CTS 6319: Cyber Security: Measurement and Data Analysis

Credits: 3 credits

Textbook, Title, Author, and Year:


Reference Materials:

Research Papers (subject to change)

Paper 1:

Paper 2:

Paper 3:

Paper 4:

Paper 5:

Paper 6:

Paper 7:

Paper 8:

Paper 9:

Paper 10:

Paper 11:
Specific Course Information:
This course introduces data science to the field of cyber security. Digital investigation approaches for cyber security will be discussed. Further, data analytics and traffic analysis methodologies will be presented. Data acquisition and sound analysis methods will also be elaborated. Approaches for inferring and attributing various types of cyber-attacks will be presented.

Catalog Description:
This course explores techniques and considerations for conducting cyber security research rooted in empirical observation. Topics include Internet measurement methodologies and data analytics and characterizing cyber-attacks. The ultimate goal of this course is to foster analysis of empirical data that is both sound and insightful.

Prerequisites: Graduate standing or instructor’s permission, networking basics

Specific goals for the course:

- Provide a background of networking concepts and how they can be leveraged in cyber security
- Provide practical and sound methods for the acquisition and measurement of Internet traffic for cyber security
- Demonstrate real corporate and Internet attacks
- Compare and contrast probabilistic, statistical and heuristic approaches to infer and attribute cyber security attacks through traffic analysis
- Provides practical techniques to geo-locate and report cyber security incidents

Brief List of Topics to Be Covered:

- Internet measurements for cyber security
- Denial of Service/Probing Detection
- Botnet Analysis
- Internet Censorship