

Unix-käyttöjärjestelmien tietoturva ja OpenBSD

Arto Jonsson

Marraskuu 2012

<http://iki.fi/artoj>

Luentojen sisältö

1. Kolme poimintaa tietoturvasta
2. Tietoturva yleisesti
3. OpenBSD
4. Ohjelmointirajapintojen väärinkäyttö
5. Etuoikeuksien peruuttaminen ja erottaminen

Kolme poimintaa tietoturvasta: Medtronic

- ▶ McAfeen tutkijat löysivät Medtronic-yhtiön insuliinipumpuista haavoittuvuuteen, jonka avulla hyökkääjän on mahdollista hallita laitetta
- ▶ Hyökkäys voidaan tehdä etänä useiden kymmenien metrien päästä
- ▶ <http://www.reuters.com/article/2011/10/26/us-medtronic-idUSTRE79P52620111026>

Kolme poimintaa tietoturvasta: Ammattirikolliset

- ▶ Haittaohjelmien kehittäminen ja palvelunestohyökkäysien tekeminen on nykyään bisnestä, jota harjoittavat ammattirikolliset.
- ▶ Esimerkkejä artikkelista: palvelunestohyökkäys päiväksi 30-70 dollaria, miljoonan roskapostin lähetys 10 dollaria
- ▶ <http://arstechnica.com/tech-policy/2012/11/the-russian-underground-economy-has-democratized-cybercrime/>

Kolme poimintaa tietoturvasta: Stuxnet

- ▶ Stuxnet on erittäin monimutkainen haittaohjelma, joka löydettiin vuonna 2010 Iranista.
- ▶ Stuxnet hyökkää Siemensin tuotanto-ohjelmistoja ja laitteistoja vastaan.
- ▶ Stuxnet käyttää hyväkseen useita käyttöjärjestelmässä olevia tietoturva-aukkoja. Lisäksi osa sen ohjelmakoodista on allekirjoitettu varastetulla sertifikaatilla.
- ▶ <http://arstechnica.com/security/2012/06/why-antivirus-companies-like-mine-failed-to-catch-flame-and-stuxnet/>

Tietoturva yleisesti

- ▶ Ohjelmistoja ja käyttöjärjestelmiä on kaikkialla: matkapuhelimet, televisiot, autot, pelikonsolit, sydäntahdistimet, . . .
- ▶ Ohjelmistot ovat huomattavasti monimutkaisempia kuin ennen (esim. web-selaimet)
- ▶ Tulevaisuudessa tulemme olemaan vielä riippuvaisempia ohjelmistoista ja käyttöjärjestelmistä

Tietoturvan kolme päätehtävää

1. Luottamuksellisuus (engl. *confidentiality*)
2. Eheys (engl. *integrity*)
3. Saatavuus (engl. *availability*)

Tietoturva vs. helppokäyttöisyys

- ▶ Tietoturva ja helppokäyttöisyys ovat jatkuvassa tasapainossa
- ▶ Ei riitä, että tietoturvaominaisuudet ovat käytössä niiden on oltava myös helppokäyttöisiä (“Haluatko varmasti jatkaa?”-ponnahdusikkunat)
- ▶ Tietojärjestelmän on oltava oletuksena turvallinen (engl. *secure by default*)

Haavoittuvuustilastoja

- ▶ 2001: 1677
- ▶ 2005: 4931
- ▶ 2009: 5732
- ▶ 2012: 4964

Lähteet: <http://cve.mitre.org/> ja
<http://web.nvd.nist.gov/view/vuln/statistics>

OpenBSD

- ▶ 4.4BSD:hen perustuva vapaan lähdekoodin Unixin kaltainen käyttöjärjestelmä
- ▶ Yksinkertaisuus, standardointi (ANSI, POSIX) ja siirrettävyys (eri laitteistoille)
- ▶ Ensimmäinen julkaisu lokakuussa 1996
- ▶ Nykyään noin 100 enemmän ja vähemmän aktiivista kehittäjää

OpenBSD

- ▶ Osa OpenBSD:n ohjelmista julkaistaan erillisversioina muille käyttöjärjestelmille
- ▶ OpenSSH: etäkirjautumisohjelmisto
- ▶ OpenNTPD: kellonajan synkronointi
- ▶ Packet Filter (PF) palomuuriohjelmisto

OpenBSD

- ▶ Julkaisut vuosittain marraskuussa ja toukokuussa
- ▶ Uusin versio: 5.2 (marraskuu 2012)
- ▶ <http://www.openbsd.org/>

Ohjelmointirajapintojen väärinkäyttö

- ▶ Tietoturvaavaoittovuudet ovat usein yleisiä ohjelmointivirheitä
- ▶ Yleiset ohjelmointivirheet ovat taas ohjelmointirajapintojen väärinkäyttöjä
- ▶ Puutteellinen ohjeistus, huonot esimerkit, tietämättömyys, huolimattomuus...

C-ohjelmointikieli

- ▶ Dennis Ritchien 1970-luvun alussa kehittämä ohjelmointikieli
- ▶ Soveltuu erityisesti järjestelmäohjelmointiin matalan tason primitiiviensä vuoksi
- ▶ Lähes poikkeuksetta kaikki käyttöjärjestelmät on kehitetty C:llä
- ▶ C on standardoitu ohjelmointikieli (viimeisin vuodelta 2011), mutta standardi jättää asioita implementaation määriteltäviksi tai ei määrittele joitain ollenkaan.

Yksinkertainen C-esimerkki

```
#include <stdio.h>
int main(void)
{
    int    c, chars, tabs, bl, nl;
    chars = tabs = bl = nl = 0;

    while ((c = getchar()) != EOF) {
        chars++;
        if (c == '\t')
            tabs++;
        else if (c == ' ')
            bl++;
        else if (c == '\n')
            nl++;
    }
    printf("%d %d %d %d\n", chars, tabs, bl, nl);
}
```


Merkkijonot C-kielessä

- ▶ C-kielessä ei ole merkkijonotyyppiä vaan merkkijono esitetään taulukkona merkkejä, joka päättyy arvoon NULL
- ▶ Esimerkiksi merkkijonon pituus lasketaan kasvattamalla indeksinumeroa, kunnes käsiteltävä merkki on NULL

Esimerkki merkkijonosta "UTU":

U	T	U	\0
---	---	---	----

Merkkijonot C-kielessä

- ▶ Toisin kuin esim. Javassa C:ssä ei ole ennakkotarkastuksia taulukon (merkkijonon) indeksien oikeellisuudesta
- ▶ Indeksointiin liittyvät ongelmat yleisiä C-ohjelmien haavoittuvuuksissa
- ▶ Merkkijonojen käsittelyssä useita ongelmallisia rajapintoja mm. `strcat`, `strcpy`, `sprintf` ja `gets`

gets-funktio

```
#include <stdio.h>
int main(void)
{
    char buf[128];

    if (gets(buf) != NULL)
        printf("%s\n", buf);

    return 0;
}
```

OpenBSD:n C-kääntäjä varoittaa mm. `gets`-funktion käytöstä (mutta ei estä sitä).

Ohjelmointirajapintojen väärinkäyttö ja OpenBSD

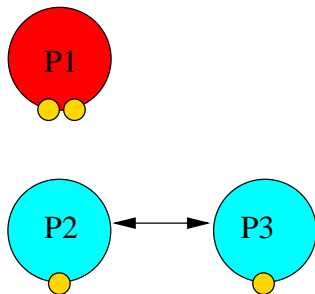
- ▶ Koodikatselmointi
- ▶ Kouluttaminen (<http://www.openbsd.org/papers/>)
- ▶ Uusien rajapintojen luonti (`strlcat`, `strlcpy`)
- ▶ Ohjeistus rajapintojen oikeasta käytöstä

Pienimmän oikeuden periaate

“Järjestelmän moduulilla tulee olla vain ne oikeudet, joilla se pystyy suoriutumaan sille määrätystä tehtävästä.”

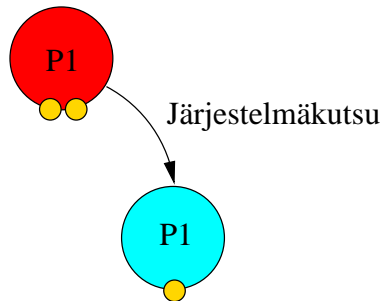
Oikeuksien erottaminen (privilege separation)

- ▶ Tarvittavat oikeudet jaetaan erillisiksi oikeuksia käyttäviksi prosesseiksi
- ▶ Prosessit kommunikoivat keskenään tarvittaessa



Oikeuksien peruuttaminen (privilege revocation)

- ▶ Prosessi luopuu oikeuksistaan kutsumalla järjestelmäkutsua



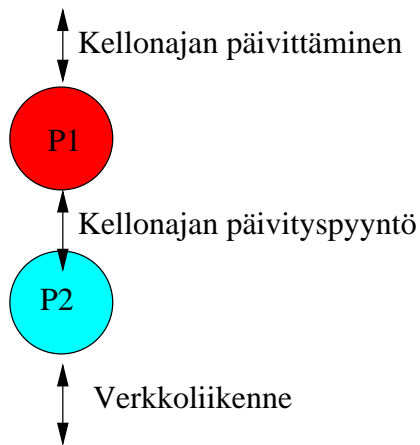
Esimerkki: openntpd

- ▶ NTP (network time protocol) on prototolla, jota käytetään synkronoimaan paikallinen kellonaika NTP serverin kellonaikaan (RFC 1305)
- ▶ openntpd on OpenBSD:n NTP toteutus
- ▶ Toteuttaa oikeuksien peruuttamisen ja erottamisen

openntpd:n rakenne

- ▶ openntpd:n toiminta on jaettu pääasiallisesti kahteen prosessiin
- ▶ Oikeuksia pitävä prosessi kutsuu järjestelmäkutsuja, joilla kelloa päivitetään
- ▶ Oikeudet peruuttava prosessi ylläpitää listaa NTP-servereistä ja käsittelee serverien lähettämät paketit

openttpd:n rakenne



openntpd:n toiminta

1. Käynnistyessään openntpd:llä on pääkäyttäjän oikeudet (vaatimus).
2. Käynnistyvä prosessi luo uuden prosessin, joka vaihtaa juurihakemiston `/var/empty`-hakemistoon ja peruuttaa omat oikeutensa
3. Prosessien välille luodaan viestiyhteys
4. Pääkäyttäjän oikeuksilla toimiva prosessi jää odottamaan palvelupyynnöjä oikeuksien peruuttaneelta prosessilta
5. Oikeudet peruuttanut prosessi aloittaa keskustelun NTP-serverien kanssa ja tekee palvelupyynnön toiselle prosessille, kun kellonaikaa pitää päivittää.

Lähteet

1. McGraw, G., *Software Security: Building Security In*, 2006
2. Brauer, H., Dehmlow, S., *Puffy At Work - getting code right and secure, The OpenBSD way*,
<http://bulabula.org/papers/2010/bsdcan/>, haettu 2012-11-24
3. Herrb, M., *Security measures in OpenBSD*,
<http://homepages.laas.fr/matthieu/talks/openbsd-h2k9.pdf>,
haettu 2012-11-24
4. OpenBSD:n manuaalisivut,
<http://www.openbsd.org/cgi-bin/man.cgi>