ECE 525: Hardware-Oriented Security and Trust (HOST)

Instructor: Prof. Jim Plusquellic

On-Line: SP 18 Second Half Term: 3/18/2017-05/12/2018

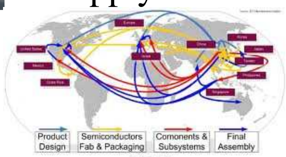
Society is increasingly dependent on microelectronic-supported infrastructures including safety-critical systems embedded in the transportation and utility infrastructures, communication and computation systems embedded in the financial and military systems, as well as the information systems supporting society's food, water, energy (smart-grid), manufacturing, aerospace, and health activities. Threats that target the integrity of such systems is a growing concern, driving the development of a new field called **Hardware-Oriented Security and Trust (HOST)**. HOST issues span a broad range including threats related 1) to the malicious insertion of Trojan circuits designed, e.g., that act as a 'kill switch' to disable a chip, 2) to integrated circuit (IC) piracy, and 3) to attacks designed to steal encryption keys from a chip.

This course covers IoT Security, Physical Unclonable Functions (PUFs), Hardware Trojans, IC obfuscation/metering, hardware encryption and authentication, side-channel attacks, etc. A background in hardware description languages (VHDL), VLSI and/or board design is a plus.

Secure boot

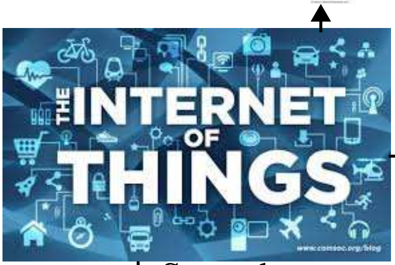
Self-driving cars

Supply chain



Secure data

Smart phone



Just smart

Chip fingerprints

↓ Smart home

Security and trust

Credit info theft