Process-aware side channel monitoring for embedded control system security

Submitted by grigby1 on Fri, 02/02/2018 - 1:17pm

Title	Process-aware side channel monitoring for embedded control system security
Publication Type	Conference Paper
Year of Publication	2017
Authors	Paul-Pena, D., Krishnamurthy, P., Karri, R., Khorrami, F.
Conference Name	2017 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)
Keywords	acoustic, actuator security, analog side channels, composability, computational loop, control logic, control systems, CPS computational nodes, CPS device, cryptography, cyber-attacks, Cyber-physical systems, embedded control system security, Embedded systems, Fans, feature extraction, heterogeneous hardware, Metrics, microcomputers, Monitoring, network connectivity, process stability, process-aware side channel monitoring, pubcrawl, real-time monitoring , Resiliency, run-time parameters, security, side channel sensors, side channel sensory modalities, side channels, software components, Temperature measurement, Temperature sensors, thermal

Abstract

Cyber-physical systems (CPS) are interconnections of heterogeneous hardware and software components (e.g., sensors, actuators, physical systems/processes, computational nodes and controllers, and communication subsystems). Increasing network connectivity of CPS computational nodes facilitates maintenance and on-demand reprogrammability and reduces operator workload. However, such increasing connectivity also raises the potential for cyber-attacks that attempt unauthorized modifications of run-time parameters or control logic in the computational nodes to hamper process stability or performance. In this paper, we analyze the effectiveness of real-time monitoring using digital and analog side channels. While analog side channels might not typically provide sufficient granularity to observe each iteration of a periodic loop in the code in the CPS device, the temporal averaging inherent to side channel sensory modalities enables observation of persistent changes to the contents of a computational loop through their resulting effect on the level of activity of the device. Changes to code can be detected by observing readings from side channel sensors over a period of time. Experimental studies are performed on an ARM-based single board computer.

URL http://ieeexplore.ieee.org/document/8203468/
DOI 10.1109/VLSI-SoC.2017.8203468
Citation Key paul-pena_process-aware_2017

actuator security acoustic analog side channels composability computational loop control logic control systems CPS computational nodes CPS device Cryptography cyber-attacks cyber-physical systems embedded control system security embedded systems Fans feature extraction heterogeneous hardware Metrics microcomputers Monitoring network connectivity process stability process-aware side channel monitoring pubcrawl Real-time monitoring Resiliency run-time parameters security side channel sensors side channel sensory modalities side channels software components Temperature measurement Temperature sensors thermal