CS 6301: Advanced Topics in AI and Network Security (Fall 2021)

Syllabus Schedule ☰

Instructor: **Shuang Hao**
Email: shao -at- utdallas.edu
Office: ECSS 3.705
Office hours: TBA

Class time: 4-6:45 pm Friday

Location: CB3 1.306

To register the class, please search class number 89071 on Galaxy

Course Overview

CS 6301 is a graduate-level AI and network security course. We will cover techniques and knowledge for conducting machine learning security, empirical network security, and data analytics research. The course will center around readings of foundational and seminal research papers. Topics include deep learning in security, intrusion detection, botnets and spam, social engineering, web attacks, search engine optimization, and measurement methodology. Students will also learn skills of reading essays and research papers and giving presentations.

Textbook and Reading List

The course has no textbook. We will read a bunch of research papers. The instructor will introduce reference books for particular topics.

1. DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning. Min Du, Feifei Li, Guineng Zheng, and Vivek Srikumar. CCS 2017.
2. LEMNA: Explaining Deep Learning based Security Applications. Wenbo Guo, Dongliang Mu , Jun Xu, Purui Su, Gang Wang, and Xinyu Xing. CCS 2018.
3. Robust Physical-World Attacks on Deep Learning Visual Classification. Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Chaowei Xiao, Atul Prakash, Tadayoshi Kohno, and Dawn Song. CVPR 2018.
4. In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking. Yuezun Li, Ming-Ching Chang, and Siwei Lyu. WIFS 2018.
5. Protecting World Leaders Against Deep Fakes. Shruti Agarwal, Hany Farid, Yuming Gu, Mingming He, Koki Nagano, and Hao Li. CVPRW 2019.
6. Your Botnet is My Botnet: Analysis of a Botnet Takeover. Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna. CCS 2009.
7. deSEO: Combating Search-Result Poisoning. John P. John, Fang Yu, Yinglian Xie, Arvind Krishnamurthy, and Martin Abadi. USENIX Security 2011.

8. Cloak and Dagger: Dynamics of Web Search cloaking. David Y. Wang, Stefan Savage, and Geoffrey M.Voelker. CCS 2011.
9. Click Trajectories: End-to-End Analysis of the Spam Value Chain. Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, Brandon Enright, Mark Felegyhazi, Chris Grier, Tristan Halvorson, Chris Kanich, Christian Kreibich, He Liu, Damon McCoy, Nicholas Weaver, Vern Paxson, Geoffrey M. Voelker, and Stefan Savage. IEEE S&P 2011.
10. You Are What You Include: Large-scale Evaluation of Remote JavaScript Inclusions. Nick Nikiforakis, Luca Invernizzi, Alexandros Kapravelos, Steven Van Acker, Wouter Joosen, Christopher Kruegel, Frank Piessens and Giovanni Vigna. CCS 2012.
11. Don't Forget to Lock the Back Door! A Characterization of IPv6 Network Security Policy. Jakub Czyz, Matthew Luckie, Mark Allman, and Michael Bailey. NDSS 2016.
12. Automated Crowdturfing Attacks and Defenses in Online Review Systems. Yuanshun Yao, Bimal Viswanath, Jenna Cryan, Haitao Zheng, and Ben Y. Zhao. CCS 2017.
13. @spam: The Underground on 140 Characters or Less. Chris Grier, Kurt Thomas, Vern Paxson, and Michael Zhang. CCS 2010.
14. Entropy/IP: Uncovering Structure in IPv6 Addresses:. Pawel Foremski, David Plonka, and Arthur Berger. IMC 2016.
15. Spamming Botnets: Signatures and Characteristics. Yinglian Xie, Fang Yu, Kannan Achan, Rina Panigrahy, Geoff Hulten,and Ivan Osipkov. SIGCOMM 2008.
16. Filtering Spam with Behavioral Blacklisting. Anirudh Ramachandran, Nick Feamster, and Santosh Vempala. CCS 2007.
17. Reading Thieves' Cant: Automatically Identifying and Understanding Dark Jargons from Cybercrime Marketplaces. Kan Yuan, Haoran Lu, Xiaojing Liao, and XiaoFeng Wang. USENIX Security 2018.
18. Detecting and Defending Against Third-Party Tracking on the Web. Franziska Roesner, Tadayoshi Kohno, and David Wetherall. NSDI 2012.

Grading Policy

The grade will be computed based on the following components:

- 5% Class Participation
- 45% In-Class Presentations
- 50% Class Project

- Class Participation will be based on attendance.

- In-Class Presentations will be presentations of research papers to the class. Each student will be assigned twice during the class to present the assigned papers. The students are expected to describe the challenges of the problems and introduce technical details of the papers.

- Class Project will be completed individually or in a team of two. The project ideas will be approved by the instructor. Please come to talk with the instructor early about the project ideas, the instructor will provide suggestions or point to the right directions.

Tentative Course Schedule

Date	Topic

08/27	Course Overview
09/03	Basic Knowledge
09/10	Paper Reading, Writing, and Review
09/17	Techniques of Measurement and Large-scale Data Analysis
09/24 A	Deep Learning for Detection [1]
09/24 B	Adversarial Machine Learning [3]
10/01 A	Fake Reviews [12]
10/01 B	Interpretable Machine Learning for Detection [2]
10/08 A	Deepfake Detection [4]
10/08 B	Deepfake Detection [5]
10/15 A	Underground Economy [9]
10/15 B	Underground Jargons [17]
10/22 A	Botnet Characteristics [15]
10/22 B	Spam Filtering [16]
10/29 A	Search Engine Poisoning[7]
10/29 B	Cloaking and Redirection [8]
11/05 A	Botnet Takeover [6]
11/05 B	Social Network Spam [13]
11/12 A	Vulnerabilities in IPv6 Networks [11]
11/12 B	Finding IPv6 Addresses [14]
11/19 A	Web Security [10]
11/19	

B	Web Tracking [18]
11/26	**Thanksgiving Break**
12/03	**Project Presentation**