Topics in Computer and Network Security

Shuai Hao - Assistant Professor - Computer Science @ Old Dominion University

In-person class, the discussed papers will be presented. Social distancing measures will be practiced. Students who are uncomfortable with participating in the classroom can submit their recorded presentations.

Course Schedule (TBD)

Ofice: 3111 E&CS Building
Email: shao-AT-odu.edu
Office hours: 2-4 pm Wednesday

Lecture time: TR 3:00 pm - 4:15 pm
Location: TBA

This course is a research-oriented, graduate-level course, centering around both classic and state-of-the-art techniques on various aspects of computer and network security. The course involves both reading/discussing research papers and a term project/final report. The course aims to provide a thorough grounding on the computer and network security for the students who are interested in conducting research in this area, as well as a comprehensive background for those generally interested in networking or security. Topics covered in the course include: System Security (Binary analysis, Memory analysis, Control-Flow Integrity), Network Security (DoS attacks, DNS security, Botnets, BGP security), Web Security (HTTPS, browser security, online spam), Cloud Security (Cloud side-channel, information leakage), Privacy (Mobile tracking, censorship), as well as other topics such as Crypto and Crytocurrency.

Presentations
The slides used to present the paper in the class must be created by the presenters. Using materials from original authors or others is allowed but needs to be properly cited.

Grading and Policies
- 5% Class Participation
- 40% Presentations
- 20% Paper Reviews
- 35% Final Report

Paper Reviews and Final Report
Each student is required to write two paper reviews. The Final report is either a research-oriented technical report or a survey paper for a specific topic within the scope of the course. Details and instruction will be given in the lecture and post later.

Course Delivery
In-person class, the discussed papers will be presented. Social distancing measures will be practiced. Students who are uncomfortable with participating in the classroom can submit their recorded presentations.

Tentative Paper List

1. System Security
   - Seful: Demystified, USENIX Security'02.

2. Network Security
   - Understanding the Mirai Botnet, USENIX Security'17.
   - A Longitudinal, End-to-End View of the DNSSEC Ecosystem, USENIX Security'12.
   - Are We There Yet? On RPS's Deployment and Security, NDSS'17.

3. Cloud Security
   - Cross-Tenant Side-channel Attacks in Public Clouds, ACM CCS'14.
   - TenantGuard: Scalable Runtime Verification of Cloud-Wide VM-Level Network Isolation, NSDI'17.

4. Web Security
   - Dynamic Phishing Attacks and Locked Same-origin Policies for Web Browsers, ACM CCS'07.
   - Characterizing Large-Scale Click Fraud in ZeroAccess, ACM CCS'14.

5. Privacy and Censorship
   - Detecting and Defending Against Third-Party Tracking on the Web, NSDI'12.

6. Miscellaneous
   - Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices, USENIX Security'12.
   - MindSweeper: An In-depth Look into Drive-by Cryptocurrency Mining and Its Defense, ACM CCS'18.
   - It's Free for a Reason: Exploring the Ecosystem of Free Live Streaming Services, NDSS'16.
   - DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning, ACM CCS'17.

Web security (HTTPS, browser security, online spam), Cloud security (Cloud side-channel, information leakage), Privacy (Mobile tracking, censorship), as well as other topics such as Crypto and Crytoccurrency.