Georgia Institute of Technology

Course Syllabus: ECE 8843 Side-Channels and Their Role in Cybersecurity

Spring 2021, ECE8843-OCY	School of Electrical and Computer Engineering, COE
Delivery: 100% Web-Based, Asynchronous	LMS for Content Delivery [to include video, all activities and assessments]
Dates course will run: [Jan. 14- May 6, 2021]	

Instructor Information

Alenka Zajic, Associate Professor	Email: Alenka.zajic@ece.gatech.edu
Milos Prvulovic, Professor	Email: milos@cc.gatech.edu
Weekly Office Hours via Blue Jeans Wednesdays 11-noon EST	

General Course Information

Description

The primary objective of this course is to provide an in-depth treatment of digital and analog side-channels and their use for attacks and defenses in cyber security. Upon completion of the course, the student will have a high degree of confidence in discussing the fundamental mechanisms of side-channel creation, analysis, and application to various cybersecurity problems, and have competence in considering these mechanisms during software and hardware development.

Pre- &/or Co-Requisites

Suggested prerequisites are graduate standing and some background in high performance computer architecture (e.g. ECE 4100/6100)

Course Goals and Learning Outcomes

As part of this course, students:

1. Will gain an insight into side-channels, how they are created and used in cybersecurity
2. Will learn and practice how to exploit digital and analog side-channels for cybersecurity
3. Will learn and practice how to analyze side-channels for program monitoring and supply chain verification

Course Learning Outcomes

Once completed, the students should have the following capabilities:

- A high degree of confidence and competence in discussing the fundamental mechanisms of side-channel creation, analysis
- A high degree of confidence and competence in applying side-channels to various cybersecurity problems.

Course Materials

Course Website and Other Classroom Management Tools

This class will use Canvas, a Learning Management System (LMS), for all announcements, project assignments, project submission, exams, and posting of scores and grades. We will also use Piazza for questions about the course material, discussions, etc. More details about submitting projects,

taking exams, etc. will be announced (via Canvas announcements) during the semester, as we release the projects and exams.

Course Requirements, Assignments & Grading

Assignment Distribution

Grading Type	Description of Graded Assignments	% Grade	Timing
Two Midterm Tests	Midterm Tests assess knowledge acquired in the first and second half of semester	40%	50 min each
Six Projects	Detailed description provided in Activities/Assignments	60%	2-3 weeks

Grading Scale

Your final grade will be assigned as a letter grade according to the following scale:

A 90-100%
B 80-89%
C 70-79%
D 60-69%
F 0-59%

Description of Graded Components

Midterm Tests: There are two midterm tests in this course. The midterm tests are designed to test knowledge acquired in the first and second half of semester. The exams are closed book and proctored.
Six Projects (10% of each): In addition to two midterms, there will be six projects each weighted 10% of the grade. Each project will require careful time allocation to complete on time (2-3 weeks). More details about projects will be posted in Canvas

Submitting Assignments

The midterm tests need to be taken in Canvas during the exam windows described above.
The projects must be completed and submitted in Canvas by the due date stated in the course schedule.

Assignment Due Dates

All assignments are due at the times listed in the course schedule. These times are subject to change so please check back often. Please convert from UTC to your local time zone using a Time Zone Converter.

Late and Make-up Work Policy

All projects must be submitted by their due time. Submissions that are up to 24 hours late will be accepted without penalty, submissions that are more than 24 but less than 48 hours late will be accepted with 50% penalty, and no submissions will be accepted if they are more than 48 hours late.

A student can begin taking a midterm test after the test "opens" in Canvas. A student's test completion is considered late if it occurs after the test's "due" time in Canvas. Tests that are completed up to 24 hours late will be accepted without penalty, test completions that are more than

24 hours but less than 48 hours late will be accepted with a 50% penalty, and no test completions will be accepted more than 48 hours after a test's due time.

Students should submit their projects and complete their tests on time. Students who submit projects or complete tests late **assume all of the risk** associated with technical, medical, and other problems, even when these problems are beyond their control. For example, if Canvas experiences a 48-hour downtime that begins a few minutes after a project is due, no late submissions will be possible. Similarly, if a s student experiences a health problem that affects them after the due time of a project (or "closing" time of an exam), no extension to the 24-hour-late and 48-hour-late submission cutoff times will be granted.

No make-up work will be available, i.e. the students' grades will be based solely on the two tests and six projects, and no additional assignments will be created to help students improve their grades.

The only exception to these late and make-up work policies are:
1) Accommodations approved by the Dean of Students, e.g. as a result of illness and other emergencies, and
2) Accommodations that were discussed with, and approved by, the instructor ahead of time. Specifically, the need for these accommodations should be brought to the instructor's attention **during the first week of the semester**, or as soon as possible if the need for an accommodation was not known to the student at the beginning of the semester.

Proctoring Information

Honorlock is utilized for student identity verification and to ensure academic integrity. Honorlock provides student identity verification via facial and ID photos. You may also be asked to scan the room around you. For proctored exams, Honorlock employs AI technology to notify course instructors of potential academic integrity violations. Course instructors are able to review video of the potential violations and resolve potential academic integrity issues. For each course in which the Honorlock is used, you will have the opportunity to take an on-boarding test so you are familiar with how it works.

While Honorlock will not require you to create an account, download software, or schedule an appointment in advance, you will need Google Chrome and download the Honorlock Chrome Extension.

Technology Requirements and Skills

Computer Hardware and Software

- High-speed Internet connection
- Laptop or desktop computer with a **minimum** of a 2 GHz processor and 2 GB of RAM
- Windows for PC computers OR Mac iOS for Apple computers.
- Complete Microsoft Office Suite or comparable and ability to use Adobe PDF software (install, download, open and convert)
- Mozilla Firefox, Chrome and/or Safari browsers

Technology Skills

To be successful in this course, students should

- Be able to modify existing and write new programs in C/C++
- Have some familiarity with operating system (OS) functionality, and be able to use some of that functionality (e.g. clock_gettime or gettimeofday) from within C/C++ programs,
- Be able to edit, compile, debug, and run programs in Linux,
- Have some familiarity with assembler-level programming, i.e. be able to follow program code examples that use assembler code
- Have at least some understanding of processor architecture, e.g. the concepts of virtual memory, caches, pipelines, etc.

Technology Help Guidelines

30-Minute Rule: When you encounter struggles with technology, give yourself 30 minutes to 'figure it out.' If you cannot, then post a message to the discussion board; your peers may have suggestions to assist you. You are also directed to contact the Helpdesk 24/7.

When posting or sending email requesting help with technology issues, whether to the Helpdesk, message board, or me use the following guidelines:

- Include a descriptive title for the subject field that includes 1) the name of course 2) the issue. Do NOT just simply type "Help" into the subject field or leave it blank.
- List the steps or describe the circumstance that preceded the technical issue or error. Include the exact wording of the error message.
- When possible, always include a screenshot(s) demonstrating the technical issue or error message.
- Also include what you have already tried to remedy the issue (rebooting, trying a different browser, etc.).

Course Policies, Expectations & Guidelines

Communication Policy

- Questions should be submitted in Piazza. Questions about grading, questions that discuss your solution to a still-open project, etc. should be submitted as a private post in Piazza. Questions of a personal nature, e.g. questions about accommodations for disabilities and medical problems, should be submitted directly to the instructor via email, using your university-assigned email account.
- Office hours will be held every **Wednesday from 11am to noon**, using BlueJeans. However, for some weeks the instructor may need to cancel or modify the office hours, and these cancellations and modifications will be communicated via announcements in Canvas.

Online Student Conduct and (N)etiquette

Communicating appropriately in the online classroom can be challenging. In order to minimize this challenge, it is important to remember several points of **"internet etiquette"** that will smooth communication for both students and instructors:

1. *Read first, Write later*. Read the ENTIRE set of posts/comments on a discussion board before posting your reply, in order to prevent repeating commentary or asking questions that have already been answered.
2. *Avoid language that may come across as strong or offensive*. Language can be easily misinterpreted in written electronic communication. Review email and discussion board posts BEFORE submitting. Humor and sarcasm may be easily misinterpreted by your reader(s). Try to be as matter-of-fact and professional as possible.

3. *Follow the language rules of the Internet*. Do not write using all capital letters, because it will appear as shouting. Also, the use of emoticons can be helpful when used to convey nonverbal feelings. ☺
4. *Consider the privacy of others.* Ask permission prior to giving out a classmate's email address or other information.
5. *Keep attachments small*. If it is necessary to send pictures, change the size to an acceptable 250kb or less (one free, web-based tool to try is picresize.com).
6. *No inappropriate material*. Do not forward virus warnings, chain letters, jokes, etc. to classmates or instructors. The sharing of pornographic material is forbidden.

NOTE: The instructor reserves the right to remove posts that are not collegial in nature and/or do not meet the Online Student Conduct and Etiquette guidelines listed above.

University Use of Electronic Email

A university-assigned student e-mail account is the official university means of communication with all students at Georgia Institute of Technology. Students are responsible for all information sent to them via their university-assigned e-mail account. If a student chooses to forward information in their university e-mail account, he or she is responsible for all information, including attachments, sent to any other e-mail account. To stay current with university information, students are expected to check their official university e-mail account and other electronic communications on a frequent and consistent basis. Recognizing that some communications may be time-critical, the university recommends that electronic communications be checked minimally twice a week.

Plagiarism & Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. All students enrolled at Georgia Tech, and all its campuses, are to perform their academic work according to standards set by faculty members, departments, schools and colleges of the university; and cheating and plagiarism constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted and will be applied. For information on Georgia Tech's Academic Honor Code, please visit http://www.catalog.gatech.edu/policies/honor-code/ or http://www.catalog.gatech.edu/rules/18/.

Any student suspected of cheating or plagiarizing on a quiz, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services at (404)894-2563 or http://disabilityservices.gatech.edu/, as soon as possible, to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail me as soon as possible in order to set up a time to discuss your learning needs.

Collaboration & Group Work

You are encouraged to form virtual groups to discuss topics covered in class. Such discussion can enhance learning and could include clarifications of questions related to a topic or a project. However, individual work that you submit as part of an assessment and claim as yours must be yours.

All work for this class is to be done individually. You are strongly urged to familiarize yourself with the **GT Student Honor Code (Links to an external site.) rules. Specifically, the following is not allowed:**

- Copying, with or without modification, someone else's work when this work is not meant to be publicly accessible *(e.g., a classmate's program or solution).*
- Submission of material that is wholly or substantially identical to that created or published by another person or persons, without adequate credit notations indicating authorship *(plagiarism).*
- Putting your projects on public Github. If a student in the future copies your code/reports, the student obviously violates the honor code but you will also be responsible for the violation.

Any public material that you use *(open-source software, help from a text, or substantial help from a friend, etc...)* should be acknowledged explicitly in anything you submit. If you have any doubt about whether something is allowed or not, please do check with the class Instructor or the TA.

Extensions, Late Assignments, & Re-Scheduled/Missed Exams

All projects must be submitted by their due time. Submissions that are up to 24 hours late will be accepted without penalty, submissions that are more than 24 but less than 48 hours late will be accepted with 50% penalty, and no submissions will be accepted if they are more than 48 hours late.

Student-Faculty Expectations Agreement

At Georgia Tech we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and the student body. See http://www.catalog.gatech.edu/rules/22/ for an articulation of some basic expectation that you can have of me and that I have of you. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Therefore, I encourage you to remain committed to the ideals of Georgia Tech while in this class.

Course Schedule

Subject to Change Statement

The syllabus and course schedule may be subject to change. Changes will be communicated via Canvas announcement. It is the responsibility of students to check email messages and course announcements to stay current in their online courses.

Week	Dates	Topics
1	Jan 14-22	Side Channels - what are they and what kinds are there
	Jan 18	Official School Holiday
2	Jan 25-29	Input/Output-Observable Side Channels
	Jan 27	Project 1 Released
3	Feb 1-5	Software-Observable Side Channels
	Feb 3	Project 2 Released
4	Feb 8-12	Software-Observable Side-Channels Beyond Resource Contention
	Feb 10	Project 1 Due at midnight AOE (GMT-12)
5	Feb 15-19	Physically Observable Side Channels
	Feb 17	Project 3 Released
6	Feb 22-26	More about Physically Observable Side Channels
	Feb 24	Project 2 Due at midnight AOE (GMT-12)
7	Mar 1-5	Parameters that Affect Physically Observable Side Channels
	Mar 3	Project 4 Released
	Mar 5-7	Midterm Test 1 (2-hour proctored exam)

Week	Dates	Topics
8	Mar 8-12	Fine-Grained Analysis of Physically Observable Side-channels
	Mar 10	Project 3 Due at midnight AOE (GMT-12)
9	Mar 15-19	Software-Created Covert Channels
	Mar 16	No classes
	Mar 17	Last day to drop course with "W" grade
	Mar 17	Project 5 Released
10	Mar 22-26	Fault Injection Attacks
	Mar 24	Project 6 Released
	Mar 25	Project 4 Due at midnight AOE (GMT-12)
	Mar 24	No classes
11	Mar 29-Apr 2	Backscattering Side Channels
12	Apr 5-9	Using Side Channels for Hardware Trojan Detection
	Apr 7	Project 5 Due at midnight AOE (GMT-12)
13	Apr 12-16	Historical Overview of Software-Visible Side-channel Attacks
14	Apr 19-23	Historical Overview of physically observable side-channel Attacks
	Apr 21	Project 6 Due at midnight AOE (GMT-12)
15	Apr 26-27	Review and Prepare for Exams
	April 28	Reading Day (Prepare for Exams)
16	Apr 30- May 2	Midterm Test 2 (2-hour proctored exam)

Course Outline

WEEK #1:

Title: What are side-channels and their classification
Week Overview: Define side-channels. Describe II/O-observable, software-observable (timing, resource oriented, speculative execution) and physically-observable (EM, power, acoustic, temperature, backscattering) side-channels.

Week Objectives: At the end of this lesson, you will be able to:

- Define side-channels
- Classify side-channels
- Describe differences between software visible and hardware/software produced side-channels
- Define properties of software visible and hardware/software produced side-channels

Pre-Readings:

- none

Week 1 e-Lecture Lessons	Week 1 Activities/ Assessments
1. What are side-channels 2. What are I/O-observable side-channels 3. Execution timing example 4. What are software-observable side-channels 1-2 5. Resource oriented side-channels (cache, memory) 6. Speculative execution 7. What are physically-observable side-channels 8. Examples of passive physically-observable side-channels 9. Examples of active physically-observable side-channels	• Knowledge check quiz after the video lessons for this week

WEEK #2

Title: Input/Output-Observable Side-channels
Week Overview: Introduction into I/O timing side-channels. Malicious uses of timing side-channels. Benign uses of timing side-channels (SW attestation example).

Week Objectives: At the end of this lesson, you will be able to:

- Define (termination) timing side-channels
- Explain (and provide examples of) information leakage through timing side-channels
- Explain (and provide an example of) benign uses of timing side-channels

Pre-Readings:

- none

Week 2 e-Lecture Lessons	Week 2 Activities/ Assessments
1. What are I/O observable side-channels? 2. Example over-the-internet attack scenario 3. Mitigation of timing side-channel risks 4. Attacks via I/O observable side-channels 5. Benign uses of I/O-observable side-channels	• Knowledge-check quiz after the video lessons for this week • Project 1 Release: Attack on a Password Checker In this project the students use the execution time as a side channel to recover a secret password. We implement a set of password checkers that compare the entered password to a student-specific password character by character, and students need to use the execution time side channel to discover the secret password. The set of password checkers have different time-per-character, form pretty long (easy to break) to pretty short (hard to break), and the score is based on how many of these the student did break.

WEEK #3

Title: Software-Observable Side-channels
Week Overview: Introduction into different software-observable side-channels and detailed explanation of side-channels based on resource contention, suing cache-based side-channels as an example.

Week Objectives: At the end of this lesson, you will be able to:

- Categorize software-observable side-channels
- Explain the general principles of operation for side-channels based on resource contention
- Provide detailed examples of a cache-based side channel attack

Pre-Readings:

- none

Week 3 e-Lecture Lessons	Week 3 Activities/ Assessments
1. Introduction into software-observable side-channels 2. Co-location of attacker's and victim's program 3. Performance events and resource contention 4. Shared cache as a side channel 5. Other software-observable side-channels	• Knowledge check quiz after the video lessons for this week • Project 2 Release: Cache Side Channel Attack In this project the students use the shared cache as a side channel to recover a secret RSA key. On our server, an RSA implementation that is susceptible to cache attacks is repeatedly performing encryption with a secret RSA key, one per student. The students are each given a shared key and are asked to recover the secret key that corresponds to it. They are supposed to write a program that will run co-located with the RSA code on the server. The score is based on how many bits of the key are recovered.

WEEK #4

Title: Software-Observable Side-Channels Beyond Resource Contention
Week Overview: We continue discussion of software-observable side-channels, focusing on side-channels that leverage speculative execution and resource management
Week Objectives: At the end of this lesson, you will be able to:

- Explain how speculative execution helps side channel attacks
- Explain the operation of Spectre, Meltdown, and related attacks.
- Explain (and provide examples of) how resource management within the computer system can create side channel vulnerabilities
- Explain how the resource usage side-channels can be used to detect anomalies in the system's operation

Pre-Readings:

- none

Week 4 e-Lecture Lessons	Week 4 Activities/ Assessments
1. Mitigation for traditional attacks 2. What are speculation-assisted attacks 3. Speculation-assisted attack example 4. Resource and power management 5. Benevolent uses	• Knowledge check quiz after the video lessons for this week • Project 1 due

WEEK #5

Title: Physically Observable Side-channels
Week Overview: We start discussion on physically observable side-channels, focusing on side-channels that leverage low frequency range (0-50 MHz)
Week Objectives: At the end of this lesson, you will be able to:

- Explain how physically observable side-channels are created
- Explain relationship between physically observable signals and performing computation

- Explain (and provide examples of) time-domain signal analysis for low-frequency signals
- Explain traditional methods for cryptography side-channel attacks such as SEMA, DEMA

Pre-Readings:

- none

Week 5 e-Lecture Lessons	Week 5 Activities/ Assessments
1. Physical side-effects of performing computation (EM, power, temperature, optical variation) 2. Power side channel 3. Low frequency EM side channel 4. Example - program execution and EM side channel signals 5. EM and power side-channels created by voltage regulators 6. Other observables: temperature, acoustic, chassis potential 7. Simple power-EM analysis attacks 8. Differential power-EM analysis attacks	• Knowledge check quiz after the video lessons for this week • Project 3 Release: Differential Electromagnetic Analysis on RSA algorithm In this project the students use differential electromagnetic analysis to recover a secret RSA key. They are given a real EM signal that corresponds to an encryption using an RSA secret key They are asked to implement differential electromagnetic analysis algorithm that can recover the secret key. The score is based on how many bits of the key they recover.

WEEK #6

Title: Other Physically Observable Side-channels
Week Overview: We continue discussion on physically observable side-channels, focusing on side-channels that leverage modulated frequencies (500 MHz – 2 GHz)
Week Objectives: At the end of this lesson, you will be able to:

- Explain how modulated physically observable side-channels are created
- Explain relationship between physically observable modulated signals and performing computation
- Explain (and provide examples of) frequency-domain signal analysis for high-frequency signals
- Perform program loop tracking using frequency-domain machine-learning

Pre-Readings:

- none

Week 6 e-Lecture Lessons	Week 6 Activities/ Assessments
1. Electromagnetic emanations 2. AM, FM modulated signals 3. How side-channels get modulated onto digital logic, clocks, etc. 4. Example: Digital logic, clocking, and modulated EM side channel signals 5. “Screaming” side-channels 6. SAVAT 7. Monitoring program loop activities	• Knowledge check quiz after the video lessons for this week • Project 2 due • The first midterm exam

8. Spectral monitoring of side-channel signals	

WEEK #7

Title: Parameters that Affect Physically Observable Side-channels
Week Overview: We discuss parameters that impact physically observable channels such as bandwidth, distance, sensitivity, antenna gain, etc.
Week Objectives: At the end of this lesson, you will be able to:

- Explain how bandwidth impacts side-channel capacity
- Explain how sampling rate impacts side-channel capacity
- Explain how distance (gain, directionality, frequency selectivity, probes and antennas) impact side-channels

Pre-Readings:

- none

Week 7 e-Lecture Lessons	Week 7 Activities/ Assessments
1. Brief intro to channel capacity (Shannon mostly) 2. Definition of signal bandwidth and sampling rate 3. Thermal noise, power supply noise, signal to noise ratio 4. How bandwidth and sampling rate impact side-channel measurements 5. An example of bandwidth and sampling rate impact on side-channel signal 6. Distance (gain, directionality, frequency selectivity, probes and antennas) 7. How distance affects EM side channel results 8. Distance demos/examples and through wall demos/examples	• Knowledge check quiz after the video lessons for this week • Project 4 Release: Program Tracking via the EM Side Channel In this project the students use spectral analysis to recover a secret RSA key. They are given a real EM signal that corresponds to an encryption using an RSA secret key in a double-and-add implementation of RSA (with a key that is large enough to allow double and add to show up in the spectrogram, and are also given the corresponding public key. They are asked to implement program tracking (find occurrences of double and add) that can recover the secret key. The score is based on how many bits of the key they recover.

WEEK #8

Title: Fine-Grained Analysis of Physically Observable Side-channels
Week Overview: We will use time-domain and frequency-domain signals to detect various sizes of malware intrusion as well as track program execution.
Week Objectives: At the end of this lesson, you will be able to:

- Detect various sizes of malware intrusion using side-channels
- Track program execution using side-channels at various levels of granularity

Pre-Readings:

- none

Week 8 e-Lecture Lessons	Week 8 Activities/ Assessments
1. Frequency-domain analysis of EM side-channel signals 2. Example: EDDIE 3. Time-domain analysis of EM side-channel signals 4. Machine-learning techniques for EM side-channel signal tracking 5. Speech recognition techniques EM side-channel analysis 6. Neural network techniques for EM side-channel analysis	• Knowledge check quiz after the video lessons for this week • Project 3 due

WEEK #9

Title: Software Created Covert Channels
Week Overview: We will discuss several ways messages can be sent via software-created covert channel. We will also discuss how this channel can be modelled as wireless communication channel and what is capacity of such a channel.
Week Objectives: At the end of this lesson, you will be able to:

- Create covert side-channels that can leak information
- Explain software-modulation process that creates covert channel
- Estimate capacity of these channels

Pre-Readings:

- none

Week 9 e-Lecture Lessons	Week 9 Activities/ Assessments
1. Introduction to software created covert channels 2. An example of covert channels 3. Through wall demo 4. Modeling side/covert channel 5. Estimation of capacity in covert channels	• Knowledge check quiz after the video lessons for this week • Project 5 release: EM covert channel In this project students are given a non-leaky implementation of RSA and the EMSim (simulator of analog side channel signal). They can modify the RSA code to leak the key through the EM side channel, and they need to write the code that takes the (simulator-generated) EM signal and recovers the entire RSA key. The score is based on the edit distance between the original and the new RSA code.

WEEK #10

Title: Fault Injection Attacks

Week Overview: We introduce the concept of fault injection attacks
Week Objectives: At the end of this lesson, you will be able to:

- Define fault injection attacks and describe their general method of operation
- Identify viable approaches for implementing a basic fault-injection attack on a system that has predictable (faulty) behavior after a fault has been introduced

Pre-Readings:

- None
-

Week 10 e-Lecture Lessons	Week 10 Activities/ Assessments
1. Hardware faults and their effects 2. Using faults to cause information leakage 3. Example: A fault-injection attack on RSA	• Knowledge check quiz after the video lessons for this week • Project 4 due • Project 6 Release: Error Injection Side-Channel In this project, students work with a simulator that executes side-channel resistant RSA encryption, and they can inject bit-flips (specified as <exe-unit, bit-position, cycle-number> tuples) into the outputs of execution units within the processor, and they get the outputs of the encryption. The goal is to recover the RSA key.

WEEK #11

Title: Backscattering Side-channels
Week Overview: We introduce new physical side-channel called backscattering side-channel and explain how it differs from other physically observable side-channels.
Week Objectives: At the end of this lesson, you will be able to:

- Explain new concepts related to backscattering side-channels
- Explain benefits of using this side-channel for sub-clock cycle computer system monitoring

Pre-Readings:

- none

Week 11 e-Lecture Lessons	Week 11 Activities/ Assessments
1. Physical concepts related to backscattering 2. Reflection coefficient and impedance 3. How backscattering signals pick up side-modulated side-channel signals from digital logic. 4. Example: digital logic, clocking, and modulated backscattering side channel signals 5. Example: program execution and backscattering side channel signals 6. How input power, frequency, and distance affects backscattering side channel results	• Knowledge check quiz after the video lessons for this week

WEEK #12

Title: Hardware Trojan Detection
Week Overview: Brief overview of Hardware Trojans (a.k.a. Hardware Trojan Horses). Side-channels as a method for detecting Hardware Trojans, with examples that leverage circuit timing, power/current consumption, electromagnetic emanations, and back-scattering.
Week Objectives: At the end of this lesson, you will be able to:

- Define Hardware Trojans, describe their basic operation and security risks they case.
- Describe how a Hardware Trojan affects physically observable side-channel signals of the affected digital circuit
- Describe the advantages and disadvantages of detecting Hardware Trojans by measuring timing of various paths within a digital circuit
- Describe the advantages and disadvantages of detecting Hardware Trojans by measuring power/current/voltage during operation of a digital circuit
- Describe the advantages and disadvantages of detecting Hardware Trojans using the back-scattering side channel

Pre-Readings:

- None

Week 12 e-Lecture Lessons	Week 12 Activities/ Assessments
1. What are hardware Trojans (HT) 2. HT triggering and payloads 3. Overview of methods for HT detection 4. How HTs affect side channel signals (delays, power, EM, impedance) 5. Delay-based detection of HTs 6. Backscattering-based detection of HTs 7. Power, EM-based detection of HTs	• Knowledge check quiz after the video lessons for this week • Project 5 due

WEEK #13

Title: Historical Overview of Software-Visible Side-channel Attacks

Week Overview: How cryptographic implementations have evolved in response to software-visible side channel attacks. Details of specific attacks and mitigations for RSA implementations. Secure enclave implementation, attacks, and mitigation.
Week Objectives: At the end of this lesson, you will be able to:

- Describe how specific categories of software-visible side channel attacks have influenced the modern implementations of cryptographic primitives.
- Describe key ideas for constructing side-channel resilient cryptographic implementations
- Explain the purpose and ideas behind secure enclave technology
- Describe several specific attacks against secure enclaves and how they can be mitigated

Pre-Readings:

- None

Week 13 e-Lecture Lessons	Week 13 Activities/ Assessments
1. Historical overview of cache-based side-channel attacks 2. Historical overview of cache-based side-channel attacks – Part 2 3. Historical overview of cache-based side-channel attacks – Part 3	• Knowledge check quiz after the video lessons for this week • Project 6 due

WEEK #14

Title: Historical Overview of physically observable side-channel Attacks
Week Overview: How cryptographic implementations have evolved in response to physical side channel attacks. Details of specific attacks and mitigations for RSA implementations. Details on how ECC implementations have leveraged the lessons learned from RSA.
Week Objectives: At the end of this lesson, you will be able to:

- Describe how specific categories of analog side channel attacks have influenced the modern implementations of cryptographic primitives
- Describe key ideas for constructing side-channel resilient cryptographic implementations
- Describe how attacks and mitigations for one cryptosystem (RSA can influence implementations of another cryptosystem (ECC)

Pre-Readings:

- none

Week 14 e-Lecture Lessons	Week 14 Activities/ Assessments
• Historical overview of analog attacks on RSA • Differential power analysis attacks on RSA • Chosen Chipertext Attacks on RSA • One&Done – fine-grained attacks on RSA	• Knowledge check quiz after the video lessons for this week • The second midterm exam