Aalto-yliopisto

Väitöstiedote **30.10.2020**

Laitteistoavusteiset puolustuskeinot suojaavat tulevaisuuden älylaitteita tietomurroilta

Väitöskirjan nimi	Toward Hardware-assisted Run-time Protection
Väitöskirjan sisältö	Väitöskirja tutkii kuinka laitteistoavusteiset puolustuskeinot voivat suojata mobiililaitteita ja sulautettuja järjestelmiä verkkohyökkäyksiltä. Merkittävä syy edellä mainittujen järjestelmien haavoittuvuuteen ovat ohjelmistovirheet, jotka heikentävät ohjelmiston muistiturvallisuutta. Hyökkääjä voi hyväksikäyttää muistihaavoittuvuuksia, kaapata niiden avulla ohjelmiston suorituksen ja jopa ottaa haavoittuva tietojärjestelmä täysin haltuunsa. Tietoturvatutkimusta on viimeisen kolmenkymmenen vuoden aikana sävyttänyt kilpavarustelu yhä edistyneempien hyökkäysten ja niitä vastaan kehitettyjen puolustuskeinojen välillä. Ymmärrys hyökkäyksistä on lisääntynyt huomattavasti viime aikoina ja näiden hyökkäysten estämiseksi suunniteltujen puolustuskeinojen kehityksessä on nähty huomattavia editysaskeleita. Ohjelmistotason puolustukset, jotka jälkiasentavat ohjelmistojen ajonaikaista eheyttä ylläpitäviä mekanismeja C tai C++ -ohjelmiin, estävät useat hyökkäykset, mutta niistä aiheutuvat huomattavat suorituskykykustannukset rajoittavat niiden käyttöönottoa. Puolustuskeinoja suunniteltaessa onkin aina pyrittävä löytämään optimaalinen tasapaino turvallisuuden, suorituskyvyn ja käytettävyyden välillä. Tämän väitöskirjan tulokset osoittavat, että laitteistoavusteisia puolustukeinoja voidaan hyödyntää ajonaikaisen eheyden ylläpitämiseen tai ohjelman käyttäytymisen todentamiseksi heikentämättä ohjelmistojen suorituskykyä huomattavasti. Väitöskirjassa sovelletaan laitteistoavusteisia puolustuskeinoja sekä sulatettuihin järjestelmään, että ARM-prosessoreihin, joita löytyy jo tällä hetkellä miljardeista älylaitteista.
Väitöskirjan ala	Tietoturva
Tohtorikoulutettava	Thomas Nyman, Filosofian maisteri
Väitöksen ajankohta	10.11.2020 klo 12
Paikka	Väitöstilaisuus järjestetään etäyhteydellä Zoomissa: https://aalto.zoom.us/j/65326571050
Vastaväittäjä	professori Mathias Payer, EPFL, Sveitsi
Kustos	professori N. Asokan, Aalto-yliopiston perustieteiden korkeakoulu, tietotekniikan laitos
Väitöskirjan verkko-osoite	http://urn.fi/URN:ISBN:978-952-64-0065-5
Tohtorikoulutettavan yhteystiedot	Thomas Nyman, Tietotekniikan laitos thomas.nyman@aalto.fi

Aalto-universitetet

Disputationsmeddelande 30.10.2020

Hårdvaruassisterade försvarsmekanismer skyddar framtida smarta enheter från dataintrång

Doktorsavhandlingens titel	Toward Hardware-assisted Run-time Protection
Doktorsavhandlingens innehåll	Doktorsavhandlingen undersöker hur hårdvaruassisterade försvarsmekanismer kan skydda framtida mobila och inbyggda system från nätattacker. En betydande orsak till sårbarheter i ovannämda system är programmeringsfel som försämrar minnessäkerheten i mjukvaruprogram. En angripare kan utnyttja minnessårbarheter för att kapa programutförandet och t.o.m. ta fullständig kontroll över sårbara datasystem. Forskningen inom datasäkerhet har under de senaste trettio åren präglats av en kapprustningen mellan alltmer sofistikerade attacker och försvarsmekanismer emot dem. Väsentliga framsteg har skett i förståelsen av attacker och försvarsmekanismer. Mjukvarubaserade försvar som lägger till mekanismer för upprätthållandet av programintegritet under utförandet i program skrivna i C eller C++ kan skydda mot en stor del av möjliga attacker, men försämrar däremot programprestandan betydligt. Praktiska försvarsmekanismer måste hitta en optimal balans mellan säkerhet, prestanda och tillämpbarhet. Resultaten i denna doktorsavhandling visar att hårdvaruassisterade försvarsmekanismer kan användas för att skydda eller utföra intyg gällande programintegritet under programutförandet utan att försämra programmets prestanda nämnvärt. Doktosavhandlingen tillämpar hårdvaruassisterade försvarsmekanismer såväl för inbyggda system som ARM processorer, som i dagens läge redan finns i biljoner av smarta enheter.
Forskningsområde	Datasäkerhet
Doktorand	Thomas Nyman, fil.mag.
Tidpunkt för disputationen	10.11.2020 kl 12
Plats	Disputation sker via fjärranslutningen i Zoom: https://aalto.zoom.us/j/65326571050
Opponent	professor Mathias Payer, EPFL, Schweiz
Kustos	professor N. Asokan., Aalto-universitet högskolan för teknikvetenskaper, institutionen för datateknik
Internetadress	http://urn.fi/URN:ISBN:978-952-64-0065-5
Doktorandens kontaktinformation	Thomas Nyman, Institutionen för datateknik thomas.nyman@aalto.fi

Aalto University

Dissertation press release 30.10.2020

Hardware-assisted defenses will protect future smart devices from cyberattacks

Title of the dissertation	Toward Hardware-assisted Run-time Protection
Contents of the dissertation	The dissertation explores how hardware-assisted defenses can protect mobile and embedded devices from run-time attacks. A prominent cause of vulnerabilities in aforementioned systems are programming errors, which undermine a software program's memory safety. An attacker can exploit such memory vulnerabilities to hijack the execution of the software, and even gain complete control of a vulnerable system. Over the past thirty years, there has been an ever-escalating arms race between increasingly sophisticated attacks and defenses designed to thwart them. Recently, there has been significant advances in understanding and defending against of run-time attacks. Software-only defenses, that retrofit mechanisms to maintain a program's run-time integrity to software written in C and C++ can be effective, but are prohibitively expensive in terms run-time overhead. Practical defenses must consider how to optimally trade-off security, performance and deployability. The results presented by this dissertation show that hardware-assisted defenses can be leveraged to protect, or to remotely attest, the run-time integrity of software without significant penalty to performance. The dissertation applies hardware-assisted defenses to embedded platforms, as well as ARM processors that can already now be found in billions of smart devices.
Field of the dissertation	Information security
Doctoral candidate	Thomas Nyman, M.Sc.
Time of the defence	10 November 2020 at 12 noon
Place of the defence	The defence is organized remotely on Zoom: https://aalto.zoom.us/j/65326571050
Opponent	Professor Mathias Payer, EPFL, Switzerland
Custos	Professor N. Asokan, Aalto University School of Science, Department of Computer Science
Electronic dissertation	http://urn.fi/URN:ISBN:978-952-64-0065-5
Doctoral candidate's contact information	Thomas Nyman, Department of Computer Science thomas.nyman@aalto.fi