Week 4 Side Channel Attacks and Countermeasures

Help Center

Overview

This week, we focus on side channel attacks (SCA). We will study in-depth the following SCAs: cache attacks, power analysis, timing attacks, scan chain attacks. We will also learn the available countermeasures from software, hardware, and algorithm design.

Learning Objectives

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

- learn the vulnerabilities of information leak from side channels.
- understand how attacks can be launched from various side channels.
- consider the potential side channel information leak when you design a secure system.
- get better understanding on how to implement security primitives such as RSA securely.
- develop the system engineering approach of building secure systems (e.g. both SCA attacks and the countermeasures can come from all phases of the system design).

Video Lectures

- Introduction to Side Channel Attacks (14'03") PDF
- Memory Vulnerabilities and Cache Attacks (19'45") PDF
- Power Analysis (16'19") PDF
- More Attacks and Countermeasures (13'02") PDF
- Modified Modular Exponentiation (22'59") PDF

Readings

- K. Mai, "Side Channel Attacks and Countermeasures", in *Introduction to Hardware Security and Trust*, pp. 175 - 194, Springer, ISBN 978-1-4419-8079-3, 2012.
- P. Kocher. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems", CRYPTO'96, 1996.
- P. Kocher, J, Jaffe, and B. Jun, "Differential power analysis", CRYPTO'99, 1999.
- D. Mukhopadhyay and R. S. Chakraborty, "Cache Attacks on Ciphers", in *Hardware Security and Trust: Design, Threats, and Safeguards*, pp. 265-291, CRC Press, 2015.

Discussions

Click here to view the Week 4 Discussion Questions.

Quizzes

Click here to take the quiz.

Created Tue 29 Apr 2014 9:43 AM PDT

Last Modified Tue 3 Feb 2015 6:32 AM PST