Editorial: Embedded Security Challenge: Cyber Security Contests in the Embedded Computing Domain

Recently, we held a cyber security contest as part of worldwide Cyber Security Awareness Week (CSAW) competitions spearheaded by the Tandon School of Engineering at New York University (NYU). CSAW was initiated by the team at NYU back in 2003 in the United States. Over the years, it has evolved into concurrent regional events across the world—in India, Europe, Israel, the Middle East, and Africa. The event usually happens during the last 3 days of the second week of November. Most regions hold final rounds of the events for participants in their jurisdiction. In India, the event has been organized by the Indian Institute of Technology, Kanpur (IITK), for the past 3 years. One of those events is the Embedded Security Challenge (ESC)—which is of interest to readers of this journal. Every year, the challenge is released several months ahead of the November finals, and students from various universities are invited to participate. An international team led by NYU designs the challenge along with the regional ESC leaders. Once the problem is released, in the first phase, participants must analyze the problem and the challenge-specific hardware/software system and write a report on the kind of security vulnerabilities they expect to see in the system, the attack surfaces, and the threat models, and submit it for selection. If selected, the competing teams receive the embedded system artifact on which the challenge is designed, in the form of boards—such as an FPGA board, a Raspberry Pi board, or smart IoT devices. In the second phase, they must actually carry out the attacks and demonstrate the exploits. After they submit their second report, an international committee selects the finalists, who are then invited to the regional centers (e.g., US and Canadian finalists go to NYU; Indian participants go to IITK; European participants go to Grenoble, France).

At the finals, regional panels of expert judges listen to short presentations by the finalist teams, in which the attack models are discussed, and upcoming demonstration expectations are set. Finally, the teams demonstrate the attacks to the judges and the awardees are selected.

This year, the problem was chosen from the domain of IoT security. Currently, we are starting to see wide deployment of IoT devices in industrial settings, home and office automation, agriculture, critical infrastructure, and many other domains. Therefore, it is quite relevant to pose a question about the enhanced security attack surface exposed by such deployments and bring awareness about cyber security threats created by them. Teams worked on showing how side channels such as the chromatic variety of light emitted by smart bulbs can be analyzed to exfiltrate information.

Last year, the contestants were given Raspberry Pi boards to implement openPLC—an open-source programmable logic controller—and then find various ways of compromising security in a PLC, such as malicious inputs to mis-operate the PLC. In 2016, the problem given to the competitors was implementing openRISC on an FPGA board and finding control flow integrity and memory corruption vulnerabilities and countermeasures.

NYU has been holding this particular “capture the chip” competition for a while; in India, we have been organizing this competition since 2016.

One might be curious as to why such competitions are important and worth an editorial in our journal. Having watched the enthusiastic students (albeit small in number) actually working on

these problems at the nitty-gritty level of controllers, embedded processors, or smart devices and finding minute details in which are hidden the seeds of attacks, I feel that this is an important exercise for the future workforce to gain knowledge in embedded security, and also to understand the subtle attack paths that might not be obvious.

Notwithstanding that embedded security researchers have been working on finding hardware vulnerabilities for a long time now, “capture the chip” has not been mainstreamed as much as “capture the flag” (CTF)-type contests, where many young minds feel excited to find vulnerabilities in servers, databases, web services, and network stacks. Routinely, we have seen almost 50 teams participating in the CTF contests from India itself, whereas only eight teams participated in the embedded systems challenge. However, what is encouraging is that the numbers are increasing year to year, and not only are teams from top institutions participating but also, this time, we have had participation from state universities. In fact, this year, in the Indian regional CSAW, the best ESC award went to a state university—Cochin University of Science and Technology. This gives us hope that the mainstreaming of the embedded systems hacking, and protection is starting to happen.

I am therefore using this editorial to bring attention to the need for these kinds of events around the world, or perhaps as parts of conferences, workshops, and so forth, so that more and more people get involved in finding security attack surfaces and vulnerabilities of embedded systems, IoTs, and critical infrastructure test beds. Surely, we will need workforce development along these lines and more research in embedded security.

Also, to close Volume 17, I would like to express my gratitude to Laura Lander, ACM journals publication manager; Kelly Crooks, journal publication coordinator; and Arriane Bustillo, our journal assistant, for their unparalleled help in making ACM Transactions on Embedded Computing Systems publish in time and keeping the editorial process smooth and painless. I also thank my co-EiCs, senior editors Tulika Mitra and Hiren Patel, for helping me with the reviewing process and with planning and executing editorial activities. Finally, I thank all of our associate editors for their cooperation in keeping the review process as timely as possible. Last but not least, I thank all the reviewers and authors for their contributions throughout Volume 17.

I hope the readers enjoy this issue.

Sandeep K. Shukla
Indian Institute of Technology Kanpur
November 15, 2018
Editor-in-Chief