

CS444/544: CYBERSECURITY SYLLABUS

- Course Introduction, Ethics and Legal Issues
 - Responsibilities of Knowledge and Power
 - Ethical Disclosure
 - Surveillance vs Attack
 - Is Finding Security Holes a Good Idea?; *Grey Hat Hacking* (<http://www.amazon.com/Gray-Hat-Hacking-Second-Handbook/dp/0071495681>)
- Brief history of computer security
- Classes of Attack
 - Code injection
 - Time-of-check-to-time-of-use race conditions
 - Sybil attack,
 - Distributed Denial of Service and other network attacks (“How to own the Internet in 5 Minutes,” BGP hijacking, etc.)
- Systems Security
 - Authentication
 - Policy
 - Secure design principles (Saltzer and Schroeder)
 - Information flow
- Network Security:
 - Web: SQL command injection, phishing, and cross-site scripting (XSS)
 - No trusted external party
 - Network reconnaissance and information theory
 - Botnets
- Data Hiding:
 - Cryptography
 - Obfuscation and diversity methods
 - Differential Privacy (Dwork)
 - Anonymity: Sybil attacks, attacks on anonymity (Dwork and Kleinberg)
- Intrusion Detection and Response
 - Anomaly (network and host)
 - Specification based (network and host)
 - Viruses, worms, Denial of Service
- Human Factors:
 - Captcha’s
 - Social engineering, e.g., phishing
 - Economics of Security
 - Incentives and motivations for attack

- Special Topics:
 - Censorship,
 - Biological Inspired Security,
 - Game Theory