CprE 536: Computer and Network Forensics

Cyber-attack prevention, detection, response, and investigation with the goals of counteracting cybercrime, cyberterrorism, and cyberpredators, and making the responsible persons/groups accountable.

Course Objectives

The knowledge of computer and network forensics has become essential in securing today's network-centric computing environment. This new course will give the students both the fundamental knowledge and hands-on practice on computer and network forensics. The added exposure to forensics will enhance the marketability of our students and serve the students who carry the skills and knowledge forward into their future careers.

Upon completing this course, the students are expected to understand the basics of computer and network forensics, to be well-trained as next-generation computer crime investigators, and to be prepared for active research at the forefront of these areas.

News and Events

Fall 2013 (Please keep an eye on this news box for the latest.)

1. Our kick-off meeting will be held on Aug. 27, 2013, at Howe 1344. Welcome to our fall Forensics class!
2. If you have any questions or suggestions about the Blackboard course site (streaming lectures and in-class annotations), please email edehelp@iastate.edu and copy it to the instructor (yguan@iastate.edu).
3. DC3 Challenge: You are welcome to join or start a team formed by the students in our forensics class. Please find more info about it at: http://www.dc3.mil/challenge/.
4. More to be added.

Course Description

Computer and network forensics studies cyber-attack prevention, planning,
detection, response, and investigation with the goals of counteracting cybercrimes, and making the responsible persons/groups accountable. The topics covered in this course include fundamentals of digital forensics, forensic duplication and analysis, network surveillance, intrusion detection and response, incident response, anti-forensics techniques, anonymity and pseudonymity, cyber law, computer security policies and guidelines, court report writing and presentation, and case studies.

Course projects will be done using the licensed toolkits and equipments in the NSF-funded Cyber Forensics Lab at Coover 3223.

The course will consist of three course projects (i.e., machine problems), two exams, and one term paper. We will have a small number of homework assignments, demonstrations (on your course projects), and presentations. The students will:

1. Write a 8-pages (double column and single space) term paper: including defining a specific problem, surveying existing work, developing a (better) solution, and evaluating your results. A list of selected topics/problems will be provided. You are also welcome to propose your own one.
2. Learn to use and evaluate digital forensic toolkits and write reports on them.
3. Give demos and/or presentations on projects, and term papers.

Course Outline:

Module I: Digital Forensics: An Overview
Module II: Forensics Basics and Criminalistics
Module III: Basics of OS and Networking: A Review
Module IV: Advanced Topics in Computer and Network Forensics
Forensic Modeling and Principles
Forensic Duplication
Forensics Analytics
File Carving
Cyber Forensics Tools and the Testing Thereof
Mobile Device Forensics
Network Surveillance and Accountability
Network Attack Traceback and Attribution
Multicast Fingerprinting
Multimedia Forensics
Module V: Intrusion and Online Frauds Detection
Module VI: Steganography & Steganalysis
Module VII: Anonymity/Pseudonymity/P3P
Module VIII: Cyber Law, Security and Privacy Policies and Guidelines
Module IX: Case Studies, and ethical issues
Module X: Court Testimony and Report Writing Skills

Course Materials

There will be no textbooks. Most readings are from the lecture notes and papers published in
recent years from top security/forensics conferences/workshops or journals, reference books, and related Internet web sites. Two reading lists will be given. The required readings are 30-35 papers and a suggested reading list includes 130+ papers published within the last 10 years. The following are a list of reference books:


Lecture slides and notes can be accessed through Blackboard.

The required and suggested reading lists can be accessed through Blackboard.

Useful On-line Resources:

Scientific Working Group on Digital Evidence
International Journal of Digital Evidence
Department of Defense Computer Forensics Lab
Digital Forensics Research Workshop
National White Collar Crime Center
Department of Justice CCIPS
International Organization on Computer Evidence
High Tech Crime Investigators Association
UK National High Tech Crime Unit
CERIAS Forensics Research
University of Central Florida Digital Evidence Site
Encase
Seminal papers at Computer Security Archives Project at UC, Davis
Committee on National Security Systems page (NSTISSI standards)

Course Prerequisite

CprE 308 and 489, or at least familiar with basic concepts in operating systems and networking.

Grading and Acad. Policy

Grading will be on the absolute scale. The cutoff for an `A' will be at most 90% of total score, 80% for a `B', 70% for a `C', and 60% for a `D'. However, these cutoffs might be lowered at the end of the semester to accommodate the actual distribution of grades.

1. Mid-term & Final Exam: 40%
2. Course Projects: 30%
3. Presentations and Participation in Class Discussions: 5%
4. Term Papers: 25%

Academic Policy:

- All incidents of academic dishonesty will be dealt with according to the university policy. No exceptions.
  a. All references must be properly cited, including internet web pages (URL must be provided). If plagiarism is detected, i.e. without proper citation and quotation, you will automatically receive an F. When in doubt, please ask the instructor if it is reasonable to include other's work in your assignments.
- We welcome active participation and discussions about the topics/materials covered in the class.
- Due date for term papers and course projects is hard (no late hand-in will be accepted.) except that you have reasonable reason. However, for the whole semester, you can have at most one time no-reason three-day extension.

Lecture and Office Hours

Dr. Yong Guan, Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011. Office: Coover 3216. Email: yguan@iastate.edu. Phone: (515) 294-8378. Fax: (515) 294-8432.

Lecture: Tuesday & Thursday, 9:30-10:45am, Howe 1344.

Office Hours: Monday, 10:00-10:59am, Coover 3219.

Further Information

For further information, please contact Yong Guan (yguan@iastate.edu) by email
or drop by office Coover 3216.