Design of Network Forensics Course

Dr. Kewei Sha

Dept. of Computing Sciences & Cyber Security Institute

University of Houston – Clear Lake

sha@uhcl.edu

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Agenda

- ❑ Motivation
- ❑ Design Goals
- ❑ Learning Outcomes
- ❑ Modules
- ❑ Challenges
- ❑ Conclusion

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Motivation

- Pervasive networked systems
- Many successful real world hacking activities
- Severe lose caused by cyber attacks
- Requirements of National Center of Academic Excellence in Cyber Defense Designation
- Workforce shortage in Network Forensics
- Students needs of knowledge in CS, CIS, and IT
- Missing network forensics in current CS curriculum

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Design Goals

- Complement to the existing curriculum
- An excellent coverage of Network Forensics topics
- A pluggable module-based approach
  - Modules, sub-modules, and units
- Simulated organization network environment
- Hands-on activities

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Course Goals

This course introduces and explains the fundamental concepts of network forensics, core of network forensics related to different network devices and network based applications, and tools used to collect, analyze and report forensics related data.

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Learning Outcomes

- ❑ Understand the concept of digital evidence
- ❑ Understand the design of network sensors and deployment
- ❑ Understand mechanisms to investigate network devices
- ❑ Understand mechanisms to investigate network applications
- ❑ Be able to use data collection tools and data analysis tools
- ❑ Be able to write network forensics report
- ❑ Understand the privacy issues in network forensics

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Modules

- Module 1: Foundations of Network Forensics
- Module 2: Core of Network Forensics
  - Submodule 1: Investigating Network Devices/Components
  - Submodule 2: Investigating Network Attacks
  - Submodule 3: Focused Topics in Network Forensics
- Module 3: Forensics and Privacy
- Module 4: Network Forensics Tools and Hands-on Activities

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Module 1: Foundations of Network Forensics

- Unit ND_1: Review of Network Threats
- Unit ND_2: Review of Computer Forensics
- Unit ND_3: Event Logs
- Unit ND_4: Evidences
- Unit ND_5: Location Awareness
- Unit ND_6: Co-relating Attacks

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Module 2.1: Investigating Network Devices/Components

- Unit ND_7: Proxies and Forensics
- Unit ND_8: Firewalls and Forensics
- Unit ND_9: NIDS & NIPS and Forensics
- Unit ND_10: VPN and Forensics
- Unit ND_11: Router and Forensics

University of Houston Clear Lake

Module 2.2: Investigating Network Attacks

- Unit ND_12: BotNet Forensics
- Unit ND_13: DDoS Forensics
- Unit ND_14: Malware Forensics

University
of Houston
Clear Lake

Module 2.3: Focused Topics in Network Forensics

- Unit ND_15: Media Forensics
- Unit ND_16: Web Forensics
- Unit ND_17: Email Forensics
- Unit ND_18: Smartphone Forensics
- Unit ND_19: Cloud Forensics
- Unit ND_20: IoT Forensics

Cyber Security Institute
University of Houston-Clear Lake

Module 3: Forensics and Privacy

- Unit ND_21: Privacy and Forensics
- Unit ND_22: Ethics and Forensics
- Unit ND_23: Reporting Investigation Results

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Module 4: Network Forensics Tools and Hands-on Activities (Labs)

- Unit ND_24: Lab - Tcpdumping with the libpcap library
- Unit ND_25: Lab - Sniffing wireless traffic with Wireshark
- Unit ND_26: Lab - Packet sniffing and analysis with NetworkMiner
- Unit ND_27: Lab - Malware identifying with YARA
- Unit ND_28: Lab - Evidence acquisition with SNORT
- Unit ND_29: Lab - Collect and analyze log file with Splunk

Cyber Security Institute
University of Houston-Clear Lake

Challenges

- Difficult to configure a lab for network forensics
- Short of Available guidance on hands-on activities
- Lack of high quality textbooks
- No experienced colleagues in department

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Conclusion

- Needs of Network Forensics course
  - Workforce needs
  - Department needs
  - Designation needs
- Design of Network Forensics course
  - A pluggable module-base approach
  - Good coverage
  - Rich hands-on activates
- Challenges

University of Houston Clear Lake

Cyber Security Institute
University of Houston-Clear Lake

Thank you!

University
of Houston
Clear Lake