Cybersecurity Informatics: Introduction

Wingyan Chung, Ph.D.

Instructor: Dr. Wingyan Chung

- Welcome!
- Wingyan Chung
  - Faculty at Institute for Simulation and Training, UCF
  - Ph.D., Management Information Systems, University of Arizona
  - Research areas: cybersecurity, social media analytics, business intelligence, big data, text and web mining, human-computer interaction, and network science
- Contact
  - Email: wchung@ucf.edu
  - Telephone: +1 (407) 882-1435
  - Address: 3100 Technology Pkwy., PII 131F, Orlando, FL 32826
  - Website: http://pegasus.cc.ucf.edu/~cyber/wchung

Motivation

- Concern about cybersecurity has been growing rapidly in both public and private sectors.
- Rising volume, velocity, and variety of data generated generated in response to cybersecurity issues call for well-equipped professionals to lead the efforts of handling, analyzing, and interpreting these data.
- Intelligence and Security Informatics (ISI) is an academic and practical discipline of developing and applying data-driven analytical, modeling, and simulation techniques to the data.
- However, training materials and courses for cybersecurity informatics are not widely available.

Course Description

The course introduces fundamental concepts, techniques, and tools in managing, analyzing, and interpreting data for cybersecurity informatics. The concepts and techniques include data description, modeling of user requirements and data properties, data storage, making inferences from data, machine learning, and network analytics. Students will learn to use contemporary software tools to automate the informatics process and to support research development.

Cybersecurity Informatics

- This course introduces fundamental concepts, techniques, and tools in managing, analyzing, and interpreting data for cybersecurity informatics
    - Data Summarization for Understanding the Cyber Landscape
    - Making inferences from cyber event and media data
    - Scientific Assessment of Cybersecurity Threats
    - Correlating Events with Cybersecurity Phenomena
    - Machine Learning for Cyber Event Exploration and Prediction
    - Network Science for Community Analyses
- The cyber domain: cybersecurity, cyber intelligence, analytics
- Software tools: R studio and WEKA

Course Modules (Week-by-Week)

<u>Data Summarization for Understanding the Cyber Landscape</u>

1. Understanding the cybersecurity landscape and the data environment

2. Data Summarization and Description in Cybersecurity Analysis

<u>Making Inferences from Event and Media Data</u>

3. Developing confidence intervals for cybersecurity data

4. Interpreting confidence interval for understanding cyber phenomena

<u>Scientific Assessment of Cybersecurity Threats</u>

5. The scientific process of detecting cybersecurity threats

6. Procedure and tools for interpreting testing results

7. Mid-term Exam

<u>Correlating Events with Cybersecurity Phenomena</u>

8. Correlational research in cybersecurity

9. Predicting activities in cybersecurity events

<u>Unsupervised Learning for Event Exploration</u>

10. Exploratory study of cyber phenomena

11. Clustering cybersecurity cases and data

<u>Supervised Learning for Event Prediction</u>

12. Profiling and categorizing intelligence factors

13. Classifying cybersecurity incidents and threats

<u>Network Science for Community Analyses</u>

14. Understanding networks of actors in cybersecurity incidents

15. Modeling networks for community analyses

16. Final Exam

Evaluation

- Online Examinations
  - Mid-term Exam (Week 7)
  - Final Exam (Week 16)
- Assignment due Thu. 11:59 pm each week
  - Problem Set (7)
  - Online Discussion and Peer Review (8)
- Individual Paper due last week (Thu. 11:59 pm)
  - To be facilitated by online discussions and group peer review.
  - Each student develops a CI study, collect data, and analyze the data, and produce a final report.
  - Example papers will be provided as reading assignments.