WAYNE STATE UNIVERSITY
COLLEGE OF ENGINEERING

Computer Science Department

CSC 6991

Section 001

Topics in Computer Security

Fall 2018

State Hall (STAT) 0403

M W 10:00 A.M. - 11:15 A.M.

http://www.cs.wayne.edu/fengwei/18fa-csc6991/index.html

Instructor:
Name: Dr. Fengwei Zhang
Office location: 5057 Woodward Ave; Suite 14109.3
Phone: 313-577-1648
Email: fengwei@wayne.edu

Office Hours: Monday, Wednesday 11:15 AM - 12:15 PM

Course Description:

The course is designed for students interested in computer security research and helps them get started. It will focus on computer security research topics including system security, web security, mobile security, authentication and password management, privacy and anonymity, hardware security, and attacks. The course centers around readings and discussions; it has a term project. Students are expected to read the assigned papers, answer the posted reading questions, and present papers. The term project is essentially a mini research project that involves building a new system, improving an existing technique, or performing a large case study.

Credit Hours:

3 Credit Hours

Perquisite:

CSC 4290 (Introduction to Computer Networking), CSC 4420 (Computer Operating Systems), and CSC 5270 (Computer Systems Security); or permission of the instructor.

.

Text(s) Book:

No textbook is required for this course. Most of course readings come from seminal papers.

Computer Programs:

No special program is required.

Course contents:

Date	Topic	Reading (tentative)	Speaker/Notes
08/29/2017	Course overview	How to Read an Engineering Research Paper. William G. Griswold. Writing Technical Papers in CS/EE. Henning Schulzrinne. The Elements of Style. Strunk and White.	Fengwei Zhang
09/03/2017	Holiday - University Closed		
09/05/2017	Hardware Isolated Execution Environments	Assigned: SoK: A Study of Using Hardware-assisted Isolated Execution Environments for Security. Fengwei Zhang and Hongwei Zhang. In HASP'16. [Link] Optional: Using Hardware Isolated Execution Environments for Securing Systems, Fengwei Zhang, Ph.D. Thesis. [Link]	Fengwei Zhang
09/10/2017	Transparent Malware Analysis on x86	Assigned: Using Hardware Features for Increased Debugging Transparency. Fengwei Zhang, Kevin Leach, Angelos Stavrou, Haining Wang, and Kun Sun. In S&P'15. [Link] Optional: MalGene: Automatic Extraction of Malware Analysis Evasion Signature. Dhilung Kirat and Giovanni Vigna. In CCS'15. [Link]	
09/12/2017	Transportation Security I	Assigned: Green Lights Forever: Analyzing the Security of Traffic Infrastructure. William Beyer, Branden Ghena, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman. In WOOT'14. [Link] Optional: Hacking US (and UK, Australia, France, etc.) Traffic Control Systems. Cesar Cerrudo. In IOActive Blog 2014. [Link]	\
09/17/2017	Transparent Malware Analysis on ARM	Assigned: Ninja: Towards Transparent Tracing and Debugging on ARM. Zhenyu Ning and Fengwei Zhang. In USENIX Security'17. [Link] Optional: Evading Android Runtime Analysis via Sandbox Detection. Timothy Vidas and Nicolas Christin. In AsiaCCS'14. [Link] BareDroid: Large-Scale Analysis of Android Apps on Real Devices. Simone Mutti, Yanick Fratantonio, Antonio Bianchi, Luca Invernizzi, Jacopo Corbetta, Dhilung Kirat, Christopher Kruegel, Giovanni Vigna. In ACSAC'15. [Link]	
09/19/2017	Denial of Service (DoS) Attack	Assigned: Low-Rate TCP-Targeted Denial of Service Attacks (The Shrew vs. the Mice and Elephants). Aleksandar Kuzmanovic and Edward W. Knightly. In ACM SIGCOMM'03. [Link] Optional: Practical Study of a Defense Against Low-Rate TCP-Targeted DoS Attack. Petros Efstathopoulos. In ICITST'09. [Link] Low-Rate	

		DDoS Attacks Detection and Traceback by Using New Information Metrics. Yang Xiang, Ke Li, and Wanlei Zhou. In TIFS'11. [Link]	
09/24/2017	Car Hacking I	Assigned: Lock It and Still Lose Itâ€"On the (In)Security of Automotive Remote Keyless Entry Systems. Flavio D. Garcia, David Oswald, Timo Kasper, and Pierre PavlidÃ¨s. In UsenixSecurity'16. [Link] Optional: Remote Exploitation of an Unaltered Passenger Vehicle. Charlie Miller and Chris Valasek. In BlackHat USA'15. [Link]	
09/26/2017	Car Hacking II	Assigned: Fingerprinting Electronic Control Units for Vehicle Intrusion Detection. Kyong-Tak Cho and Kang G. Shin. In UsenixSecurity'16. [Link] Optional: Comprehensive Experimental Analyses of Automotive Attack Surfaces. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. In UsenixSecurity'11. [Link]	
10/01/2017	Ransomware	Project Proposals Due Assigned: UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware. Amin Kharaz, Sajjad Arshad, Collin Mulliner, William Robertson, and Engin Kirda. In UsenixSecurity'16. [Link] Optional: CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin Butler. In ICDCS'16 [Link]	
10/03/2017	Term Project Proposal	Proposal Presentations and Discussion	
10/08/2016	Hardware Supported Security	Assigned: Breaking Kernel Address Space Layout Randomization with Intel TSX. Yeongjin Jang, Sangho Lee, and Taesoo Kim. In CCS'16. [Link]	
10/10/2017	Memory Forensic	Assigned: Screen after Previous Screens: Spatial-Temporal Recreation of Android App Displays from Memory Images. Brendan Saltaformaggio, Rohit Bhatia, Xiangyu Zhang, Dongyan Xu, and Golden G. Richard III. In UsenixSecurity'16. [Link] Optional: GUITAR: Piecing Together Android App GUIs from Memory Images. Brendan Saltaformaggio, Rohit Bhatia, Zhongshu Gu, Xiangyu Zhang, Dongyan Xu. In CCS'15 [Link]	
10/15/2017	iOS Security	Assigned: SandScout: Automatic Detection of Flaws in iOS Sandbox Profiles. RË˜azvan Deaconescu, Luke Deshotels, Mihai Bucicoiu, William Enck, Lucas Davi, and Ahmad-Reza Sadeghi. In CCS'16. [Link] Optional: On the Feasibility of Large-Scale Infections of iOS Devices. Tielei Wang, Yeongjin Jang, Yizheng Chen, Pak-Ho Chung, Billy Lau, and Wenke Lee. In UsenixSecurity'14. [Link]	
10/17/2017	Android Security I	Assigned: Going Native: Using a Large-Scale Analysis of Android Apps to Create a Practical Native-Code Sandboxing Policy. Vitor Afonso, Paulo de Geus, Antonio Bianchi, Yanick Fratantonio, Christopher Kruegel, Giovanni Vigna, Adam Doupe, and Mario Polino . In NDSS'16. [Link]	
10/22/2017	Android Security II	Assigned: TaintART: A Practical Multi-level Information-Flow Tracking System for Android RunTime. Mingshen Sun, Tao Wei, and John C.S. Lui. In CCS'16. [Link]	
10/24/2017	Cache	Assigned: CaSE: Cache-Assisted Secure Execution on ARM	

	Security	Processors. Ning Zhang, Kun Sun, and Wenjing Lou, and Y. Thomas Hou. In S&P'16. [Link]	
10/28/2017	IoT Security	Assigned: FlowFence: Practical Data Protection for Emerging IoT Application Frameworks. Earlence Fernandes, Justin Paupore, Amir Rahmati, Daniel Simionato, Mauro Conti, and Atul Prakash. In UsenixSecurity'16. [Link] Optional: Security Analysis of Emerging Smart Home Applications. Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. In S&P'16. [Link]	
10/31/2017	Plausibly Deniable Encryption (PDE)	Assigned: DEFY: A Deniable, Encrypted File System for Log-Structured Storage. Timothy M. Peters, Mark A. Gondree, and Zachary N. J. Peterson. In NDSS'15. [Link] Optional: MobiPluto: File System Friendly Deniable Storage for Mobile Devices. Bing Chang, Zhan Wang, Bo Chen, and Fengwei Zhang. In ACSAC'15. [Link] Mobiflage: Deniable Storage Encryptionfor Mobile Devices. Adam Skillen and Mohammad Mannan. In NDSS'13 and TDSC'14. [Link]	
11/05/2017	TEEs on ARM	Assigned: SKEE: A lightweight Secure Kernel-level Execution Environment for ARM. Ahmed Azab, Kirk Swidowski, Rohan Bhutkar, Jia Ma, Wenbo Shen, Ruowen Wang and Peng Ning. In NDSS'16. [Link] Optional: TrustOTP: Transforming Smartphones into Secure One-Time Password Tokens. He Sun, Kun Sun, Yuewu Wang, Jiwu Jing. In CCS'15. [Link] Hypervision Across Worlds: Real-time Kernel Protection from the ARM TrustZone Secure World. Ahmed Azab, Peng Ning, Jitesh Shah, Quan Chen, Rohan Bhutkar, Guruprasad Ganesh, Jia Ma, and Wenbo Shen. In CCS'14. [Link]	
11/07/2017	Intel SGX II	Assigned: SCONE: Secure Linux Containers with Intel SGX. Sergei Arnautov, Bohdan Trach, Franz Gregor, Thomas Knauth, Andre Martin, Christian Priebe, Joshua Lind, Divya Muthukumaran, Daniel O'Keeffe, Mark L Stillwell, David Goltzsche, Dave Eyers, RÃ¼diger Kapitza, Peter Pietzuch, and Christof Fetzer. In OSDI'16. [Link] Optional: AsyncShock: Exploiting Synchronisation Bugs in Intel SGX Enclaves. Nico Weichbrodt, Anil Kurmus, Peter Pietzuch and Rudiger Kapitza. In ESORICS'16. [Link]	
11/12/2017	BlockChain	Assigned: Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. In S&P'16. [Link] Optional: On the Security and Performance of Proof of Work Blockchains. Arthur Gervais, Ghassan O. Karame, Karl WÃ¼st, Vasileios Glykantzis, Hubert Ritzdorf and Srdjan Capkun. In CCS'16. [Link]	
11/14/2017	Firmware Security	Assigned: A Large-Scale Analysis of the Security of Embedded Firmwares. Andrei Costin, Jonas Zaddach, Aurelien Francillon, and Davide Balzarotti. In UsenixSecurity'14. [Link] Optional: Thunderstrike: EFI firmware bootkits for Apple MacBooks. Trammell Hudson. In 31C3. [Link]	
11/19/2017	Term Project Discussion	Working Class for Term Project (Q & A)	
11/21/2017	Holiday - University Closed		
11/26/2017	Moving Target	Assigned: Survey of Cyber Moving Targets. H. Okhravi, M.A. Rabe, T.J. Mayberry, W.G. Leonard, T.R. Hobson, D. Bigelow, W.W.	

	Defense	Streilein. Technical Report, MIT Lincoln Laboratory, 2013. [Link]	
11/28/2017	Android Malware Unpacking	Assigned: AppSpear: Bytecode Decrypting and DEX Reassembling for Packed Android Malware. Wenbo Yang; Juanru Li; Bodong Li; Junliang Shu; Wenjun Hu; Yuanyuan Zhang; Dawu Gu. In RAID'15. [Link] Optional: DexHunter: Toward Extracting Hidden Code from Packed Android Applications. Yueqian Zhang, Xiapu Luo, Haoyang Yin. In ESORICS'15. [Link]	
12/03/2017	Privacy	Assigned: Protecting Privacy of BLE Device Users. Kassem Fawaz, Kyu-Han Kim, and Kang G. Shin. In UsenixSecurity'16. [Link]	
12/05/2017	Term Project Presentation		
12/10/2017	Term Project Presentation	***Project Final Reports Due***	

Laboratory:

No lab for this course

Course Learning Objectives:

This course offers an in depth introduction to computer security research. Upon successful completion of this class, the student will gain experience in:

- Understand research topics in computer security
- Read the state-of-the-art research papers and point out their strengths and weaknesses
- Learn typical cyber attacks and their defense
- Get started with their own research projects in computer security

Assessment:

- Class Participation: 10%
- Review Questions: 20%
- Class Presentations: 30%
- Term Project: 40%

Grading Scale:

The grades for the course will be based upon the percentages given below

A	90 - 100%	C	70 - 73%
A-	87 - 89%	C-	67 - 69%
B+	84 - 86%	D+	64 - 66%
B	80 - 83%	D	60 - 63%
B-	77 - 79%	D-	57 - 59%
C+	74 - 76%	F	0 - 56%

Religious Holidays:

Because of the extraordinary variety of religious affiliations of the University student body and staff, the Academic Calendar makes no provisions for religious holidays. However, it is University policy to respect the faith and religious obligations of the individual. Students with classes or examinations that conflict with their religious observances are expected to notify their instructors well in advance so that mutually agreeable alternatives may be worked out.

Student Disabilities Services:

- If you have a documented disability that requires accommodations, you will need to register with Student Disability Services for coordination of your academic accommodations. The Student Disability Services (SDS) office is located at 1600 David Adamany Undergraduate Library in the Student Academic Success Services department. The SDS telephone number is 313-577-1851 or 313-202-4216 for videophone use. Once you have your accommodations in place, I will be glad to meet with you privately during my office hours to discuss your special needs. Student Disability Services' mission is to assist the university in creating an accessible community where students with disabilities have an equal opportunity to fully participate in their educational experience at Wayne State University. You can learn more about the disability office at www.studentdisability.wayne.edu.

- To register with Student Disability Services, complete the online registration form at: https://wayne-accommodate.symplicity.com/public_accommodation/

Academic Dishonesty - Plagiarism and Cheating:
Academic misbehavior means any activity that tends to compromise the academic integrity of the institution or subvert the education process. All forms of academic misbehavior are prohibited at Wayne State University, as outlined in the Student Code of Conduct (http://www.doso.wayne.edu/student-conduct-services.html). Students who commit or assist in committing dishonest acts are subject to downgrading (to a failing grade for the test, paper, or other course-related activity in question, or for the entire course) and/or additional sanctions as described in the Student Code of Conduct.

- **Cheating:** Intentionally using or attempting to use, or intentionally providing or attempting to provide, unauthorized materials, information or assistance in any academic exercise. Examples include: (a) copying from another student's test paper; (b) allowing another student to copy from a test paper; (c) using unauthorized material such as a "cheat sheet" during an exam.
- **Fabrication:** Intentional and unauthorized falsification of any information or citation. Examples include: (a) citation of information not taken from the source indicated; (b) listing sources in a bibliography not used in a research paper.
- **Plagiarism:** To take and use another's words or ideas as one's own. Examples include: (a) failure to use appropriate referencing when using the words or ideas of other persons; (b) altering the language, paraphrasing, omitting, rearranging, or forming new combinations of words in an attempt to make the thoughts of another appear as your own.

- **Othe**r forms of academic misbehavior include, but are not limited to: (a) unauthorized use of resources, or any attempt to limit another student's access to educational resources, or any attempt to alter equipment so as to lead to an incorrect answer for subsequent users; (b) enlisting the assistance of a substitute in the taking of examinations; (c) violating course rules as defined in the course syllabus or other written information provided to the student; (d) selling, buying or stealing all or part of an un-administered test or answers to the test; (e) changing or altering a grade on a test or other academic grade records.

Course Drops and Withdrawals:

There will be no in-completes given for the course.

In the first two weeks of the (full) term, students can drop this class and receive 100% tuition and course fee cancellation. After the end of the second week there is no tuition or fee cancellation. Students who wish to withdraw from the class can initiate a withdrawal request on Pipeline. You will receive a transcript notation of WP (passing), WF (failing), or WN (no graded work) at the time of withdrawal. No withdrawals can be initiated after the end of the tenth week. Students enrolled in the 10th week and beyond will receive a grade. Because withdrawing from courses may have negative academic and financial consequences, students considering course withdrawal should make sure they fully understand all the consequences before taking this step. More information on this can be found at:
http://reg.wayne.edu/pdf-policies/students.pdf

Student services:

- The Academic Success Center (1600 Undergraduate Library) assists students with content in select courses and in strengthening study skills. Visitwww.success.wayne.edu for schedules and information on study skills workshops, tutoring and supplemental instruction (primarily in 1000 and 2000 level courses).
- The Writing Center is located on the 2nd floor of the Undergraduate Library and provides individual tutoring consultations free of charge. Visit http://clasweb.clas.wayne.edu/writing to obtain information on tutors, appointments, and the type of help they can provide.

Class recordings:

Students need prior written permission from the instructor before recording any portion of this class. If permission is granted, the audio and/or video recording is to be used only for the student's personal instructional use. Such recordings are not intended for a wider public audience, such as postings to the internet or sharing with others. Students registered with Student Disabilities Services (SDS) who wish to record class materials must present their specific accommodation to the instructor, who will subsequently comply with the request unless there is some specific reason why s/he cannot, such as discussion of confidential or protected information.

Other issues

- Foods and drinks are not allowed during the lecture or lab hours.
- Cell phones and other two-way communication devices: Students are expected to turn off their devices or turn them to the silent mode when they come to the lecture or to the

lab. If a device is used in any way in the lab, you will receive a verbal warning first and then you will be asked to leave immediately.