

Väitöstiedote**08.01.2020**

Tietoturva-aukkojen ehkäisy laitteistotuen avulla

Väitöskirjan nimi Hardware-assisted memory safety

Väitöskirjan sisältö Nyky-yhteiskunnassa tietojärjestelmät ovat keskeisessä asemassa. Tietokoneohjelmat ovat kuitenkin erehtyväisten ihmisten kehittämiä ja niissä esiintyy usein muistivirheitä, jotka johtavat tietoturva-aukkoihin. Järjestelmien laaja suojaaminen edellyttää että tietoturva voidaan integroida jo käytössä oleviin työkaluihin ja ohjelmointikieliin. Tällaisilla ohjelmistopohjaisilla lähestymistavoilla on kuitenkin perinteisesti huono suorituskyky. Tässä väitöskirjassa osoitan kuinka uusien suorittimien tietoturvaominaisuuksia voidaan hyödyntää tehokkaasti ilman merkittäviä lisäkustannuksia.

Tutkimukseni keskittyy ARM Pointer Authentication (PA) ja Intel Memory Protection Extension (MPX) -ominaisuuksien analysointiin. Osoitan miten aiempien sovellusten heikkouksia voidaan paikata ja kuinka PA:n avulla voidaan toteuttaa ajonaikainen tyyppien tarkistus sekä tarkka paluusoitteiden varmentaminen. Esitän myös suojausmenetelmän, joka sallii MPX:n käytön käyttöjärjestelmän ytimessä. Osoitan myös miten Intel Software Guard Extensions branch-shadowing -sivukanavahyökkäys voidaan estää ohjelman kontrollivuon hämärtämisellä.

Koska tuki esittämille tietoturvamenetelmille toteutetaan kääntäjään, niiden käyttö on vaivatonta eikä vaadi muutoksia ohjelman lähdekoodiin. Menetelmät hyödyntävät suorittimeen sisäänrakennettuja ominaisuuksia ja ovat siksi ohjelmistopohjaisia menetelmiä suorituskykyisempiä. Tämä väitöskirja osoittaa siten että laajasti saatavilla olevien tietoturvaominaisuuksien avulla voidaan kattavasti ja tehokkaasti parantaa sekä nykyisten että tulevien tietojärjestelmien tietoturvaa.

Väitöskirjan ala Tietotekniikka, tietoturva

Tohtorikoulutettava Hans Liljestrand, MSc

Väitöksen ajankohta 20.01.2020 klo 12:00

Paikka Aalto-yliopiston perustieteiden korkeakoulun AS1 sali, Maarintie 8, Espoo

Vastaväittäjä Professori Juha Rönning, Oulun Yliopisto

Kustos Professori N. Asokan, Aalto-yliopiston perustieteiden korkeakoulu, tietotekniikan laitos

Väitöskirjan verkko-osoite

Tohtorikoulutettavan yhteystiedot Hans Liljestrand
Tietotekniikan laitos
+358 (0)45 323 9394
hans@liljestrand.dev