TITLE: Secure Code Execution on Untrusted Remote Devices

ABSTRACT

Our society is increasingly reliant upon a wide range of Cyber-Physical Systems (CPS), Internet-of-Things (IoT), embedded, and so-called "smart", devices. They often perform safety-critical functions in numerous settings, e.g., home, office, medical, automotive and industrial. Some devices are small, cheap and specialized sensors and/or actuators. They tend to have meager resources, run simple software, sometimes upon "bare metal". If such devices are left unprotected, consequences of forged sensor readings or ignored actuation commands can be catastrophic, particularly, in safety-critical settings. This prompts the following three questions: (1) How to trust data produced by a simple remote embedded device? (2) How to ascertain that this data was produced via execution of expected software? And, (3) Is it possible to attain (1) and (2) under the assumption that all software on the remote device might be modified or compromised? In this talk, we answer these questions by describing APEX: (Verified) Architecture for Proofs of Execution [1], the first of its kind result for low-end embedded systems. This work has a range of applications, especially, to authenticated sensing and trustworthy actuation, APEX incurs low overhead, making it affordable even for lowest-end embedded devices; it is also publicly available.

BIOGRAPHY

Gene Tsudik is a Distinguished Professor of Computer Science at the University of California, Irvine (UCI). He obtained his PhD in Computer Science from USC in 1991. Before coming to UCI in 2000, he was at the IBM Zurich Research Laboratory (1991-1996) and USC/ISI (1996-2000). His research interests include many topics in security, privacy and applied cryptography. Gene Tsudik is a Fulbright Scholar, Fulbright Specialist (twice), a fellow of ACM, IEEE, AAAS, IFIP and a foreign member of Academia Europaea. From 2009 to 2015 he served as Editor-in-Chief of ACM Transactions on Information and Systems Security (TISSEC, renamed TOPS in 2016). Gene was the recipient of 2017 ACM SIGSAC Outstanding Contribution Award. He is also the author of the first crypto-poem published as a refereed paper.