Aalto University

Dissertation press release 08.01.2020

Utilizing off-the-shelf hardware for efficient memory protection

Title of the dissertation	Hardware-assisted memory safety
Contents of the dissertation	Computers today are ubiquitous. But programs are made by fallible humans and run on imperfect hardware. As a result, computers are plagued by memory vulnerabilities. Remedies exist but are often costly. To achieve wide-spread use, security must be effortlessly integrated into existing tools and languages. Meanwhile, new security features are being rolled out in commodity hardware but are non-trivial to use effectively. In this dissertation, I explore the utilization of such hardware features. I focus on ARM Pointer Authentication (PA), Intel Memory Protection Extensions (MPX) and Intel Software Guard Extensions (SGX). I show how to address weaknesses in prior PA-based defenses and present novel PA-based solutions for memory safety. I also explore kernel protection using MPX and present a compile-time mitigation for a branch-shadowing attack on SGX. The presented security schemes achieve minimal performance overheads by using features in off-the-shelf hardware. Compile-time instrumentation integrates these features into existing code, without developer intervention. The dissertation thus paves way towards widely deployable and performant security solutions for a large range of systems.
Field of the dissertation	Computer science, memory safety
Doctoral candidate	Hans Liljestrand, MSc
Time of the defence	20.01.2020 at 12:00
Place of the defence	Aalto University School of Science, lecture hall AS1, Maarintie 8, Espoo
Opponent	Professor Juha Röning, University of Oulu
Custos	Professor N. Asokan, Aalto University School of Science, Department of Computer Science
Electronic dissertation	
Doctoral candidate's contact information	Hans Liljestrand Department of Computer Science +358 (0)45 323 9394 hans@liljestrand.dev