

# Security and Privacy, SCS Concentration

## Security & Privacy Concentration

**This concentration is available to SCS students only. (ECE students should consult their department for an equivalent concentration.)**

Lujo Bauer, *Concentration Director and Advisor*  
Location: CIC 2203

In a world where data breaches and cyber-attacks are ever-present, the need for technologists who have a solid understanding of the principles that underlie strong security and privacy practices is greater than ever.

The Security & Privacy concentration is designed to expose students to the key facets of and concerns about computer security and privacy that drive practice, research, and legislation. On completing the curriculum, students are well prepared to continue developing their interests in security or privacy through graduate study; to take jobs in security or privacy that will provide further training in applicable areas; and to be informed participants in public and other processes that shape how organizations and society develop to meet new challenges related to computer security or privacy.

## Learning Objectives

After completing this concentration, students should:

- Understand how to reason about the adversary in computer systems.
- Be familiar with common security vulnerabilities, from buffer overflows and return oriented programming to cross-site scripting, and widely deployed defenses against these vulnerabilities.
- Be familiar with and understand how to apply the basic concepts in cryptography and secure system design and analysis.
- Understand the key properties of commonly used cryptographic primitives and properties commonly desired of cryptographic protocols.
- Be familiar with current and upcoming research directions in secure system design, software analysis, and cryptography.
- Be familiar with the breadth of concerns and topics relevant to computer security and privacy, ranging from technical topics to ethics, regulation, usability, and economics.
- Be familiar with the key concepts in privacy, ranging from conceptions of privacy to privacy algorithms to regulation and policy.
- Gain a more in-depth understanding of one “context” area: usable security and privacy, or policy.

## Curriculum

### Prerequisites

Students interested in pursuing this concentration should have the following courses completed before starting the concentration:

|        |                                               |    |
|--------|-----------------------------------------------|----|
| 15-151 | Mathematical Foundations for Computer Science | 12 |
| 15-213 | Introduction to Computer Systems              | 12 |
| 15-251 | Great Ideas in Theoretical Computer Science   | 12 |

### Course Requirements

A distinguishing feature of this field is the ubiquitous need to consider an adversary, and the resulting interplay between attack and defense that routinely advances both theory and practice. In order to understand widely-deployed defensive techniques and secure-by-design approaches, students must also understand the attacks that motivate them and the “adversarial mindset” that leads to new forms of attack. The curriculum is designed around this principle.

Students in the Security & Privacy concentration take courses that cover the basic principles (*Introduction and Basics Course Area*), the underlying theory (*Theoretical Foundations Course Area*), and the practical application (*System Design Course Area*) of security and privacy. Additionally, students are required to select a course which covers either usability or policy (*Context Course Area*). Finally, students will be required to explore a topic of their choosing within security and privacy in depth (*Depth Course Area*).

Requirements (5 courses, minimum 48 units):

|                                          |       |
|------------------------------------------|-------|
| Introduction/Portal Entry course         | Units |
| 15-330 Introduction to Computer Security | 12    |

#### Crosslisted courses allowed.

|                                                     |       |
|-----------------------------------------------------|-------|
| Theoretical Foundations course (choose one option): | Units |
| 15-356 Introduction to Cryptography                 | 12    |
| or both:                                            |       |
| 17-731 Foundations of Privacy                       | 12    |
| 18-733 Applied Cryptography                         | 12    |

#### Crosslisted courses allowed.

|                                                     |       |
|-----------------------------------------------------|-------|
| System Design course (choose one):                  | Units |
| 15-316 Software Foundations of Security and Privacy | 9     |
| 18-335 Secure Software Systems                      |       |

|                                                                                               |       |
|-----------------------------------------------------------------------------------------------|-------|
| Context Course (select one):                                                                  | Units |
| 17-334 Usable Privacy and Security                                                            | 9     |
| or one of:                                                                                    |       |
| 17-333 Privacy Policy, Law, and Technology                                                    | 9     |
| 17-731 Foundations of Privacy (not available if used for Theoretical Foundations requirement) | 12    |

|                                                                                                                                                                                                                         |       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Depth Course (complete one option below):                                                                                                                                                                               | Units |
| Option 1: Complete an elective course from the below list of approved electives, at least 9 units                                                                                                                       | 9     |
| Option 2: Complete an additional course from the prior categories                                                                                                                                                       | 9     |
| Option 3: Complete at least 9 units of Independent Study - this option must be pre-approved by your primary advisor as well as the Concentration Director, and an appropriate faculty advisor and study plan submitted. | 9     |

#### Approved Elective List:

|                                                           |    |
|-----------------------------------------------------------|----|
| 11-488 Concepts in Digital Multimedia and Cyber Forensics | 12 |
| 14-795 AI Applications in Information Security            | 12 |
| 14-809 Introduction to Cyber Intelligence                 | 12 |
| 14-814 Wireless Network Security                          | 12 |
| 14-819 Introduction to Software Reverse-Engineering       | 12 |
| 14-822 Host-Based Forensics                               | 12 |
| 14-823 Network Forensics                                  | 12 |
| 14-828 Browser Security                                   | 12 |
| 14-829 Mobile and IoT Security                            | 12 |
| 15-435 Foundations of Blockchains                         | 12 |
| 17-303 Cryptocurrencies, Blockchains and Applications     | 9  |
| 17-735 Engineering Privacy in Software                    | 12 |
| 18-334 Network Security                                   | 12 |
| 18-436 Browser Security                                   | 12 |
| 18-632 Introduction to Hardware Security                  | 12 |
| 18-636 Browser Security                                   | 12 |

#### Crosslisted courses allowed.

Students can apply one semester of a senior honors research thesis or research-based independent study in a topic related to this concentration, as approved by the concentration director/advisor, as one of the elective courses for this concentration (see option 3 above). This research must have a significant communication component, including a paper or technical report, and a poster presentation. Any research course can count for at most 12 units toward the concentration and can count for at most one elective.

### Anti-requisites

When two (or more) courses overlap significantly in the material they cover, only one can count toward the security and privacy concentration. An example pair is 15-316 Software Foundations of Security and Privacy and 18-335 Secure Software Systems. Another excluded pair is 15-356 Introduction to Cryptography and 18-733 Applied Cryptography. Other such anti-requisites may occur; please consult the concentration director when scheduling courses.

### Excluded Courses

Some security and privacy courses may not be counted towards concentration requirements. These courses all serve specific important different purposes, but do not fit into the concentration as currently designed. For example, 17-331 is more suitable for students who are interested in a broader single-course introduction to information security, but has too much overlap with the concentration's required intro course to be able to count toward the concentration. For other excluded courses, please consult the concentration website.

### Double Counting

Only two of the courses that are counted toward concentration requirements can also be counted towards core course requirements of other majors and minors being pursued by the student. SCS or ECE General Education Requirements are not included in this double-counting limit.

### Advising and Management

The concentration is open to all undergraduates in the School of Computer Science. There is no formal admissions process. Students intending to pursue the concentration should contact the concentration coordinator to register their intention. Curriculum for the concentration will be reviewed by the coordinator annually in consultation with faculty in supporting departments.