EECE401Senior Design I
Instructor: Dr. Charles Kim
www.mwftr.com/SD1415.html

Security Evaluation of Cryptographic Algorithms on FPGAs against Hardware Trojan Attacks

Prof. Hassan Salmani

Presented by Candace Ross

Backgrounds

- Security is main constituent of any computing machine
- Cryptographic algorithms are used to protect sensitive information from leakage or modification
- Modern FPGAs with significant resources are widely used to realize complex computation, like cryptographic algorithms, at the hardware level to enhance the over performance of computing systems
- Varity of attacks have been implanted to interfere cryptographic operations to expose secret information

Objectives

- Implementing cryptographic algorithms
- Study hardware Trojans
- Study vulnerabilities of the cryptographic algorithms against hardware Trojan attacks.
- Introduce technique(s) to prevent/detect the hardware Trojan attacks

Requirements

- Study security and security primitives
- Study and implement one cryptographic algorithm on FPGA
- Optimize the algorithm in terms of power, performance, and size
- Study hardware Trojan attacks
- Implement a couple of hardware Trojan attacks on your cryptographic algorithm
- Introduce technique(s) to prevent/detect the hardware Trojan attacks

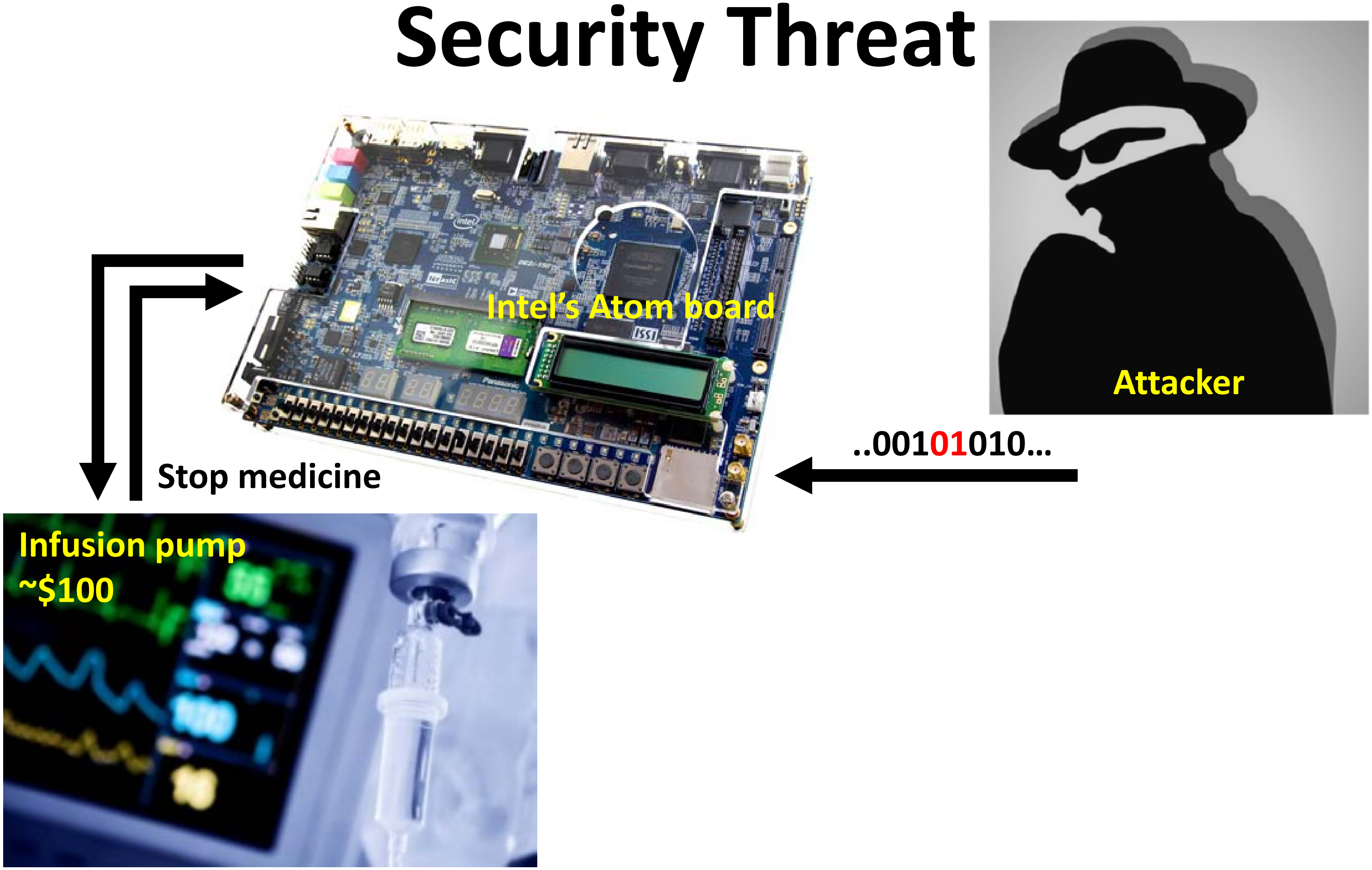
Deliverables

- Presenting the implemented cryptographic algorithms on Intel Atom boards
- Lunching some hardware Trojan attacks
- Evaluating proposed security measures against hardware Trojan attacks.

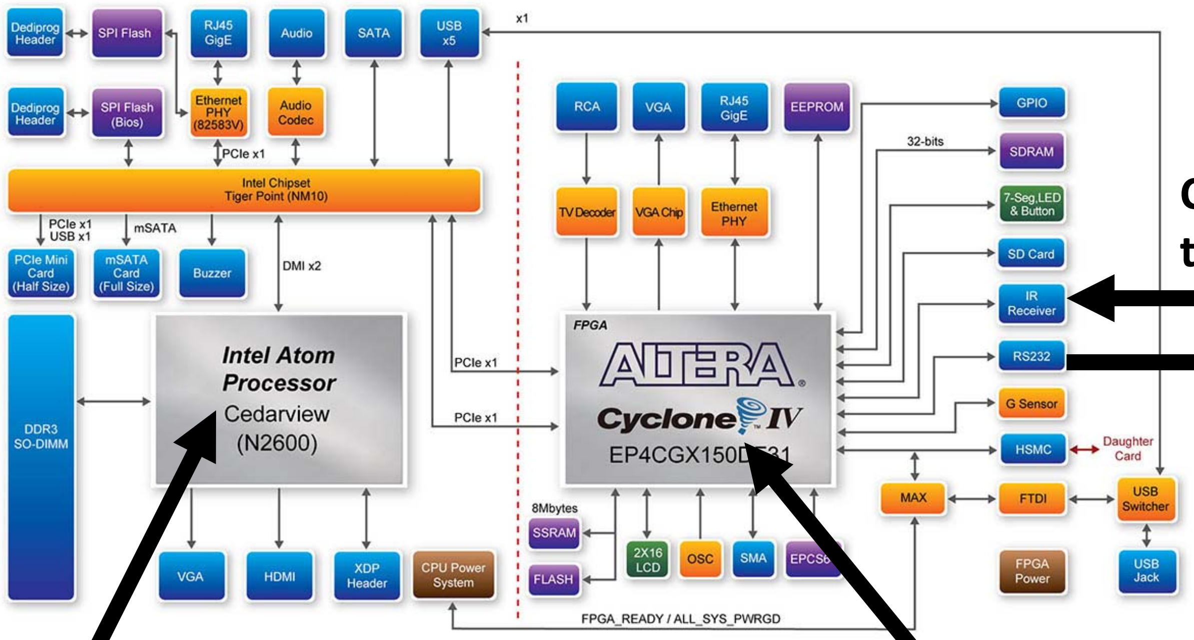
Cyber Security of Medical Devices

Prof. Hassan Salmani

Security Threat



System Implementation



Command inputs through IR input

Command outputs to a medical devices

Issuing command after validation or announcing an attack

Validate the command’s issuer