Week 3 Physical Attacks and Modular Exponentiation

Help Center

Overview

This week you will learn the fundamentals about physical attacks: what are physical attacks, who are the attackers, what are their motivations, how can they attack your system (from hardware), what kind of skills/tools/equipment they should need to break your system, etc. You will also see what are the available countermeasures. You will learn how system security level and tamper resistance level are defined and some general guidelines on how to make your system secure by design.

In the second part, you will learn a useful mathematical operation called modular exponentiation. It is widely used in modern cryptography but it is very computational expensive. You will see how security vulnerability might be introduced during the implementation of this operation and thus make the mathematically sound cryptographic primitives breakable. This will also be important for you to learn side channel attack next week.

Learning Objectives

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

- understand the vulnerability to a system from hardware (physical attacks)
- learn the available countermeasures to physical attacks

- perform security evaluation for the hardware implementation of security modules
- modular exponentiation, various ways to evaluate it and the security vulnerability

Video Lectures

- Physical Attacks (PA) Basics (14'32") PDF
- Physical Attacks and Countermeasures (13'55") PDF
- Building Secure Systems (10'25") PDF
- Modular Exponentiation (ME) Basics (6'15") PDF
- ME in Cryptography (8'54") PDF
- ME Implementation and Vulnerability (14'25") PDF
- Montgomery Reduction (11'51") PDF

Readings

- S. Skorobogatov, "Physical Attacks and Tamper Resistance", in *Introduction to Hardware Security and Trust*, pp. 143 - 174, Springer, ISBN 978-1-4419-8079-3, 2012. (see his slides: http://www.cl.cam.ac.uk/~sps32/PartII_030214.pdf)
- R. Anderson, M. Kuhn. *Tamper Resistance - A Cautionary Note.* COAST TR 96-08; Cambridge University, 1996.

Discussions

Click here to view the Week 3 Discussion Questions.

Quizzes

Click here to take the quiz.

Created Tue 29 Apr 2014 9:43 AM PDT

Last Modified Thu 15 Jan 2015 4:37 AM PST