CS5984 Theory and Practice of Web Security and Privacy

Instructor: Danfeng Yao, Assistant Professor of Computer Science

Homework: 40%
Midterm: 15%
Final project: 45%

This course is to give an in-depth description of all aspects related to Internet security and privacy, with particular focuses on secure browser design, web application security, identity management, web traffic analysis, web malware (malicious software), botnet detection, outsource security, and anonymous surfing. The participants are introduced to the technical challenges and real-world problems in securing the web from both host and server perspective. Both classic and modern algorithms, models, and tools for web security and privacy are discussed. Real-world security examples are analyzed. This course does not teach web-application development.

Textbook
There is no required textbook. Instead, research papers of relevant topics will be read.

Syllabus

The following is an approximate list of topics that we will cover.

- Fundamentals including cryptography, HTTPS, networking basics, browser basics
- Secure browser design, browser as an operating system, same-origin policy, mashup security
- Web application security, ActiveX vulnerabilities, JavaScript security and their analysis, information-flow analysis, detecting cross-site scripting, cross-site request forgery
- Browser vulnerabilities, Firefox extension vulnerability, remote code execution, shell code, heap spray attack
- Web malware, drive-by-download, web spam and filtering, code obfuscation
- Botnet detection, IRC, P2P bots, web traffic analysis
- Federated identity management, advanced authentication mechanisms, e-commerce security
- Security of outsource computation, cloud computing security
- Web surfing privacy, detecting information leaking
- Anonymous routing, data anonymization models and algorithms
- Integrity verification, Merkle hash tree, authenticated data structure, broadcast encryption
- Cryptography in securing emails, spam detection, steganography

Prerequisites
        CS3214: Operating Systems or equivalent
        CS4254: Computer Network Architecture and Programming or equivalent