

Turvallinen ohjelmointi

*FT Marko Helenius,
yliopisto-opettaja*

*Tampereen teknillinen yliopisto,
Tietotekniikka, NISEC-ryhmä*

*<http://www.cs.tut.fi/~heleniu3/>,
e-mail: marko.t.helenius@tut.fi*

BLENDED ATTACKS EXPLOITS, VULNERABILITIES AND BUFFER-OVERFLOW TECHNIQUES IN COMPUTER VIRUSES

- ◆ Ensimmäinen hyökkäys 1988: Internet Worm (artikkelissa Morris Worm)
- ◆ Järjestelmät kuormittuivat madon vuoksi

Joitakin termejä

◆ Pino (stack tai call stack)

- LIFO (Last In First Out)
- Pinon kehys laitetaan pohjalle ja sisältää mm.
 - ❖ paluuosoitteen, parametrit ja paikalliset muuttujat
- IP = Instruction pointer, käytetään myös EIP, seuraavaksi suoritettavan käskyn osoite
- EBP = Base Pointer, Osoittaa oletuspinoon kehyksen loppuun. Käytetään paikallisten muuttujien käsittelyyn.
- ESP = Stack Pointer, Osoittaa oletuspinoon kehyksen alkuun. Käytetään paikallisten muuttujien käsittelyyn.

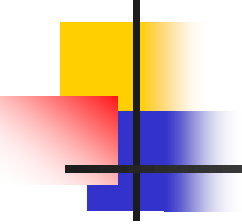
◆ Heap-muisti (kasa)

- dynaamisesti varattavalle muistille varattu muistialue
- esim. malloc, free, new, delete
- normaalisti järjestelmä huolehtii automaattisesti heap-muistille varatusta tilasta

Puskuriylivuodot

◆ Kolme sukupolvea:

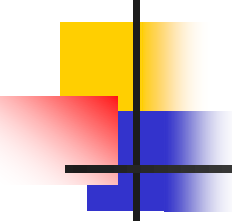
- 1. pino
- 2. kasamuisti, funktioiden (metodien) osoittimet ja yhden tavun haavoittuvuus (off-by-one exploit)
- 3. merkkijonojen muotoilu ja kasan rakenne



Turvallinen ohjelmointi

Puolesta?

- Parantaa tietoturvallisuutta
- Työntekijät saa parempaa palkkaa
- Mato voi saastuttaa ja aiheuttaa kustannuksia
- Palvelusta saadaan vakaampi, kun ei ole virheitä
- Ohjelmoijien taidot paranevat
- Tietyillä sovellusalueilla virheet maksavat liikaa (esim. terveys ja rahan käsittely)
- Koodari ei tarvitse omaa asuntoa, voi asua työpaikalla
- Koodari voi tykätä siitä, että tekee asioita oikein
- Saadaan säästöjä siitä, että päästään virheisiin kiinni nopeammin
- Asiakastyytyväisyys



Turvallinen ohjelmointi

Vastaan?

- Asiakkaat ei maksa
- Asiakkaan ongelma
- Asiakkailta saadaan rahaa ohjelman virheistä ja lisätyöstä
- Virheitä voidaan myydä vihamielisille osapuolille
- Ajan hukkaa, projekti viivästyy
- Työkalut hoitaa meidän tietoturvan, ei ohjelmoijan tarvitse välittää
- Ohjelmasta tulee hitaampi, kun siihen lisätään tietoturvaa
- Ei niitä aukkoja kukaan löydä
- Voidaan palkata halvempia ohjelmoijia
- Pitää olla virustorjulle ja palomuurintekijöillekin hommia