CS 4330 : 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.
Prerequisites: CS 3270 or corequisite of CS 4390, and a grade of C or better in CS 3320. Credit cannot be earned for both CS 4330 and CS 5330.

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.
LIST OF TOPICS COVERED

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

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

• Forensic Imagery (~14%)
  o Log process
  o Refinement and visualization
  o Integrity checks

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

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

• Recovery of protected data (~5%)
  o Encrypted media
  o Password cracking
• Reporting (~5%)
  o Elements & organization
• Platform-based Techniques (~5%)
  o Windows and Unix
  o IOS and Android