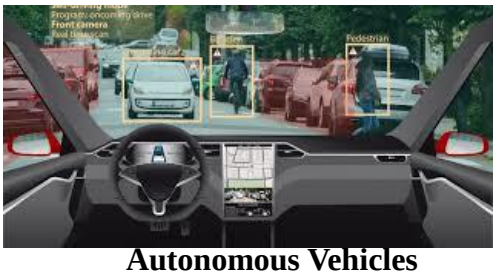
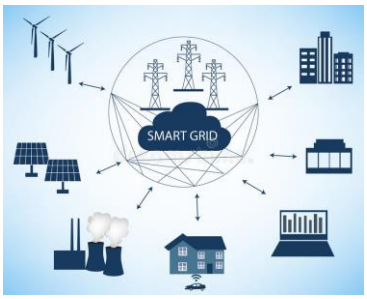
EE 458/558: Hardware Security & Trust (Fall 2019)

Smart House

Smart Wearables



Autonomous Vehicles



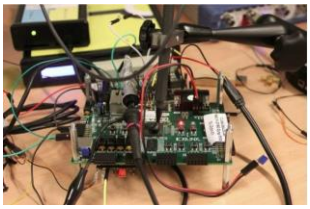
Smart Grid

Hardware Security & Trust

Semiconductor Supply Chain

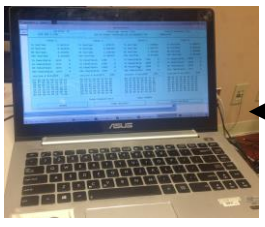
The rapidly growing number of Internet of Things (IoT) devices is changing the way we work, communicate and think. It is estimated that currently there are more than 10 billion connected IoT devices and this number is expected to rise to 50 billion by the year 2020. Threats that target the security, confidentiality and integrity of such microelectronic systems are of a growing concern, driving the development of a new field called Hardware-Oriented Security and Trust (HOST). This course introduces and investigates recent technology and development for the design and evaluation of secure and trustworthy hardware and embedded systems. The following topics will be discussed as well as their applications to the Internet-of-Things (IoT), machine learning, automotive/autonomous vehicles, smart devices, smart grid, communications and network systems: (1) IoT security and cryptography basics, (2) hardware security primitives including Physically Unclonable Functions (PUFs) and Random Number Generator (RNG), (3) authentications and key generations, (4) side channel attacks and countermeasures, (5) hardware trojans (6) secure boot and trusted execution environment, etc. Students will gain practical hands-on experience on the Xilinx Zynq-7000 ARM/FPGA SoC board (with an ARM dual-core Cortex A9 microprocessor integrated with programmable FPGA fabric). The main prerequisite includes C programing. Background in digital circuits is a plus.

Please contact the instructor Dr. Wenjie Che at wche@nmsu.edu for more course information.



Fault Injection Attack

Zybo Zynq 7000 ARM/FPGA SoC



Verifier (Server)

Prover (Tokens)

Hardware-based Authentication