CTS 6319: Cyber Security: Measurement and Data Analysis

Credits: 3 credits

Textbook, Title, Author, and Year:

Cybersecurity and Cyberwar: What Everyone Needs to Know, by P.W. Singer and Allan Friedman, ISBN-10: 0199918090 1st Edition, 2014

Data Analysis for Network Cyber-Security, by Niall Adams and Nicholas Heard, ISBN: 978-1-78326-374-5, 2014

Communication Networks: Fundamental Concepts and Key Architectures, by Alberto Leon- Garcia, ISBN-10: 007246352X 2nd Edition, 2003

Reference Materials:

Research Papers (subject to change)

Paper 1:
Paxson, Vern. "Strategies for sound internet measurement." Proceedings of the 4th ACM SIGCOMM conference on Internet measurement. ACM, 2004.

Paper 2:
Moore, David, et al. "Inferring internet denial-of-service activity." *ACM Transactions on Computer Systems (TOCS)* 24.2 (2006): 115-139.

Paper 3:
Paxson, Vern. "An analysis of using reflectors for distributed denial-of-service attacks." *ACM SIGCOMM Computer Communication Review* 31.3 (2001): 38-47.

Paper 4:
Fayaz, Seyed K., et al. "Bohatei: flexible and elastic DDoS defense." *arXiv preprint arXiv:1506.08501* (2015).

Paper 5:
Bou-Harb, Elias, Mourad Debbabi, and Chadi Assi. "Cyber scanning: a comprehensive survey." *Communications Surveys & Tutorials, IEEE* 16.3 (2013): 1496-1519.

Paper 6:
Stone-Gross, Brett, et al. "Your botnet is my botnet: analysis of a botnet takeover." *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009.

Paper 7:
Paxson, Vern. "Bro: a system for detecting network intruders in real-time."*Computer networks* 31.23 (1999): 2435-2463.

Paper 8:
Handley, Mark, Vern Paxson, and Christian Kreibich. "Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-End Protocol Semantics." *USENIX Security Symposium*. 2001.

Paper 9:
Xie, Yinglian, et al. "Spamming botnets: signatures and characteristics." *ACM SIGCOMM Computer Communication Review*. Vol. 38. No. 4. ACM, 2008.

Paper 10:
Dainotti, Alberto, et al. "Analysis of country-wide internet outages caused by censorship." *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 2011.

Paper 11:
Burstein, Aaron J. "Conducting Cybersecurity Research Legally and Ethically."*LEET* 8 (2008): 1-8

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