Week 6 Good Practice and Emerging Technologies

Help Center

Overview

This is the last week and we will cover some positive things on hardware security. We start with trust platform module (TPM), followed by physical unclonable functin (PUF), and FPGA-based system design. We conclude with a short discussion on the roles that hardware play in security and trust.

Learning Objectives

After the completion of this week, you will be able to:

- know the basics of TPM
- understand what is PUF and how it can help to build more secure system
- learn the vulnerabilities and countermeasures in FPGA design and FPGA-based systems

Video Lectures

- Trust Platform Module and Other Good Practices (8'59") PDF
- Physical Unclonable Functions (PUF) Basics (16'23") PDF
- RO PUF: Reliability (8'06") PDF
- FPGA Implementation of Crypto (13'44") PDF
- Vulnerabilities and Countermeasures in FPGA Systems (10'22") PDF
- Role of Hardware in Security and Trust (5'34") PDF

Discussions

Click here to view the Week 6 Discussion Questions.

Quizzes

Click here to take the quiz.

Created Tue 29 Apr 2014 9:43 AM PDT

Last Modified Wed 11 Feb 2015 5:14 AM PST