The Department of Electrical and Computer Engineering Presents

A DISTINGUISHED SEMINAR

GENE TSUDIK

RECONCILING SECURITY AND REAL-TIME CONSTRAINTS FOR SIMPLE IOT DEVICES

ABSTRACT

Remote attestation (RA) is a means of malware detection, typically realized as an interaction between a trusted verifier and a potentially compromised remote device (prover). RA is especially relevant for low-end embedded devices that are incapable of protecting themselves against malware infection. Most current RA techniques require on-demand and uninterruptible (atomic) operation. The former fails to detect transient malware that enters and leaves between successive RA instances; the latter involves performing potentially time-consuming computation over prover's memory and/or storage, which can be harmful to the device's safety-critical functionality and general availability. However, relaxing either on-demand or atomic RA operation is tricky and prone to vulnerabilities. This work identifies some issues that arise in reconciling requirements of safety-critical operation with those of secure remote attestation, including detection of transient and self-relocating malware. It also investigates mitigation techniques, including periodic self-measurements as well as interruptible attestation modality that involves shuffled memory traversals and various memory locking mechanisms.

This talk is based, in part, on joint work with N. Rattanavipanon, I. Oliveira Nunes, K. Eldefrawy, X. Carpent and A. Sadeghi. (An earlier version of this talk was presented at DAC 2018.)

BIOGRAPHY

Gene Tsudik is a Chancellor's 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 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, a fellow of IEEE, a fellow of AAAS, 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 to 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.

April 1, 2019

WCH 205/206

11:10 a.m. - 12:00 p.m.