IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 2020

Mid-Summer Webinar Panel, July 28, 12:00-1:30pm EST, 2020

Title: How Can Hardware Security Contribute to the Fight Against COVID-19 and to Post Pandemic Life?

Panel Organizers: Jim Plusquellic, Saverio Fazzari and Domenic Forte

The COVID-19 pandemic has had unprecedented and widespread impacts on the economy, travel, politics, education, research, and human social lives in 2020. It is widely agreed that technology will play a critical role (both short-term and long-term) in mitigating the spread of the COVID-19 and establishing a "new normal". Personal protective equipment (PPE) is minimizing exposure to virus. Social distancing is being maintained through remote work, education, and health services, online retail, and on-demand food delivery. Scalable methods for fever screening and contact tracing are being developed to quickly identify the infected, warn patient contacts of exposure, and break chains of virus transmission. In the post-pandemic world, some of these 'best' practices may continue while new ones (e.g., contact-less everything, robot/drone delivery, etc.) emerge. Confidence in the hardware is more important because of the impact of the threat.

The new normal and upcoming practices/technologies have opened up the door to unfamiliar security and privacy issues. During this webinar, the moderator and panelists will discuss some of the risks, opportunities, and possible roadmaps for researchers in the field of hardware security to address them.

Moderator:

Saverio Fazzari, Booz Allen Hamilton

Panelists:

- Sae Woo Nam, National Institute of Standards and Technology
- Will Zortman, Sandia National Laboratories
- James Joshi, National Science Foundation
- Jim Plusquellic, University of New Mexico
- Rob Aitken, ARM

Topics:

The panel will primarily focus on the following topic areas and questions:

- *Data Privacy*: How secure are the devices being used for contact tracking, health monitoring, online shopping, etc.? How to avoid being tracked outside the workplace? How to protect against unauthorized access to my tracking and health information? How should such data be stored and for how long?

- *Data Transmission*: During teleconferences, how should audio and video be protected efficiently in hardware? How can unwanted intrusions (i.e., Zoom bombing) be prevented? How to enforce digital rights management?
- *User Authentication*: How should organizations provide access control for employees working from home, especially on security/IP sensitive tasks? How to verify who we are really talking to? What features need to be present in the hardware to support authentication, e.g., fingerprints, facial recognition, voice recognition, other biometrics?
- *Supply Chain/Counterfeit*: Are front-line workers, state governments, etc. getting genuine, PPE, medicine, vaccines? How can hardware security prevent price-gouging, and enable independence of international suppliers?
- *Hardware Trust*: Can the hardware built on top of low-cost embedded systems used for pandemic and post-pandemic technologies/practices (e.g., contact tracing, telework, telehealth, etc.) be trusted? How can hardware security make such hardware more trustworthy, and how can that trust be quantified?

All attendees must register using the following link:
https://event.on24.com/wcc/r/2508996/23DF48DE5BCC5A86AECBE618C8F53040?partnerref=panel