CS 463 Computer Security II: Syllabus and Course Schedule

Course Description

The course focuses on various aspects of data-centric security and privacy. Topics include applied cryptography, trusted base, privacy, anonymity, non-interference, information flow, intrusion detection, machine learning and security, password security, policy composition and analysis, formal approaches to specification and verification of secure systems, and security and privacy of emerging systems.

Meeting Schedule / Contact hours

Two 75-minute lectures per week; online, asynchronous via coursera. One invited lecture at the end of the course (synchronous meeting).

Required textbook

No required textbook

Pre-requisites

CS 225. The course assumes a basic knowledge of programming, computer systems, and statistics. The class will expect the ability to program in Python (primary), and Java (secondary).

Learning outcomes

- Identify and address privacy issues in online social networks;
- Apply machine learning to security and address adversarial machine learning;
- Use crypto constructs (homomorphic encryption, multi-party computation, etc.);
- Identify and address issues with de-identification;
- Use hardware designed to support trusted computing;
- Reason about information flow, computational security for encryption;
- Recognize threats and design mitigations for security in key sectors (e.g., healthcare);
- Understand architecture and recognize threats for smartphone security;
- Recognize issues with web privacy (especially tracking and advertising);
- Analyze human factors as they affect privacy and security;
- Recognize and reason about password security;
- Understand side-channel attacks and recognize their threats to security;
- Recognize drivers and tactics in cyber warfare, and other topics of emerging interest in security and privacy.

Course Schedule

Week	Topic	Note
Week 1	Course Plan & Introduction, Security Models	
Week 2	Online Social Networks, De-Identification	MP1 open
Week 3	Machine Learning 1 & 2	
Week 4	Basic Crypto, Crypto Constructs	MP2 open
Week 5	Trusted Computing 1 & 2	
Week 6	Bitcoin, Information Flow	
Week 7	Midterm, Health IT	Midterm. MP3 open
Week 8	Smartphones 1 & 2	
Week 9	Spring Break	Spring Break
Week 10	Crypto Models 1 & 2	MP4 open
Week 11	Web Privacy, Deepfake	
Week 12	Automobiles, Automobiles AML	
Week 13	Password Security, Side-Channel Attacks	Mp5 open
Week 14	Code Stylometry, Cyber Warfare	
Week 15	Invited Lecture, Conclusion	
Week 16	Break / Reading Day	MP5 Video
Week 16	Final Exam	Final Exam Week