Turvallinen ohjelmointi

FT Marko Helenius,

yliopisto-opettaja

Tampereen yliopisto,

Tietotekniikka, NISEC-ryhmä

marko.helenius@tuni.fi

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

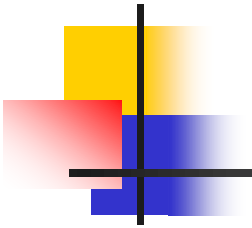
- Ensimmäinen hyökkäys 1988: Internet Worm (artikkelissa Morris Worm)
- Järjestelmät kuormittuivat madon vuoksi

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 muös EIP, seuraavaksi suoritettavan käskyn osoite
  - EBP = Base Pointer, Osoittaa oletuspinon kehyksen loppuun. Käytetään paikallisten muuttujien käsittelyyn.
  - ESP = Stack Pointer, Osoittaa oletuspinon 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

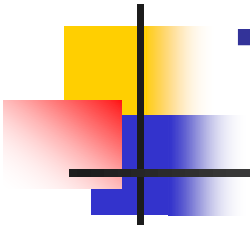
- Kolme sukupolvea:
  - 1. pino
  - 2. kasamuisti, funktioiden (metodien) osoittimet ja yhden tavun haavoittuvuus (off-by-one exploit)
  - 3. merkkijonojen muotoilu ja kasan rakenne



Turvallinen ohjelmointi

Puolesta?

- Korjaaminen halvempaa
- Ei kerry teknistä velkaa
  - Ylläpito on helpompaa
- Haavoittuvuus voi kaataa yhtiön
- Ei tarvita konsulttia
- Lainsäädännölliset vaatimukset ja sanktiot
- Kansallinen turvallisuus (valtion yhtiöt)
- Ohjelma ei kaadu
- Raketin tuhoutuminen ohjelmavirheen vuoksi, oltaisiin voitu välttää
- Insinöörien vika, ei ohjelmoijan



Turvallinen ohjelmointi

Vastaan?

- Halvempaa
- Ylläpitona voi tehdä
- Aikataulu paukkuu
- Yksin voi koodata turvattomasti
- Voi tehdä huolettomia oletuksia
- Konsultin voi aina palkata
- Turvaohjelmat huolehtii
- Ei käytetä henkilötietoja
- Henkilö vuotaa tietoja, ei ohjelma
- Ekspertit tarkastavat, ohjelmoijan ei tarvitse