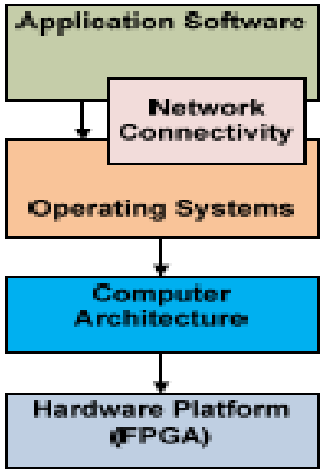
Integrating Embedded Systems Security into Computer Engineering/Science Curricula

Challenges:

- Internet of Thing (IoT) devices pose daunting security challenges
- Curricula focusing on unique challenges of IoT security not yet well developed



Scientific Impact:

- Development of security course modules related to software, networking, OS, architecture and hardware
- Integration of modules into existing courses
- Development of a unified IoT security course

Solution:

- Systematic security design method
- Course modules of IoT security enable easy integration into exiting curricula

Lecture I:	**FPGA circuit modules for security applications** • FPGA based cryptography engine • FPGA based pattern matching circuit for intrusion detection
Lecture II:	**Security attack methods and countermeasure techniques for embedded FPGA hardware** • Overview of the security vulnerability of FPGA systems • Case study: side channel and fault injection attacks to FPGA cryptographic engines and countermeasure techniques • Protecting FPGA design IP and configuration bit streams • Secure remote reconfiguration
Project:	FPGA Implementation of a RSA Encryption Engine

5-layer security module & Outline of hardware security

Broader Impact:

- Impact on over 100 students per year
- Dissemination through conference & journal articles, an archival CD-ROM, a dedicated website for course material, and through organized workshops

PIs: Drs. Ning Weng, Haibo Wang, Meera Komarraju (Southern Illinois University); Harini Ramaprasad, UNC Charlotte; Meng Yu, UT San Antonio; Wei Zhang, Virginia Commonwealth University.

Project numbers: 1623353/ 1623247/1623268/1623277

Contact: Ning Weng (nweng@siu.edu)