Special Issue on Embedded System Security: Foreword

Alan Burns
University of York, UK

Steve Goddard
University of Iowa, Iowa City, US

2012 ACM Subject Classification Security and privacy → Embedded systems security
Keywords and Phrases Foreword, Embedded System Security
Digital Object Identifier 10.4230/LITES.7.1.0
Published 2021-08-12
Editor Alan Burns and Steve Goddard
Special Issue Special Issue on Embedded System Security

Embedded systems are now an integral part of our lives. We have smart phones, smart meters, smart appliances, smart cars, smart grids, and smart houses–most relying on embedded systems with outdated security mechanisms, if they have any at all. A renewed emphasis on embedded systems security research is critical to our economies and our daily lives. This special issue on Embedded System Security attempts to contribute to this work by drawing attention to a number of key topics including Intrusion Detection and Tolerance, Confidence and Threat Modelling, Enhancing Dependability in Embedded Systems, and reducing Vulnerabilities in System Architectures for Embedded Systems.

Two papers are included in this initial instalment of the Special Issue. In the first paper "Randomization as Mitigation of Directed Timing Inference Based Attacks on Time-Triggered Real-Time Systems with Task Replication" by Kristin Krüger, Nils Vreman, Richard Pates, Martina Maggio, Marcus Völp and Gerhard Fohler, the vulnerabilities of time-triggered systems are investigated. They note that the assumption that faults are independent, which is often made for accidental faults, is not valid for malicious attacks. They go on to introduce two runtime mitigation strategies to withstand directed timing inference. Both involve the introduction of a level of randomization within the usual deterministic behaviour of time-triggered systems.

In the second paper "We know what you're doing! Application detection using thermal data", Philipp Miedl, Rehan Ahmed and Lothar Thiele consider how sensitive runtime information can be extracted from a system by just using temperature sensor readings from a mobile device. They employ a Convolutional-Neural-Network to identify the sequence of executed applications over time. They test their hypothesis via collected data from two state-of-the-art smartphones and real user usage patterns. The accuracy of their finding demonstrated that this is a clear vulnerability in mobile devices, including the potential to compromise sensitive user data.

Alan Burns and Steve Goddard
August, 2021