WAYNE STATE UNIVERSITY
COLLEGE OF ENGINEERING

Computer Science Department

CSC 6991

Section 002

Topics in Computer Science - Advanced Computer Security

Fall 2015

0015 PERN

M W 11:00 A.M. – 12:20 P.M.

http://www.cs.wayne.edu/fengwei/15fa-csc6991/index.html

Instructor:
Name: Dr. Fengwei Zhang
Office location: 5057 Woodward Ave; Suite 14109.3
Phone: 313-577-1187
Email: fengwei@wayne.edu

Office Hours: Monday, Wednesday 10:00 AM - 11:00 AM

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
09/02/2015	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
09/07/2015	Holiday - University Closed		
09/09/2015	Isolated Execution Environments	Using Hardware Isolated Execution Environments for Securing Systems, Fengwei Zhang, Ph.D. Thesis.	Fengwei Zhang
09/14/2015	Memory Attacks and Introspection	SPECTRE: A Dependable Introspection Framework via System Management Mode. Fengwei Zhang, Kevin Leach, Kun Sun, and Angelos Stavrou. In DSN'13.	Fengwei Zhang
09/16/2015	Transparent Malware Analysis I	Using Hardware Features for Increased Debugging Transparency. Fengwei Zhang, Kevin Leach, Angelos Stavrou, Haining Wang, and Kun Sun. In S&P'15. MalGene: Automatic Extraction of Malware Analysis Evasion Signature. Dhilung Kirat and Giovanni Vigna. In CCS'15.	Fengwei Zhang
09/21/2015	Transparent Malware Analysis II	Evading Android Runtime Analysis via Sandbox Detection. Timothy Vidas and Nicolas Christin. In AsiaCCS'14. Morpheus: automatically generating heuristics to detect Android emulators.Yiming Jing, Ziming Zhao, Gail-Joon Ahn, and Hongxin Hu. In ACSAC'14.	
09/23/2015	DDoS Attack	Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics. Yang Xiang, Ke Li, and Wanlei Zhou. In TIFS'11. Delving into Internet DDoS Attacks by Botnets: Characterization and Analysis. An Wang, Aziz Mohaisen, Wentao Chang, Songqing Chen. DSN'15.	
09/28/2015	Car Hacking I	Remote Exploitation of an Unaltered Passenger Vehicle. Charlie Miller and Chris Valasek. In BlackHat USA'15.	

09/30/2015	Car Hacking	Comprehensive Experimental Analyses of Automotive Attack Surfaces. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. In UsenixSecurity'11.	
10/05/2015	OS Security	ret2dir: Rethinking Kernel Isolation. Vasileios P. Kemerlis, Michalis Polychronakis, and Angelos D. Keromytis. In UsenixSecurity'14.	
10/07/2015	DMA Attacks	Run-DMA. Gorka Irazoqui, Michael Rushanan and Stephen Checkoway. In WOOT'15. Understanding DMA Malware. Patrick Stewin and Iurii Bystrov. In DIMVA'12.	
10/12/2015	Password Management	Password Managers: Attacks and Defenses. David Silver, Suman Jana, Dan Boneh, Eric Chen and Collin Jackson. In UsenixSecurity'14.	
10/14/2015	TrustZone on ARM	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. TrustICE: Hardware-assisted Isolated Computing Environments on Mobile Devices. He Sun, Kun Sun, Yuewu Wang, Jiwu Jing, and Haining Wang. In DSN'15.	
10/19/2015	iOS Security	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.	
10/21/2015	Android Security I	Leave Me Alone: App-level Protection Against Runtime Information Gathering on Android. Nan Zhang, Kan Yuan, Muhammad Naveed, Xiaoyong Zhou, and XiaoFeng Wang. In S&P'15. Effective Real-time Android Application Auditing. Mingyuan Xia, Lu Gong, Yuanhao Lv, Zhengwei Qi, Xue Liu. In S&P'15.	
10/26/2015	Android Security II	Android Permissions Remystified: A Field Study on Contextual Integrity. Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, Konstantin Beznosov. In UsenixSecurity'15. What the App is That? Deception and Countermeasures in the Android User Interface. Antonio Bianchi, Jacopo Corbetta, Luca Invernizzi, Yanick Fratantonio, Christopher Kruegel and Giovanni Vigna. In S&P'15.	
10/28/2015	ROP Attack	The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86). Hovav Shacham. In CCS'07.	
11/02/2015	Bitcoin	SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. In In S&P'15.	

11/04/2015	Cloud Side Channels	S$A: A Shared Cache Attack that Works Across Cores and Defies VM Sandboxing-and its Application to AES. Gorka Irazoqui, Thomas Eisenbarth, and Berk Sunar. In S&P'15. Nomad: Mitigating Arbitrary Cloud Side Channels via Provider-Assisted Migration. Soo-Jin Moon, Vyas Sekar, and Michael K. Reiter. in CCS'15.	
11/09/2015	Memory Forensic	DSCRETE: Automatic Rendering of Forensic Information from Memory Images via Application Logic Reuse. Brendan Saltaformaggio, Zhongshu Gu, Xiangyu Zhang, and Dongyan Xu. In UsenixSecurity'14.	
11/11/2015	Semantic Gap Problem	SoK: Introspections on Trust and the Semantic Gap. Bhushan Jain, Mirza Basim Baig, Dongli Zhang, Donald E. Porter, and Radu Sion. In S&P'14.	
11/16/2015	Software Guard Extensions (SGX)	Shielding Applications from an Untrusted Cloud with Haven. Andrew Baumann, Marcus Peinado, and Galen Hunt. In OSDI'14. Innovative Instructions and Software Model for Isolated Execution. Frank Mckeen, Ilya Alexandrovich, Alex Berenzon, Carlos Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday Savagaonkar. In HASP'13.	
11/18/2015	Plausibly Deniable Encryption (PDE)	Mobiflage: Deniable Storage Encryptionfor Mobile Devices. Adam Skillen and Mohammad Mannan. In NDSS'13 and TDSC'14.	
11/23/2015	Moving Target Defense	Survey of Cyber Moving Targets. H. Okhravi, M.A. Rabe, T.J. Mayberry, W.G. Leonard, T.R. Hobson, D. Bigelow, W.W. Streilein. Technical Report, MIT Lincoln Laboratory, 2013.	
11/25/2015	Holiday - University Closed		
11/30/2015	Firmware Security	A Large-Scale Analysis of the Security of Embedded Firmwares. Andrei Costin, Jonas Zaddach, Aurelien Francillon, and Davide Balzarotti. In UsenixSecurity'14. Thunderstrike: EFI firmware bootkits for Apple MacBooks. Trammell Hudson. In 31C3.	
12/02/2015	Web Security	ZigZag: Automatically Hardening Web Applications Against Client-side Validation Vulnerabilities. Michael Weissbacher, William Robertson, Engin Kirda, Christopher Kruegel and Giovanni Vigna. In UsenixSecurity'15.	
12/07/2015	Privacy in Pharmacogenetics	Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing. Matthew Fredrikson, Eric Lantz, Somesh Jha, Simon Lin, David Page and Thomas Ristenpart. In UsenixSecurity'14.	
12/09/2015	Term Project		

	Presentation		
12/14/2015	Term Project Presentation		

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 in the Adamany Undergraduate Library. The SDS telephone number is 313-577-1851 or 313-202-4216 (Videophone use only). Once your accommodation is in place, someone can meet with you privately 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.
- Students who are registered with Student Disability Services and who are eligible for alternate testing accommodations such as extended test time and/or a distraction-reduced environment should present the required test permit to the professor at least one week in advance of the exam. Federal law requires that a student registered with SDS is entitled to the reasonable accommodations specified in the student's accommodation letter, which might include allowing the student to take the final exam on a day different than the rest of the class.

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.