CS 1310: CYBERSECURITY FOR BEGINNERS

Semester Hours: 3.0  
Contact Hours: 3

Coordinator: S. Roy  
Text: Readings provided by instructor  
Author(s): VARIED  
Year: Varied

SPECIFIC COURSE INFORMATION

Catalog Description:

Cyber threats in day-to-day computer use, Web security issues and countermeasures, vulnerabilities of smart phones and their mitigation, common cyber-security technologies, hands-on lab activities. Prerequisites: N/A.

Course type: ELECTIVE

SPECIFIC COURSE GOALS

• I can explain the common cyber threats.
• I can use basic cybersecurity tools.
• I can securely use a browser to access the Internet.
• I can protect my computer.
• I can explain the common privacy and security issues of using a smartphone, and I can apply countermeasures.

STUDENT OUTCOMES ADDRESSED BY THIS COURSE

• B.2. Use current techniques, skills, and tools in computing practice
• B.4 Understand the impact of professional, ethical, and social issues in computing

LIST OF TOPICS COVERED

• Nuts-and-Bolts of cyber-security (~7%)
• A big picture of the problem: computers, smartphones, the Internet, and threats
• Key components (hardware and software) of a computer, and how they work together
• Representing and storing information in digital form
  • E.g., how a computer processes and stores an English word, etc.
• Pillars of information security: confidentiality, integrity, and availability

• Ethics and Economics of cybersecurity (~15%)
  • Tension between cost and security
  • Tradeoff between usability and security
  • Individual privacy vs. law enforcement
  • Ethical hacking

• Fun with encryption/decryption schemes (~7%)
  • Overview of one popular encryption/decryption algorithm
  • Symmetric key system vs. public/private key system.

• On Password-based authentication (~7%)
  • Measuring the strength of a password
  • Tools for cracking password, etc.
  • How CAPTCHA helps against password cracking

• Access control and authentication (~14%)
  • Access control (i.e., read, write, execute permission) of a file in a computer
  • Usage of a one-way hash function
  • How a computer recognizes a user (user authentication)
    • Case study: Linux system’s scheme for access control and user authentication
  • Newer authentication schemes
    • Single-Sign-On (e.g., accessing Canvas via my.bgsu.edu)
    • Multi-factor authentication (e.g., DUO code to login to my.bgsu.edu)

• Security issues in computer networks and web browsing (~15%)
  • Basic structure/architecture of the Internet
    • LAN, subnet, IP address.
  • Security issues of home/public Wi-Fi; attacks on a web session
    • Man-in-the-middle attack
    • Sniffing computer network traffic (Wireshark tool)
• Stealing Cookie
  o Countermeasures
    ▪ Public key infrastructure (PKI), Virtual Private Network (VPN).
• Software vulnerability/maliciousness. (~7%)
  o Security issue/hole in software
  o Intentional maliciousness vs. unintentional vulnerability.
• Common schemes of cyber-attacks and countermeasures: (~7%)
  o Social Engineering, phishing, drive-by-download, clicking email-attachment
  o Spyware, adware, ransomware
• Security and privacy issues of smartphones (~7%)
  o Basic design of an android/iPhone app
  o Common threats and Countermeasures
• Security and privacy issues of online social networks (~7%)
  o Privacy issues in sharing information publicly
  o Common threats and Countermeasures
• Protecting a personal computer (~7%)
  o Why to run only updated software on a computer
  o How to safely install software only from a trusted party
  o Running an antimalware (and firewall) to protect a computer