CS 239, Advanced Topics in Computer Security
Fall 2010
Instructor: Peter Reiher

This class will discuss advanced topics in computer and network security. Topics to be covered include network security (distributed denial of service attacks, BGP and DNS security, botnets, wireless network security issues), systems security (taint tracking, insider threat detection, malware analysis, trusted computing platforms), general security issues (trust, security vs. usability, security education), and privacy (data mining issues, network privacy issues, social networking and privacy). The class will be in a seminar form, with students presenting material and participating in discussions. Grading will be on the basis of a midterm exam, a group project, and class participation.

Topics to be covered will be selected from the following list. Time will not permit discussion of all these topics, so the set to be covered will be decided on based on student interest.

- Taint tracking
- Distributed denial of service attacks
- Privacy and social networking
- TPM and related technologies
- Malware for portable devices
- Botnets
- Security for ubiquitous computing
- Security versus usability
- BGP security
- DNS security
- Cyberwarfare and cyber-deterrence
- Novel hardware attacks (e.g., cold boot, firmware attacks)
- Privacy and data mining
- Security education
- Web security
- Internet tools for privacy
- Measuring security
- Data provenance tracking
- Attack attribution
- Insider threat detection
- Trust
- Novel access control mechanisms
- Biometric authentication
- Security for vehicular networks
- Analyzing malware
- Virtual machine approaches to security
- Security for cloud computing
- Preventing information leaks
- Social engineering and defenses against it
- Computer forensics