ECE 4451-001 (22765), ECE 5451-001 (22777):
HARDWARE SECURITY – SPRING 2017

Lecture: MoWe 3:35-4:50 PM, CHM T114

Instructor: Prof. Marten van Dijk **Office:** ITEB 431 **Email**: marten.van_dijk@uconn.edu

TA: Phuong Ha Nguyen **Email**: Phuong_ha.nguyen@uconn.edu **Office Hours:** By appointment TBD

Course Description

This course treats several topics in hardware security: The main focus is secure processor architectures – we will discuss Intel SGX as well as academic processors such as Aegis, Ascend, and Sanctum and we will discuss cryptographic concepts (no proofs or formal definitions) such as AES, RSA, Hash, MAC, digital signatures, public key encryption, ORAM. During the second half of the course we explain side channel attacks, physical unclonable functions, TRNG, supply chain management, and hardware Trojans in more detail and we give an overview of several other topics (in particular, we will talk about the power grid and smart cities). Several coding labs will give sufficient understanding of the most important taught subjects.

Prerequisite

Since this course is completely new, ECE 3401 is no longer a prerequisite. Students need to make an appointment with the instructor to obtain a permission number. During each meeting the instructor verifies whether the student understands the workload and whether the student has some basic understanding of computer architecture and/or crypto – even though the course is self-contained some prior understanding will make the workload less. Students are required to have some level of independence in taking responsibility for their own success.

Learning Objectives (EAC outcomes (a) an ability to apply knowledge of engineering, and (k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice):

To understand main hardware security concepts:

- To be able to converse intelligently in secure processor architectures and understand or even to be able to simulate performance of added hardware modules.
- Understand a wide range of hardware security concepts. In particular, be able to reason about security in terms of adversarial models, hardware vulnerabilities, and attacks.
- To have a conceptual understanding of how the field of hardware security is evolving.

Distribution of slide decks, lab problems, other reading material, etc.: If you have not already received an invitation, you can sign up for Piazza yourself by following the link https://piazza.com/uconn/spring2017/ece4451and5451/home. We will use Piazza as a forum for discussion and Q&A as well as the method of preference to post lab assignments, distribute solutions to questions, additional reading material and emailing the class.

Spring 2017 Course Schedule and Student Activities:

Before coming to first lecture/lab:

- Make sure to have set up Eclipse/GCC
- Sign up for Piazza (https://piazza.com/uconn/spring2017/ece4451and5451/home)

wks	Date	Lecture	Assignment
1	18-Jan	Lec1: Course outline, report requirements + Application layer	
2	23-Jan	Lec2a: Code injection	**Required** reading: (1) Aleph One, "Smashing the stack for fun and profit," http://phrack.org/issues/49/14.html#article (2) Y. Younan, W. Joosen, and F. Piessens, "Runtime countermeasures for code injection attacks against C and C++ programs," ACM Computing Surveys 44(3):1-28, June 2012 Lab1 assignment: Buffer Overflow
	25-Jan	Lec2b: Computer architecture background	Suggested reading: Chapter 2 and Appendix B in D. A. Patterson, "Computer architecture: A quantitative approach," 5th edition
3	30-Jan	Lec3a: Untrusted OS + History of secure processors	**Required** reading: (1) J. Rutkowska, "Intel x86 considered harmful," 2015 (2) "ORWL – The first open source, physically secure computer," https://www.crowdsupply.com/design-shift/orwl Suggested reading: Chapter 3.1 and 4 in T. W. Doeppner, "Operating Systems In Depth: Design and Programming"
	1-Feb	Lec3b: Introduction to Intel SGX, secure enclaves	**Due Lab1 (Buffer Overflow)** Lab2 assignment: Cache Controller Suggested reading: V. Coston and S. Devadas, "Intel SGX explained," https://eprint.iacr.org/2016/086.pdf
4	6-Feb	Lec4a: Life cycle of an SGX enclave	
	8-Feb	Lec4b: Public key infrastructure, Digital signature, Local and remote attestation, Quoting enclave	Suggested reading: Sections 10.1 -- 10.4, 12.1 – 12.7 in J. Katz and Y. Lindell, "Introduction to modern cryptography"

5	13- Feb	Lec5: Review session	**Due Lab2 (Cache Controller)**
	15-Feb	**Quiz (Weeks 1 to 5)**	
6	20-Feb	Lec6a: Lec4b cnt'd: AES, RSA, Hash, MAC	Suggested reading: Sections 4.1 – 4.7, 5.1 -- 5.5 in J. Katz and Y. Lindell, "Introduction to modern cryptography"
	22-Feb	Lec6b: Memory integrity checking: Merkle tree with caching, Intel's MAC Tree + Aegis (a secure processor architecture)	Lab3 assignment: Implementation of Merkle tree and MAC tree with caching + comparison **Required** reading: (1) R. Elbaz, D. Champagne, C. Gebotys, R. B. Lee, N. Potlapally, and L. Torres, "Hardware mechanisms for memory authentication: A survey of existing techniques and engines," Transactions on Computational Science IV, LNCS 5340, 2009 (2) G. E. Suh, D. Clarke, B. Gassend, M. van Dijk, and S. Devadas, "Efficient memory integrity verification and encryption for secure processors," MICRO 2003
7	27-Feb	Lec 7a: Sanctum: Memory striping, Security monitor, Secure bootstrapping	**Required** reading: V. Costan, I. Lebedev, and S. Devadas, "Sanctum: Minimal hardware extensions for strong software isolation," Usenix Security 2016
	1-Mar	Lec7b: Ascend: Architecture for secure computation on encrypted data + Oblivious RAM (ORAM): Write-only vs. fully functional + Timing channel	**Required** reading: S. H. Kamran and M. van Dijk, "Flat ORAM: A simplified write-only oblivious RAM construction for secure processor architectures," https://arxiv.org/pdf/1611.01571.pdf
8	6-Mar	Lec8a: Power side channel	
	8-Mar	Lec8b: Cache side channel + DMA attack	**Due Lab3 (Merkle and MAC tree)** Assignment Lab4: Cache side channel (demonstration and counter measure)
	13-Mar	SPRING BREAK	
	15-Mar	SPRING BREAK	
9	20-Mar	Lec9a: Data flow verification + Supply chain management	**Required** reading: C. Jin and M. van Dijk, "Secure and efficient initialization and authentication protocols for SHIELD," https://eprint.iacr.org/2015/210

	22-Mar	Lec9b: Hardware Trojan + Kleptography	**Required** reading: S. H. Haider, C. Jin, and M. van Dijk, "Advancing the state-of-the-art in hardware Trojan design," https://arxiv.org/abs/1605.08413
10	27-Mar	Lec10: Review session	**Due Lab4 (Cache side channel)**
	29-Mar	**Quiz (Weeks 6 to 10)**	
11	3-Apr	Lec11a: Physical Unclonable Functions (PUFs)	Lab5 assignment: Modeling attack XOR-Arbiter PUF
	5-Apr	Lec11b: Modeling attack on PUFs + Different adversarial models; Bad PUFs, reusable PUFs, communication PUFs	Suggested reading: To be written (details on modeling attacks on PUFs)
12	10-Apr	Lec12a: TRNG	
	12-Apr	Lec12b: Power grid	
13	17-Apr	Lec13a: Smart city	**Due Lab5 (Modeling attack)** Lab6 assignment: Essay on automotive security **Required** reading: E. Ronen and A. Shamir, "Extended functionality attacks on IoT devices: The case of smart lights," IEEE S&P 2016
	19-Apr	Lec13b: Isolation principle vs crypto + Hardware as a service	**Required** reading: J. Hennessey, C. Hill, I. Denhardt, V. Venugopal, G. Silvis, O. Krieger, and P. Desnoyers, "Hardware as a service – enabling dynamic, user-level bare metal provisioning of pools of data center resources," HPEC 2014
14	24-Apr	Lec14a: Voting machines + Secure JTAG + Reverse engineering	**Required** reading: S. Davtyan, A. Kiayias, L. Michel, A. Russel, and A. A. Shvartsman, "Integrity of electronic voting systems: Fallacious use of cryptography," SAC 2012
	26 apr	Lec14b: Bitcoin hardware + Medical devices	**Due Lab6 (Automotive security)** **Required** reading: (1) M. B. Taylor, "Bitcoin and the age of bespoke silicon," CASES 2013

			(2) D. Kotz, K. Fu, and A. Rubin, "Security for mobile and cloud frontiers in healthcare," Communications of the ACM, 2015
	1-May	**Final (Weeks 11 to 14)**	

Disclaimer: The course schedule is subject to change.

Collaboration policy: You are encouraged to collaborate and study together. In fact, students who form study groups generally do better than do students who work alone. If you do work in a study group, however, you owe it to yourself and your group to be prepared for your study group meeting. Specifically, you should spend at least 30-45 minutes trying to understand lecture material and solve any of the open questions beforehand. If your group is unable to solve a problem, talk to other groups or ask the instructor.

Grade:

- Quiz1, Quiz2, and Final each count for 20%
- The 6 labs each count for 7% (this implies 2% bonus)

Grade conversion is done according to the following table:

Range of A minus penalty:	Letter grade:
91 - 100	A (excellent)
89 - 90	A-
87 - 88	B+ (very good)
81 - 86	B (good)
79 - 80	B-
77 - 78	C+
71 - 76	C (average)
69 - 70	C- (fair)
67 - 68	D+ (poor)
61 - 66	D
59 - 60	D- (merely passing)
Under 59	F (Failure)

The grading scheme may be adapted to a different one if needed.

Sec. 10a-50. (Formerly Sec. 10-334g). Absence of students

Students should inform their instructor about any potential conflicts with scheduled exams or other

assignments and a religious holiday that they observe. For conflicts with final examinations, students should, as usual, contact the Office of Student Services and Advocacy (formerly the Dean of Students Office). Faculty and instructors are strongly encouraged to make reasonable accommodations in response to student requests to complete work missed by absence resulting from religious observances or participation in extra-curricular activities that enrich their experience, support their scholarly development, and benefit the university community. Examples include participation in scholarly presentations, performing arts, and intercollegiate sports, when the participation is at the request of, or coordinated by, a University official. Such accommodations should be made in ways that do not dilute or preclude the requirements or learning outcomes for the course. Students anticipating such a conflict should inform their instructor in writing within the first three weeks of the semester, and prior to the anticipated absence, and should take the initiative to work out with the instructor a schedule for making up missed work. For conflicts with final examinations, students should contact the Office of the Dean of Students.

Faculty and instructors are also encouraged to respond when the Counseling Program for Intercollegiate Athletes (CPIA) requests student progress reports. This will enable the counselors to give our students appropriate advice.

Disabilities: The Center for Students with Disabilities (CSD) at UConn provides accommodations and services for qualified students with disabilities. If you have a documented disability for which you wish to request academic accommodations and have not contacted the CSD, please do so as soon as possible. The CSD is located in Wilbur Cross, Room 204 and can be reached at (860) 486-2020 or at csd@uconn.edu. Detailed information regarding the accommodations process is also available on their website at www.csd.uconn.edu.

Let the instructor know as soon as possible if you need adaptations or accommodations because of a disability (e.g. learning disability, attention deficit disorder, psychological, physical), or if you have emergency medical information which you should share with the instructor, or if you need special arrangements in case the building must be evacuated.

Policy Against Discrimination, Harassment and Related Interpersonal Violence: The University is committed to maintaining an environment free of discrimination or discriminatory harassment directed toward any person or group within its community – students, employees, or visitors. Academic and professional excellence can flourish only when each member of our community is assured an atmosphere of mutual respect. All members of the University community are responsible for the maintenance of an academic and work environment in which people are free to learn and work without fear of discrimination or discriminatory harassment. In addition, inappropriate amorous relationships can undermine the University's mission when those in positions of authority abuse or appear to abuse their authority. To that end, and in accordance with federal and state law, the University prohibits discrimination and discriminatory harassment, as well as inappropriate amorous relationships, and such behavior will be met with appropriate disciplinary action, up to and including dismissal from the University. Additionally, to protect the campus community,

all non-confidential University employees (including faculty) are required to report sexual assaults, intimate partner violence, and/or stalking involving a student that they witness or are told about to the Office of Institutional Equity. The University takes all reports with the utmost seriousness. Please be aware that while the information you provide will remain private, it will not be confidential and will be shared with University officials who can help. More information is available at http://equity.uconn.edu and http://titleix.uconn.edu.

Sexual Assault Reporting Policy: To protect the campus community, all non-confidential University employees (including faculty) are required to report assaults they witness or are told about to the Office of Diversity & Equity under the Sexual Assault Response Policy. The University takes all reports with the utmost seriousness. Please be aware that while the information you provide will remain private, it will not be confidential and will be shared with University officials who can help. More information is available at http://sexualviolence.uconn.edu/.