Fall 2012

CEG 7900-01: Special Topics: Computer and Network Security

Junjie Zhang
Wright State University - Main Campus, junjie.zhang@wright.edu

Repository Citation

Zhang, J. (2012). CEG 7900-01: Special Topics: Computer and Network Security. .
https://corescholar.libraries.wright.edu/cecs_syllabi/857

CEG-7900 Special Topics: Computer and Network Security

Prof. Junjie Zhang

junjie.zhang@wright.edu
Office: Russ 337
24 August 2012

Schedule

Tuesday and Thursday
5:00PM - 6:20PM
Russ 150

Office Hour

After class or by appointment

Course Overview

This course will introduce active research topics in computer and network security, and will focus on discussing both sophisticated cyber-attacks and the defense mechanisms. The course will cover topics including intrusion detection, malware analysis, worm detection, botnet detection, spam, phishing, DNS security, web security, cellular network security, and privacy. This class is targeted at PhD and MS students who consider conducting research in computer and network security, and students who are interested in real-world security problems.

This course will be research oriented, which will be taught as both lecture and seminar. Students will be required to present research papers selected from top security conferences or journals. Each student will also be required to write a review of assigned readings before each lecture. Additionally, there will be a term project, and each student (or a team of students) will be required to formulate, address, and document a research problem related to computer and network security, which is expected to result in a conference-style research paper.

Textbook (s): There is no required textbook. All readings will be from research papers in top security conferences and journals.

Prerequisites: Operating Systems, Computer Networks, and programming skills (e.g., C/C++, Java, or Python)

Grading

Class Participation: 5%
Homework: 15%
Paper Reviews: 20%
Paper Presentations: 15%
Research Projects: 45%

Homework

There will be one assignment. Students will be required to answer a series of questions and analyze real security data using existing network/security tools or developing their own gadgets.

Paper Reading and Reviews

Students are required to read assigned research papers before each lecture, and also write a review for each paper individually. Each review should include 1) the background and motivation, 2) comparison with related works, 3) the assumptions, designs, and experimental results, 4) conclusion, and 5) future work. *Paper reviews need to be sent to the professor the day prior to the corresponding lecture.*

Project Presentations

Each student is required to present one or multiple papers over the semester. Students who give presentation must generate the presentation materials by themselves. However, students can use the figures, graphs, and tables from the original papers. In the presentation, students will also need to prepare a list of discussion questions and moderate the discussion. The presentation should be 40-50 minutes, followed by the 15-20 minute discussion. *The slides should be given to the professor within 1 day after the class, which will be posted to the course website.*

Research Projects

Students will work on a research project individually or in a team with up to 2 members. Students can freely choose project topics but the topics should be relevant to network security, system security, or information security. Ph.D. students are especially encouraged to propose research topics related to their current research.

A research proposal needs to be submitted to the professor in the middle of the semester (refer to the schedule). The proposal should include 1) background and motivation, 2) related works, 3) proposed approach, 4) experiment setup, and 5) expected results.

By the end of this course, the research project should result in a conference-style research paper, a 30-minute presentation, and the deliverables such as data and analysis system.

Academic Integrity and Ethical Learning

Students must adhere to the "Academic Integrity" of the Code of Student Conduct in Wright State University. The knowledge learnt from this class must never be used for unethical purposes.

Schedule

Date	Topic	Lectures/Readings	Presenter & slides
Aug 28	Introduction		Dr. Zhang
Aug 30	Botnet	BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic. G. Gu, J. Zhang, and W. Lee. NDSS'08 [Optional] BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation. G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee. USENIX'07	Dr. Zhang No review required
Sep 4	Botnet	BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection. G. Gu, R. Perdisci, J. Zhang, and W. Lee. USENIX'08 Detecting Stealthy P2P Botnets Using Statistical Traffic Fingerprints. J. Zhang, R. Perdisci, W. Lee, U. Sarfraz, and X. Luo. DSN-DCCS'11	Dr. Zhang No review required
Sep 6	Spam (Measurements)	Spamalytics: An Empirical Analysis of Spam Marketing Conversion. C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. Voelker, V. Paxson, and S. Savage. CCS'08 Understanding the Network-Level Behavior of Spammers. A. Ramachandran and N. Feamster. SIGCOMM'06	

Date	Topic	Lectures/Readings	Presenter & slides
Sep 11	Spam (Detection)	Detecting Spammers with SNARE: Spatio-Temporal Network-Level Automated Reputation Engine. S. Hao, N. Feamster, A. Gray, N. Syed, and S. Krasser. USENIX'09 BotGraph: Large Scale Spamming Botnet Detection. Y. Zhao, Y. Xie, F. Yu, Q. Ke, Y. Yu, Y. Chen, and E. Gillum. NSDI'09	Dr. Zhang
Sep 13	Web	Automated Web Patrol with Strider HoneyMonkeys: Finding Web Sites That Exploit Browser Vulnerabilities. Y. M. Wang, D. Beck, X. Jiang, R. Roussev, C. Verbowski, S. Chen, and S. King. NDSS'06 Rozzle: De-Cloaking Internet Malware. C. Kolbitsch, B. Livshits, B. Zorn, and C. Seifert. Oakland'12	
Sep 18	Web	Puppetnets: Misusing Web Browsers as a Distributed Attack Infrastructure. V. T. Lam, S. Antonatos, P. Akritidis, and K. G. Anagnostakis. CCS'06. [Optional] Secure Web Browsing with the OP Web Browser. C. Grier, S. Tang, and S.T. King. Oakland'08	
Sep 20	Project Idea Presentation and Discussion		
Sep 25	Intrusion Detection	Anomalous Payload-based Network Intrusion Detection. K. Wang, and S. J. Stolfo. RAID 2004. English Shellcode. J. Mason, S. Small, F. Monrose, and G. MacManus. CCS '09	

Date	Topic	Lectures/Readings	Presenter & slides
Sep 27	Intrusion Detection	Anomaly Detection of Web-based Attacks. C. Kruegel, and G. Vigna. CCS '03 [Optional] Detecting Intrusion Using System Calls. C. Warrender, S. Forrest, and B. Pearlmutter. Oakland'99	Project Proposal Due
Oct 2	Worm	How to 0wn the Internet in Your Spare Time. S Staniford, V Paxson, and N Weaver. USENIX'02 Automated Worm Fingerprinting. S. Singh, C. Estan, G. Varghese, and S. Savage. OSDI'04 [Optional] Misleading Worm Signature Generators Using Deliberate Noise Injection. R. Perdisci, D. Dagon, W. Lee, P. Fogla, and M. Sharif. Oakland'06	
Oct 4	TCP/IP	Practical Network Support for IP Traceback, S. Savage, D. Wetherall, A. Karlin, and T. Anderson. SIGCOMM'00 [Optional]Off-Path TCP Sequence Number Inference Attack -- How Firewall Middleboxes Reduce Security. Z. Qian, and Z. M. Mao. Oakland'12	
Oct 9	DNS	Increased DNS Forgery Resistance Through 0x20-Bit Encoding. D. Dagon, M. Antonakakis, P. Vixie, J. Tatuya, and W. Lee. CCS'08 [Optional] Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority. D. Dagon, N. Provos, C. P. Lee, and W. Lee. CCS'08	Dr. Zhang

Date	Topic	Lectures/Readings	Presenter & slides
Oct 11	DNS	Measuring and Detecting Fast-Flux Service Networks. T. Holz, C. Gorecki, K. Rieck, F. C. Freiling. NDSS'08 From Throw-Away Traffic to Bots: Detecting the Rise of DGA-based Malware. M. Antonakakis, R. Perdisci, Y. Nadji, N. Vasiloglou, S. Abu-Nimeh, and W. Lee. USENIX'12	Dr. Zhang
Oct 16	Malware	Behavior-based Spyware Detection. E. Kirda, C. Kruegel, G. Banks, G. Vigna, and R. A. Kemmerer. USENIX'06 [Optional] Panorama: Capturing System-Wide Information Flow for Malware Detection and Analysis. H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda. CCS'07	
Oct 18	Malware	A Study of the Packer Problem and Its Solutions. F. Guo, P. Ferrie, and T. Chiueh. RAID'08 [Optional] Ether: Malware Analysis via Hardware Virtualization Extensions. A. Dinaburg, P. Royal, M. Sharif, and W. Lee. CCS'08.	
Oct 23	Malware	Exploring Multiple Execution Paths for Malware Analysis. A. Moser, C. Kruegel, and E. Kirda. Oakland'07. Impeding Malware Analysis Using Conditional Code Obfuscation. M. I. Sharif, Andrea Lanzi, J. T. Giffin, and W. Lee. NDSS'08.	

Date	Topic	Lectures/Readings	Presenter & slides
Oct 25	Malware	BitShred: Feature Hashing Malware for Scalable Triage and Semantic Analysis. Jiyong Jang, David Brumley and Shobha Venkataraman. CCS'11 [Optional] Scalable, Behavior-Based Malware Clustering. U. Bayer, P. Milani, C. Hlauschek, C. Kruegel, and E. Kirda. NDSS'09	
Oct 30	OS	A Virtual Machine Introspection Based Architecture for Intrusion Detection. T. Garfinkel, M. Rosenblum. NDSS'03 [Optional] Backtracking Intrusions. S. T. King, and P. M. Chen. SOSP 2003	
Nov 1	OS	Stealthy Malware Detection Through VMM-Based "Out-of-the-Box" Semantic View Reconstruction. X. Jiang, D. Xu, and X. Wang. CCS'07 [Optional] Lares: An Architecture for Secure Active Monitoring Using Virtualization. B. Payne, M. Carbone, M. Sharif, W. Lee. Oakland'08	
Nov 6	Mobile	Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, and X. Wang. NDSS'11 [Optional] On Lightweight Mobile Phone Application Certification. W. Enck, M. Ongtang, and P. McDaniel. CCS'09	
Nov 8	Mobile	On Attack Causality in Internet-Connected Cellular Networks. P. Traynor, P. McDaniel, and T. La Porta. USENIX'07	

Date	Topic	Lectures/Readings	Presenter & slides
Nov 13	Mobile	Isolating and Analyzing Fraud Activities in a Large Cellular Network via Voice Call Graph Analysis. N. Jiang, Y. Jin, A. Skudlark, W. Hsu, G. Jacobson, S. Prakasam, Z. Zhang. Mobisys'12.	
Nov 15	VoIP	PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance. V. Balasubramaniyan, A. Poonawalla, M. Ahamad, M. Hunter, and P. Traynor. CCS'10 [Optional] Spot Me If You Can: Uncovering Spoken Phrases in Encrypted VoIP Conversations. C. Wright, L. Ballard, S. Coull, F. Monrose, and G. Masson. Oakland'08	
Nov 20	Privacy	Vanish: Increasing Data Privacy with Self-Destructing Data. R. Geambasu, T. Kohno, A. A. Levy, and H. M. Levy. USENIX'09 [Optional] Practical Attack to De-Anonymize Social Network Users. G. Wondracek, T. Holz, E. Kirda, and C. Kruegel. Oakland'10	
Nov 22	Holiday		
Nov 27	Medical Device Security	They Can Hear Your Heartbeats: Non-Invasive Security for Implanted Medical Devices. S. Gollakota , H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. Sigcomm'11	
Nov 29	No Class	Prepare for the project and presentation.	
Dec 4	No Class	Prepare for the project and presentation.	
Dec 6		Project presentation	
Dec 8		Project report due	