Syllabus CS 463

MEETING SCHEDULE/CONTACT HOURS: Two 75-minute lectures per week; online, asynchronous via coursera.

REQUIRED TEXTBOOK: no required textbook

PRE-REQUISITES: CS 225. Additional prerequisites or corequisites may be specified each term. See section information.

LEARNING OUTCOMES

- Identify and address privacy issues in 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 cookies and advertising);
- Analyze human factors;
- Recognize and mitigate insider threats;
- Understand architecture and recognize threats to security;
- Recognize drivers and tactics in cyber warfare, and other topics of emerging interest in security and privacy.

SAMPLE TOPICS LIST

- Introduction & Security Models
- Online Social Networks
- De-Identification
- Machine Learning 1, 2
- Basic Crypto
- Crypto Constructs
- Trusted Computing 1, 2
- Bitcoin
- Information Flow
- Health IT
- Smartphones 1, 2
- Crypto Models 1, 2
- Web Privacy
- Deepfake
- Automobiles 1, 2
- Code Stylometry
- Side-Channel Attacks
- Insider Threats
- Cyber Warfare