Analog and Mixed-Signal Center
3128 TAMU
College Station, TX 77843-3128
Tel. (979) 845-7498
Fax. (979) 845-7161
E-mail:s-sanchez@tamu.edu

ELECTRICAL & COMPUTER ENGINEERING
TEXAS A&M UNIVERSITY

SEMINAR

Room 1035 ETB

November 13, 2017, 1:50 – 2:50 P.M.

An Embedded Platform for the Internet of Secure Things

by

Javier Elenes
Silicon Labs

Abstract: The advent of low-power, connected, embedded computing is enabling an increasing number of things to be connected to the internet. Devices have sensors and actuators and connectivity allows attacks to scale. Attacks that can sense and control physical things. Hackers can deny availability and integrity of things by exploiting vulnerabilities in hardware, software, protocols, and system design. We have seen recent exploits that open door locks, disable smart lights, take control of thermostats, and take control of connected cars, for example. This seminar is divided into three parts:
Part 1 introduces basic security principles and fundamentals of cryptography, and their applicability and relevance to embedded systems.
Part 2 describes how implementations get attacked, and countermeasures to protect against attacks. We cover side channel attacks, fault-injection attacks, and software attacks.
Part 3 introduces an embedded architecture for IoT devices. Two fundamental building blocks are covered: a Physically Unclonable Function and a True Random Number Generator. We conclude by summarizing best practices for device security.

Javier Elenes received Bachelor of Science and Master of Science degrees in electrical engineering from Drexel University in 1996. From 1996 to 2004 he held various technical positions at Telogy Networks, Motorla, and Cognio, Inc. He joined Silicon Labs in 2004 where he currently serves as Distinguished Engineer. From 2004 until 2016 he led the development and implementation of various digital signal processing algorithms for receiver synchronization, signal detection, channel estimation, adaptive equalization, weak signal handling and antenna diversity combining. He holds 29 patents in signal processing architectures, algorithms, and implementations. Since 2016 he has been working on IoT device security. His current areas of interest are cryptography, side-channel attacks, fault injection attacks, software security, protocol security, device hacking and countermeasures.