CS 5330: NETWORK SECURITY AND FORENSICS

Semester Hours: 3.0
Contact Hours: 3
Coordinator: Ruinian Li
Text: Network Forensics: Tracking Hackers through Cyberspace
Authors: SHERRI DAVIDOFF & JONATHAN HAM
Year: 2012

SPECIFIC COURSE INFORMATION

Catalog Description:

Principles and practices of network forensics. Introduction to network protocols; security and forensic components; and vulnerability and defense. Data formats, digital evidence provenance and image exchange. Forensics tools and techniques: live data forensics; database forensics; use of network logs and other datasets for incidence timelines, and subject/object associations. Prerequisite: Full Admission to MS in CS program or consent of department.

Course type: ELECTIVE

SPECIFIC COURSE GOALS

- I can compare and contrast tools used in network forensics and security applications.
- I can use certain tools (for example: network enabled forensics s/w agents; RAM analysis tools; others) to collect and analyze volatile and non-volatile data.
- I can provide technical arguments for the integrity of a certain piece of evidence.
- I can create a timeline of events and identify linkage b/w subjects and objects for synthetic and real datasets.
- I can articulate mechanisms for recovering encrypted datasets and creating process logs.
- I can explain the provenance of a piece of digital evidence.
- I can explain and process forensic datasets in a variety of formats.
- I can analyze relevant research and communicate my findings.

LIST OF TOPICS COVERED

- Overview (~8%)
- Admissibility of digital evidence
- Communication protocols
- Network forensics and security
- Relationship among components

- **Data Formats (~14%)**
  - Log files and cache
  - Image formats
  - Forensic file formats
  - Others

- **Forensic Imagery (~14%)**
  - Log process
  - Refinement and visualization
  - Integrity checks

- **Network Security and Forensic Techniques (~21%)**
  - Reconnaissance techniques
  - Protocol specifics
  - Port scans and dumps
  - Memory, non-volatile media, and web cache/traffic

- **Tool Talk – Possible Candidates (~28%)**
  - Port scan tools
  - nmap; Ether dump, SIFT
  - Autopsy
  - Recovery tools
  - Sleuth Kit, OSAF TIK
  - Encase (resource permitting)

- **Recovery of protected data (~5%)**
  - Encrypted media
  - Password cracking

- **Reporting (~5%)**
  - Elements & organization

- **Platform-based Techniques (~5%)**
- Windows and Unix
- IOS and Android