SACHa: Self-Attestation of Configurable Hardware

Submitted by aekwall on Mon, 08/17/2020 - 11:36am

Title	SACHa: Self-Attestation of Configurable Hardware
Publication Type	Conference Paper
Year of Publication	2019
Authors	Vliegen, Jo, Rabbani, Md Masoom, Conti, Mauro, Mentens, Nele
Conference Name	2019 Design, Automation Test in Europe Conference Exhibition (DATE)
Keywords	attestation, composability, Computer architecture, configurable FPGA hardware, configurable hardware, device attestation, embedded device, Embedded Software, Embedded systems, field programmable gate arrays, Field-Programmable Gate Arrays, FPGAs, Hardware, hardware-based attestation, hardware-software system, Human Behavior, intended application code, Microprocessors, physical attacks, Protocols, pubcrawl, Read only memory, remote attacks, Resiliency, SACHa, self-attestation, Software, tamper-resistant hardware module
Abstract	Device attestation is a procedure to verify whether an embedded device is running the intended application code. This way, protection against both physical attacks and remote attacks on the embedded software is aimed for. With the wide adoption of Field-Programmable Gate Arrays or FPGAs, hardware also became configurable, and hence susceptible to attacks (just like software). In addition, an upcoming trend for hardware-based attestation is the use of configurable FPGA hardware. Therefore, in order to attest a whole system that makes use of FPGAs, the status of both the software and the hardware needs to be verified, without the availability of a tamper-resistant hardware module.In this paper, we propose a solution in which a prover core on the FPGA performs an attestation of the entire FPGA, including a self-attestation. This way, the FPGA can be used as a tamper-resistant hardware module to perform hardware-based attestation of a processor, resulting in a protection of the entire hardware/software system against malicious code updates.
DOI	10.23919/DATE.2019.8714775
Citation Key	vliegen_sacha_2019

attestation composability computer architecture configurable FPGA hardware configurable hardware device attestation embedded device embedded software embedded systems field programmable gate arrays Field-Programmable Gate Arrays FPGAs Hardware hardware-based attestation hardware-software system Human behavior intended application code Microprocessors physical attacks Protocols pubcrawl Read only memory remote attacks Resiliency SACHa self-attestation Software tamper-resistant hardware module