CS 4330 : NETWORK SECURITY AND FORENSICS

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

SPECIFIC COURSE INFORMATION

Catalog Description:

This course provides a comprehensive understanding of network forensics analysis principles. Students will learn to identify network security incidents and potential sources of digital evidence and demonstrate the ability to perform basic network data acquisition and analysis using computer-based applications and utilities. Students will also demonstrate the ability to accurately document network forensics processes and analysis. Prerequisite: CS3270 or corequisite of CS4390, and a grade of C or better in CS3320.

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

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

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

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

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

5. Tool Talk – Possible Candidates (~28%)
   - Port scan tools
   - nmap; Ether dump, SIFT
   - Autopsy
   - Recovery tools
6. Recovery of protected data (~5%)
   - Encrypted media
   - Password cracking

7. Reporting (~5%)
   - Elements & organization

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