ECE 579C Applied Cryptography and Physical Attacks

When: Mondays 6:00 – 8:50 pm, starting Thursday, January 15, 2015
Where: AK 219
Instructor: Thomas Eisenbarth
email: teisenbarth@wpi.edu, phone: (508) 831-5914, office: AK 307
Office hours: Tuesday 9:00am – 10:00am, by appointment, or just come by.

Course description

This course explores practical aspects of cryptographic engineering by showing how cryptographic algorithms make their way into real-world systems. The course explores efficient implementation techniques for the most popular symmetric and asymmetric cryptographic algorithms, such as AES and RSA. Physical attacks on cryptographic systems, such as timing and power analysis, and fault injection attacks are discussed and applied. Countermeasures to protect practical security systems against physical attacks complete the course. Concepts are reinforced with project-like programming exercises.

Prerequisites: CS/ECE 578, ECE579 or a related introduction into computer security

Target Audience

The course is suited for students with a ECE, CS, or similar background. Interested undergraduate students are also welcome. The course targets students interested in cryptography or other security related fields such as trusted computing, network and OS security, or general IT security.

Course Outcomes

In this course you will build and break cryptographic solutions and learn how to protect against practical attacks. After attending the course you will:

- Understand why popular cryptographic schemes have been designed the way they are.
- Be able to build secure and efficient cryptographic engines.
- Understand methods and algorithms for efficient long number arithmetic.
- Have performed basic physical non-invasive attacks on embedded cryptographic systems, and know how to perform more advanced attacks.
- Protect cryptographic engines against specific physical attacks, as well as evaluate the security of existing engines.

Finally, the course provides an overview of relevant topics of research modern embedded cryptology.

Course Outline

The following is a tentative course outline. There will be one individual project overarching the entire course. It will include a paper writeup as well as a presentation. There will also be two smaller programming projects complementing each part of the course (a total of 4).

Part 1: Embedded Cryptographic Systems

1 - Overview of symmetric and asymmetric cryptography
2 - Symmetric Crypto: AES and AES-GCM
3 - Asymmetric crypto: RSA and RSA PKCS#1 v2.1
4 - Symmetric Implementation: AES T-Tables
5 - Asymmetric Implementation: efficient exponentiation, CRT

Project 1: Simple Implementations: AES, and RSA
Project 2: Optimized implementations: AES T-Tables, and RSA-CRT

If time permits: Random Number Generation: PRNG and TRNGs; Details on Block Cipher Constructions; Karatsuba and Montgomery implementation for RSA

Part 2: Physical Attacks and Countermeasures

6 - Fault Attack on RSA-CRT and Countermeasures
7 - SPA on RSA and countermeasures
8 - Timing Attacks: Cache attacks on AES
9 - Differential Power Analysis on AES and Template Attacks
10 - Advanced Methods for leakage Detection and Quantification
11 - Differential Fault Attacks on AES (and other block ciphers)
12 - Countermeasures against DPA: Basics and Threshold Implementation
13 - Countermeasures against Fault Attacks: Basics and Infective Computation

Project 3: Timing Attack and
Project 4: Fault attacks on RSA and DFA on AES

If time permits: Timing Attacks on RSA; Infective Computing Countermeasure;

Textbook

The course will not follow a particular text book. The Handbook of Applied Cryptography is recommended as a reference. Further material will be provided through Blackboard.

[1] (optional) Menezes, van Oorschot, Vanstone: *Handbook of Applied Cryptography*. CRC Press. 5th printing 2001. Downloads for academic purposes are available from: www.cacr.math.uwaterloo.ca/hac

[2] (optional) Mangard, Oswald, and Popp: *Power Analysis Attacks: Revealing the Secrets of Smart Cards.* 1st edition, Springer, 2010 (ISBN 978-0-387-30857-9)

[3] (optional) Cetin Kaya Koc (Editor): *Cryptographic Engineering.* 1st edition, Springer, 2009

Background on Cryptography:
[4] Paar, Pelzl: *Understanding Cryptography: A Textbook for Students and Practitioners.* 1st edition, Springer, 2009

Grading

Grading is based on a research project, and programming projects. The weights for the final grade are as follows:

Individual Project (+Paper and Presentation)	**60%**
Programming Projects	**40%**

The following grading scale will be used:

Cumulative Performance	Grade
>90%	A
>80% - 90%	B
>65% - 80%	C
55% - 65%	D
<55%	F

Honor Code

Students at WPI are expected to maintain the highest ethical standards. Academic dishonesty, including cheating and plagiarism, is considered a serious breach of these ethical standards, because it interferes with the university mission to provide a high quality education in which no student enjoys an unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and places high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. For more information, see:
http://www.wpi.edu/offices/policies/judicial/sect5.html

Students with Disabilities

If you need course adaptations or accommodations because of a disability, or if you have medical information to share with me, please make an appointment with me as soon as possible. If you are entitled to accommodation in accord with documentation on file at the Disabilities Service Office, let me know as soon as possible so I can arrange for the accommodation.

This syllabus is subject to reasonable changes at the discretion of the instructor.