# Side-Channels and Their Role in Cybersecurity
# ECE 8843

## Class Description:

| Course | Title | Cr Hrs | Instructor | Days | Time | Location |
|---|---|---|---|---|---|---|
| ECE-88xx | Side-Channels in Cybersecurity | 3-0-3 | Alenka Zajic/Milos Prvulovic | | | |

| ECE 8803 Side-Channels and Their Role in Cybersecurity |
|---|
| This class provides 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 and competence in discussing the fundamental mechanisms of side-channel creation, analysis, and application to various cybersecurity problems. |

**Instructors:** Alenka Zajic (ECE) and Milos Prvulovic (CS)

**Textbook:** Course notes will be posted online.

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

## Grading:

20% Homework – Expect approximately 4 homework assignments over the course of the semester.

20% Midterm Quiz

40% Three Projects

20% Final exam

### Course Objectives

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 Educational Outcome:

Upon completion of the course, the student will have a high degree of confidence and competence in discussing the fundamental mechanisms of side-channel creation, analysis, and application to various cybersecurity problems.

## Tentative Lecture Topics:

I. **What are side-channels and their classification** – One or two lectures will be spent reviewing software visible (timing, resource oriented, speculative execution) and hardware/software produced (EM, power, acoustic, temperature, backscattering) side-channels.

II. **Covert channels** – One or two lectures will be spent on reviewing covert channels - amplification of side-channels, fault injection, hardware Trojans, etc.

III. **Use of side-channels** – Classification of side channels into malicious use (side-channel attacks, covert channels) and benign use (program monitoring, counterfeit detection, reverse engineering).

IV. **How software-visible side-channels work** – Timing side-channel, cache side-channel, speculative execution, other resource oriented side-channels.

V. **How analog side-channels work** – Relationship between hardware operation and observed analog signals, relation between hardware/software interaction and observed analog signals, relationship between program activity and observed analog signals. In-depth treatment of relationship between baseband signals, modulated signals, available bandwidth vs. sampling rate, etc.

VI. **Side-channel attacks** – Brief history of digital and analog side-channel attacks, in-depth treatment of one digital and one analog attack example.

VII. **Side-channel based program monitoring** – Various granularities of program execution monitoring (from distinguishing between two programs, to tracking program executions on basic-block and individual instruction levels) will be analyzed though examples of published articles.

VIII. **Side-channel based hardware Trojan detection** – Brief history and methods of hardware Trojan detection, in-depth analysis of side-channels and their role in hardware Trojan detection.

IX. **Side-channel based software reverse engineering** – Brief history and methods of software reverse engineering, digital and analog side-channels and their role in software reverse engineering, in-depth analysis of signal processing methods for software reverse engineering.

**Academic Honor Code:** The Honor Code applies to every aspect of this class, with only one noteworthy exception: student discussion of concepts and techniques for solving homework problems is permitted and even encouraged outside the classroom. However, *all submitted work must be original*. More details on academic honor code can be found at: http://www.policylibrary.gatech.edu/student-affairs/academic-honor-code

**Access and Accommodations:** At Georgia Tech we strive to make learning experiences as accessible as possible. If you anticipate or experience physical or academic barriers based on disability, you are welcome to let me know so that we can discuss options. You are also encouraged to contact the Office of Disability Services to explore reasonable accommodations. More details can be found at: https://disabilityservices.gatech.edu/

**Absence Policy:** The class will follow institute absence policy detailed at http://www.catalog.gatech.edu/rules/4/