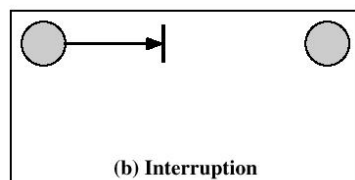
- Luottamuksellisuus (confidentiality, secrecy)
 - tietoa saa lukea vain ne, joilla siihen lupa
 - ei välttämättä tietoa edes tiedon olemassaolosta
- Eheys, koskemattomuus (integrity)
 - tietoa saa tuottaa/muuttaa vain ne, joilla siihen lupa
- Käytettävyys / Saatavuus (availability)
 - tieto oltava saatavilla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

13

Uhkia

DoS – denial of service

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



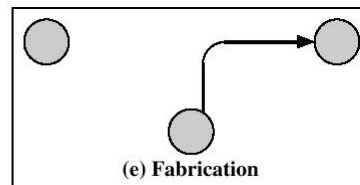
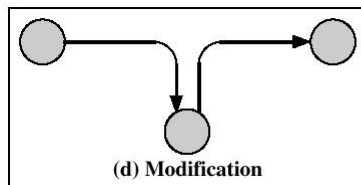
(Fig 16.2 [Stal 05])

- Sieppaus (interception)
 - luottamuksellisen liikenteen salakuuntelu
 - kopiointi

14

Uhkia

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



- Valmistus, "satuilu" (fabrication) (Fig 16.2 [Stal 05])
 - järjestelmän tietojen muuttaminen, jotta saadaan haluttu (luvaton) toiminta
 - esim. tekaistut tietueet, tunnukset, sanomat

15

Suojattavaa ja uhkia

Tbl 16.1 [Stal 05]

- Laitteisto
 - haavoittuvin osa tietokonejärjestelmää
 - saatavuus, luottamuksellisuus, eheys, oikeaksi todentaminen
 - vaikea käyttää automaattisia turvajärjestelyjä
 - lukitut konehuoneet, piilotetut kaapelitot
 - pääsynvalvonta
- Ohjelmisto
 - haavoitettavana saatavuus: tuhottu, muutettu
 - tietoturva ylläpitohenkilökunnan vastuulla
 - osa automatisoitavissa
 - varmuuskopiot
 - tarkistussummat

16

Suojattavaa ja uhkia

Tbl 16.1 [Stal 05]

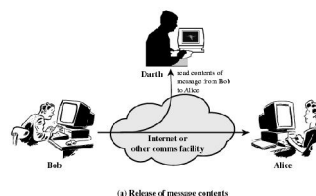
- Data
 - haavoitettavana
 - saatavuus
 - luottamuksellisuus
 - eheys
 - ylläpito käyttäjien vastuulla
 - oltava käyttöoikeuksia
 - tärkeä tieto voi olla analysoitavissa muita tietoja yhdistelemällä, vaikkei itse tietoon pääse suoraan käsiksi

17

Passiiviset hyökkäykset (kuuntelu, nuuskinta)

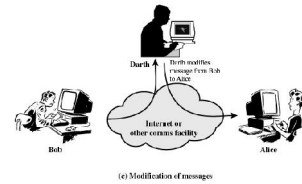
Fig 16.3 [Stal 05]

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



18

Aktiiviset hyökkäykset



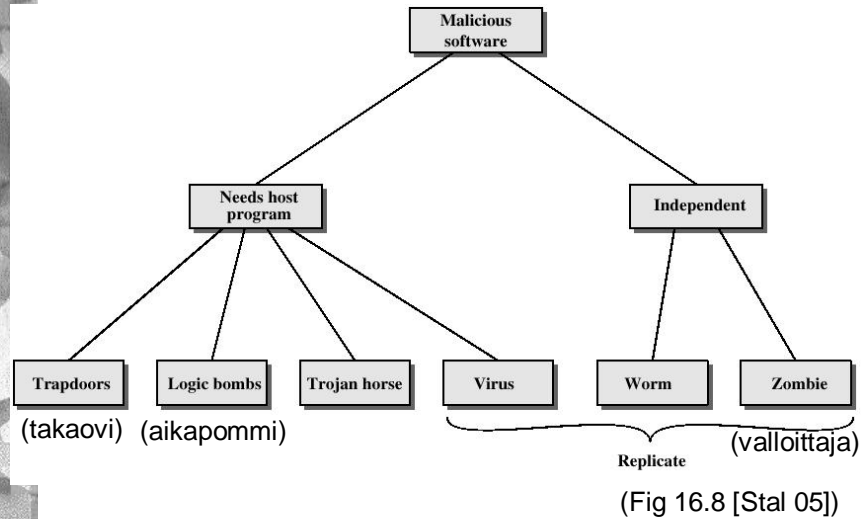
- Tiedon eheys rikkoontuu
- Tietoliikenneyhteydet, -verkko
 - lähettäjä teeskentelee olevansa joku muu (masquerade) **Fig 16.4 (a) [Stal 05]**
 - virheellinen toisto (replay) **Fig 16.4 (b) [Stal 05]**
 - viivyttäminen, muuttaminen, uudelleenjärjestely (modification of msg contents) **Fig 16.4 (c) [Stal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

19

Haittaohjelmat (Malicious software)

20

Luokittelua



21

Takaovi (salaovi, trap door)

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

Fig 9-10 [Tane 01]

22

```

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]

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

23

Looginen pommi (aikapommi, logic bomb)

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

24

Troijan hevonen

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

Fig 9-9 [Tane 01]

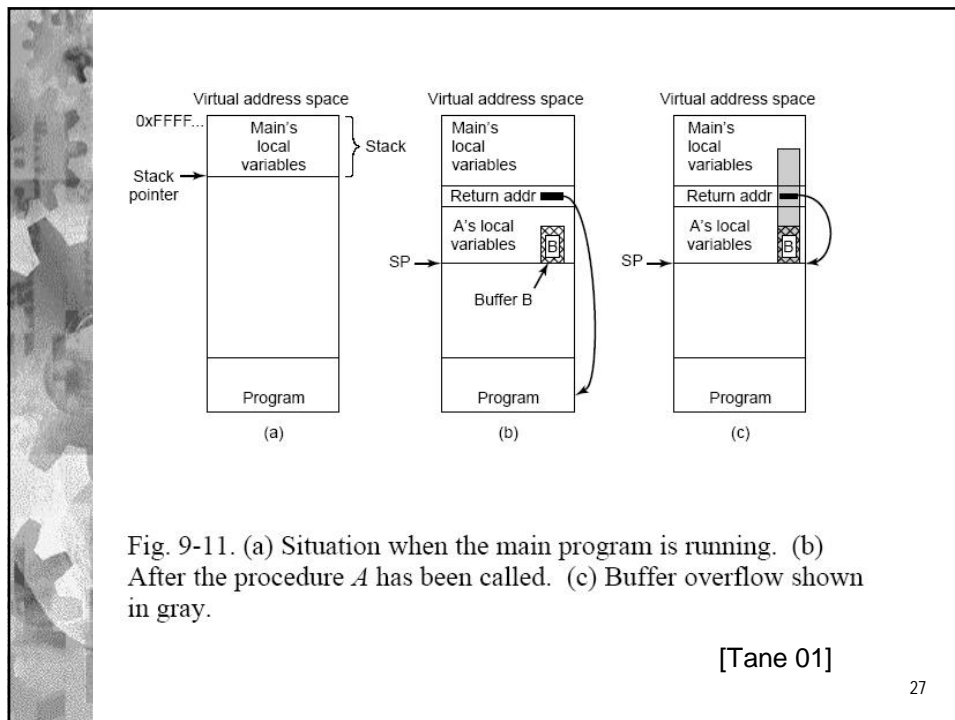
25

Puskurin ylivuoto (buffer overflow)

- Koodissa vakiopituinen taulukko
- Indeksä tai merkkijonon pituutta ei tarkisteta
- Talletus muuttaa tietoa muualla
 - esim. aliohjelmasta paluuosoite
- Perinteinen hyökkäysreitti
- Huonosti tehty ohjelma

Fig 9-11 [Tane 01]

26



27

Virus

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

28

Viruksen elinkaari

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

29

Mato

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

30

Zombie valloittaa koneen

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

31

Virustyypppejä

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

32

Virustyyppejä

- Stealth, "salamyhkäinen"
 - yrittää piiloutua virustorjuntaohjelmilta
 - saastunut ohjelman ei näytä muuttuneen
 - sieppaa esim. levytyynnön ja näyttää epäilijälle alkuperäisen tiedoston
- Polymorfinen
 - yrittää piiloutua virustorjuntaohjelmilta
 - muuttaa itseään jokaisella käynnistyskerralla
 - salakirjoittaa / purkaa itseään eri avaimin
 - muuttunut virus toiminnaltaan aiemman kaltainen, mutta bittikuviot (sormenjäljet) erilaisia
 - mutation engine

Fig 9-17 [Tane 01]

sober.f

33

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]

34

Virustyyppejä

LoveLetter

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

35

Tunkeutujat

36

Tunkeutujat (intruders)

- Kasvava ongelma
 - vieraan tunnuksen käyttö **masquerader**
 - oman tunnuksen väärinkäyttö **misfeasor**
 - salattu käyttö **clandestine user**
 - hommaa root-oikeudet, piilota jäljet
- Asiakas/palvelija ympäristö
 - ei enää keskuskoneympäristössä
 - verkon kautta tulevat yhteydenotot
- Krakkerit saavat oppia ja välineitä muilta
 - se verkko...

37

Miten sisään yritetään?

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

38

Identiteetin kalastelu (phishing)

- Identiteettivarkaus
- Huijaus
 - ei virus, ei mato
 - käyttäjää höynäytetään antamaan omat tiedot huijarille
- Uskottava väärennetty sähköposti
 - sisältää linkin väärennetylle kotisivulle
 - käyttäjä validoi itsensä ja "päivittää" tietonsa
 - validointitietojen avulla hyökkääjällä käyttäjän identiteettitiedot, tunnukset, salasanat, jne

Phishing filter – Tietokalastelun torjuntasuodatin (Microsoft IE:n termistöä)

39

Virustorjunta

40

Virustorjunta

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

41

Generic Decryption Scanner

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

42

Digital Immune System (IBM)

Fig 16.9 [Stal 05]

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

43

Digital Immune System

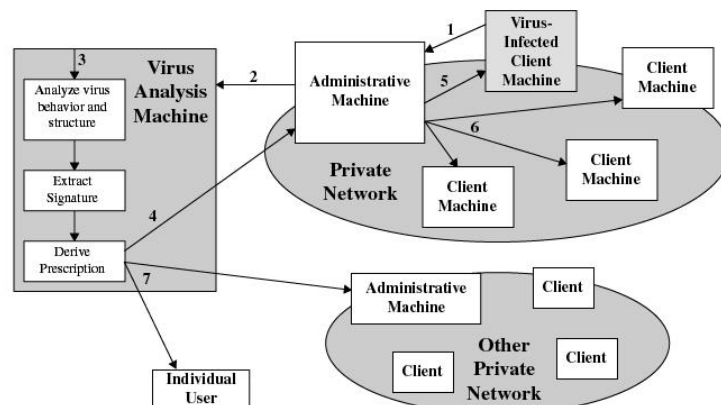


Figure 16.9 Digital Immune System

44