The Roles of Hardware in Security and Trust

Cybersecurity Specialization
-- Hardware Security

Hardware in Security and Trust

Evolving role of HW in security:

- Enabler
- Enhancer
- Enforcer

Hardware in Security and Trust

Evolving role of HW in security:

- Enabler
- Enhancer
- Enforcer

Challenges for Hardware Design

- Secure the design
  - Intellectual property (IP) piracy: overbuilding, counterfeiting, IP theft and misuse
  - Trusted integrated circuits (IC): backdoors, hardware Trojan horse
- Secure the data
  - Side channel attacks
  - Physical attacks to memory
- Provide HW security primitives
  - TPM, secure co-processor
  - PUF, xRNG
  - New devices and technology

Thank you!