Guest Editors' Introduction: Competing to Secure SoCs

Siddharth Garg
New York University

Daniel Holcomb
University of Massachusetts Amherst

Jeyavijayan (JV) Rajendran
Texas A&M University

Ahmad-Reza Sadeghi
Technische Universität Darmstadt

The recent outbreak of microarchitectural attacks is a reminder that our trust in hardware and security architectures is not always justified. These attacks illustrate that ever-increasing system complexity is fertile ground for exploitable security vulnerabilities. An exploited vulnerability in the field can lead to a system failure, generate a side channel to remotely access sensitive cryptographic keys, or gain privileged access that compromises the whole computing platform.

Although it is clearly important to find and fix vulnerabilities at design time before shipping hardware, security assurance teams working toward this goal face a difficult task. Consider securing a large system-on-chip (SoC) that integrates many intellectual property blocks. The IP blocks may be produced in-house or acquired from a third party, yet still must be vetted. Even if the constituent IPs are individually secure under assumed use-cases, bugs may arise when they are composed in the SoC.

Security assurance is a problem that cannot be solved by tools alone. Even setting aside practical concerns about scalability, verification tools are limited to checking a given set of specifications and lack the creativity to discover new weaknesses that are not already foreseen and specified. Additionally, verification takes place using models within the rigid boundaries of abstraction layers whereas security weaknesses can, and often do, cross abstraction layers. As of today, there is still a critical need for human ingenuity in security validation.

Nurturing and promoting a security mindset in human SoC designers was the impetus for the Hack@DAC competition, which has been held annually since 2017 at the Design Automation Conference. Teams participating in the competition mimic the role of a security assurance team that is responsible for the hardware and firmware of a system under test. The systems under the test provided to them are intentionally bug-laden SoCs created for the competition. Their objective is to identify vulnerabilities, assess their security impact, propose mitigation, and report them. The teams are free to use any tools and techniques of their choosing.

Through four years of the competition, over 100 teams from academia and industry have participated. The competition has evolved to have two phases. Phase I, which is distributed and takes place over a couple of months, gives the teams a first buggy SoC design, specification details, security properties, and a threat model to consider. The top-scoring teams from Phase I are invited to Phase II at DAC to test the security of a new SoC with even more bugs. Over a day and a half, the teams work frantically to detect and submit their bug reports, which are evaluated by our industry judges and reflected on a real-time scoreboard.

We are quite impressed by witnessing the growth of this competition, and by seeing its impact on developing a new generation of security-aware design and verification engineers. This success

Digital Object Identifier 10.1109/MDAT.2020.3045103
Date of current version: 10 March 2021.

is owed to the efforts of many people at Intel, TU Darmstadt, Texas A&M, support from the National Science Foundation, and of course the boundless energy of the participating teams.

The remainder of this section contains articles from four of the top-scoring teams that have competed in Hack@DAC over the past couple of years. In these articles, they describe their efforts in the competition.

We hope that you will enjoy reading these articles and that they will give you a sense of what the competition is all about.

- The article "SoC Security Evaluation: Reflections on Methodology and Tooling" demonstrates the benefit of supporting intuition with dynamic analysis flows that can quickly translate hypothesized weaknesses into proof-of-concept bug exploits.
- The article "Hardware Penetration Testing Knocks Your SoCs Off" targets the cryptography engines of the SoC to uncover the bugs that were inserted there.
- The article "Hunting Security Bugs in SoC Designs: Lessons Learned" advocates for the wider use of formal methods in security verification.
- Finally, the article "Texas A&M Hackin' Aggies' Security Verification Strategies for the 2019 Hack@DAC Competition" from a combined academia-industry team shows what can be accomplished through deep expertise with security tools. ■

■ Direct questions and comments about this article to Jeyavijayan (JV) Rajendran, Department of Electrical & Computer Engineering, Texas A&M University, College Station, TX 77843-3259 USA; jv.rajendran@tamu.edu.