Lecture Notes on Jan/10/2023

Chapter 1:
Introduction

CYENG 225: Microcontroller Essentials for Cyber Applications

Instructor: Dr. Shayan (Sean) Taheri
Gannon University (GU)

Personal Information

- Name: Shayan (Sean) Taheri.
- Date of Birth: July/28/1991.
- Past Position: Postdoctoral Fellow at University of Florida.
- Ph.D. Degree: Electrical Engineering from the University of Central Florida.
- M.S. Degree: Computer Engineering from the Utah State University.
- University Profile: https://www.gannon.edu/FacultyProfiles.aspx?profile=taheri001

Need for Secure Processor Architectures

- **Chapter 1 Overview**
  - Provision of motivation for education, research, and work on secure processor architectures.
  - Provision of an outline of the organization of this course.

- **Design of Secure Processor Architectures**
  - Provide extra hardware features which enhance commodity processors with new security capabilities.
  - The new security features may be purely in hardware → Hardware Security Architectures.
  - They may be implemented in both hardware and software → Hardware-Software Architectures.
  - Secure Processor Architectures → Designed as extensions of commodity processors, and are based on architectures such as such x86 or RISC.
  - There is an increased need for implementing security features in processor architectures in recent years due to **Three Factors**: **(1)** Software Complexity and Bugs; **(2)** Side-Channel Attacks; and **(3)** Physical Attacks.

Need for Secure Processor Architectures (Cont.)

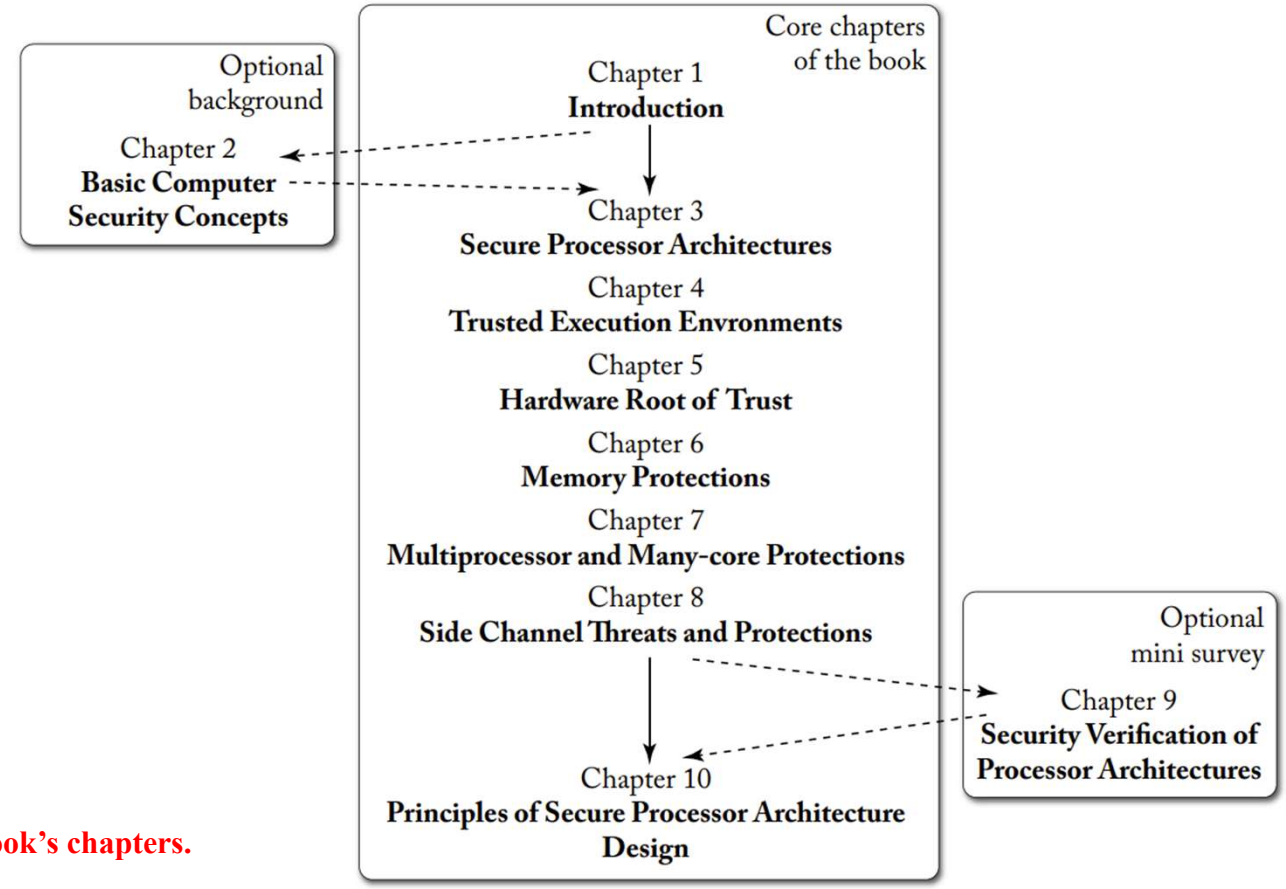
- **Software Complexity and Bugs**
  - It is impractical, or even impossible, to provide security solely based in software.
  - Increased complexity and size of the software code running on commodity processors, especially the operating system or the hypervisor code.
  - More and more lines of software code lead to increased number of software bugs and potential exploits.
  - New features (e.g., new protection levels or new hardware features for creating trusted software executing environments) are needed to provide an execution environment wherein a small, trusted code can execute separated from the rest of the untrusted code.
- **Side-Channel Attacks**
  - Computation is today often done in settings such as in cloud computing where many different users share the same physical hardware.
  - Co-residency of potential victims and attackers on same hardware can allow the attackers to learn sensitive information through shared hardware and the side channels.
  - Timing-based side channels, and also power, RF, or EM-based ones, exploit known side effects of the behavior of commodity processors when different types of computations are performed.
  - Only modifications at the architecture and hardware levels can mitigate different types of side channels and the resulting side-channel attacks.

Need for Secure Processor Architectures (Cont.)

- **Physical Attacks**
  - Attacks including physical probing of memory busses or even memory chips have necessitated protections against not just software, but hardware or physical attacks.
  - As cloud computing has increased in popularity, where users no longer have physical control over the hardware on which their code runs, new mechanisms are needed to protect the code and data against physical attacks.
  - Embedded devices or Internet-of-Things devices are prone to physical attacks as users may not have physical control over the devices at all times.

Book Organization

- The **overarching design goal** of **secure processor architectures** is to →
  - Protect **integrity** and **confidentiality** of user applications, operating system, hypervisor, or other software components, depending on the threat model and assumptions of the particular architecture.
  - Prevent **software or hardware attacks** (again, within limits of the particular threat model).



Organization of the book's chapters.

Assignment

- **Reading Assignment:**
  - Zferer, J., 2018. **Principles of secure processor architecture design**, ser. Synthesis Lectures on Computer Architecture. Morgan & Claypool Publishers, 9048, pp.1-175.
    - ✓"Chapter 1: Introduction", Pages 1-3.

Questions?