DEPAUL | COLLEGE OF COMPUTING AND DIGITAL MEDIA

9/11/16

Course Information

Course ID: CNS378
Name: Host Based Security
Quarter: Fall 2016-2017
Meeting time: TuTh 3:10PM - 4:40PM
Location: CDM 00228 at Loop Campus
Type of Instruction: lecture / lecture-discussion / lab

Instructor Information

Instructor: Filipo Sharevski
Office: Loop Campus, CDM 750
Office Hours: http://www.cdm.depaul.edu/about/pages/people/facultyinfo.aspx?fid=1341
Other times by appointment (email/text me with your request)
Office Telephone: Loop - 312-362-1075
Email: fsharevs@cdm.depaul.edu
Mobile: 765-714-9574
Skype : filipotech

Important Dates

September 13, 2016	Last day to add (or swap) classes to AQ2016 schedule
September 20, 2016	Last day to drop classes with no penalty.
September 20, 2016	Last day to select pass/fail option
September 21, 2016	Grades of "W" assigned for classes dropped on or after this day
October 25, 2016	Last day to withdraw from AQ2016 classes
November 16, 2016	End AQ2016 quarter. All assignments due.

Prerequisites

Basic knowledge of operating systems: CSC 374: Computer Systems II or TDC 311: Computers in Telecommunication Systems or IT 373: System Concepts. A bit of programming. An ability to look at things the way they were not supposed to be seen.

Course Description

Principles of host based security. Review of security methods used to ensure the confidentiality, integrity, and availability of the information stored on a host. The class will cover the basics of information security, operating systems' protections (identification, authentication, access control, and authorization), formal security modeling, software security (software vulnerabilities, control flow hijacking, and malware), web security, host-based protection (firewalls, intrusion detection/prevention systems) and information security compliance. Course includes laboratory work covering the practical implementation of the security principles elaborated in the lectures.

Textbook

There will be no required textbook. All of the course materials will be available on the D2L course page. Feel free to ask me on any security-related resources (books, papers, blogs, feeds, etc.…) for recommendation.

Course Objectives

At the conclusion of the course, students will be able to:

- Understand, detect and contextualize causes for hosts' cyber insecurity
- Understand, implement and develop cybersecurity protection techniques – (hands-on experience)
- Think critically about:
    - Relationship - data, application, host, perimeter, and network security
    - Role of a cybersecurity expert
    - Broader set of factors affecting the security of cyberspace
    - Future threats, cyber protection trends and potential solutions
- Respond in face of new cybersecurity exploits, campaigns, latest trends, and novel developments

Agenda

Week	Date	Topic	Assignment	Reading (Recommended)
Week 1	09/09/2016	**Course Overview:** Walkthrough, Learning Objectives Logistics, Deliverables, Cybersecurity News and Lessons		Charles Fleeger: *The fundamentals of information security*
Week 2	09/13/2016	**Security Basics:** Foundations, Symmetric and Asymmetric Cryptography	Choose a Cybersecurity Report to review	Shafi Goldwasser and Mihir Bellare: *Lecture Notes On Cryptography*
	09/15/2016	**Security Basics:** Cryptographic hash functions, MACs, Digital signatures	Choose a Topic for your final paper	
Week 3	09/20/2016	**System Security:** Identification and Authentication Concepts	Lab 1 – Linux Access Control http://www.cis.syr.edu/~wedu/seed/Labs_12.04/System/Capability_Exploration/	Weir et al: *Testing Metrics for Password Creation Policies*; Chen et al: *Setuid Demystifie;* Linux File Permissions
	09/22/2016	**System Security:** Access Control and Authorization Concepts		
Week 4	09/27/2016	**Unix Security:** Identification and Authentication, File Permissions		Trent Jaeger: *Security in Ordinary Operating Systems* (Chapter 4 in *Operating Systems Security*)
	09/29/2016	**Windows Security:** Registry, Active Directory, Access Control		
Week 5	10/04/2016	**Formal Security:** Multi-level security, Security Policies, Bell-LaPadula Model	Lab 2 – Shellshock Attack http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Software/Shellshock/	Troy Hunt and Jim Manico: *Understanding the Shellshock Bug* https://www.pluralsight.com/courses/shellshock-bash-bug
	10/06/2016	**Formal Security:** Integrity models, Common Criteria for Information Technology Security Evaluation (ISO 15408)		

Week 6	10/11/2016	**Software Security:** Software vulnerabilities, control flow manipulation	Lab 3 – Buffer Overflow vulnerability http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Software/Buffer_Overflow/	Ken Thompson: *Reflections of Trusting Trust*; Cowan et. al: *Attacks and Defenses for the Vulnerability of the Decade*
	10/13/2016	**Software Security:** Malware and Anti-Malware Protection		
Week 7	10/18/2016	**Web Security:** Browser security model, code injection attacks [cross-site scripting]	Lab 4 Part 1 – XSS Attack http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_XSS_Elgg/	Amit Klein: *Cross Site Scripting Explained*
	10/20/2016	**Web Security:** code injection attacks [cross-site request forgery, SQL injection]	Lab 4 Part 2 - CSRF Attack http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Web/Web_CSRF_Elgg/	Adam Barth, Collin Jackson, and John C. Mitchell: *Robust Defenses for Cross-Site Request Forgery*
Week 8	10/25/2016	**Internet Security:** Firewalls – filtering, application gateways, DPI	Lab 5 – Linux Firewall Exploration Lab: http://www.cis.syr.edu/~wedu/seed/Labs_12.04/Networking/Firewall_Linux/	NIST SP 800-41 Rev. 1. *Guidelines on Firewalls and Firewall Policy*; Axelsson *The base-rate fallacy implication for IDS*s
	10/27/2016	**Internet Security:** Intrusion detection systems, Intrusion tolerance		
Week 9	11/01/2016	**Mobile Security:** Android and iOS – Concepts, Threats and Malware	Upload your final papers and presentations	Faruki et. al: *Android Security: A Survey of Issues, Malware Penetration and Defenses*
	11/03/2016	**Risk Analysis:** Information Security Management		
Week 10	11/08/2016	**Presentations**		
	11/10/2016	**Presentations**		
Week 11	11/15/2016	**Presentations**		

Grading

Grading is based on the manner in which you fulfill the objectives of this course. I will grade all your assignments on a percentage basis, which I will then convert to a letter. I will convert percentages to letters based on the following schedule:

Percentage Grade	Letter Grade	Manner of fulfillment
92-100	A	Excellent
90-91	A-	
88-89	B+	
82-87	B	Very Good
80-81	B-	
78-79	C+	
72-77	C	Satisfactory
70-71	C-	
68-69	D+	
62-67	D	Poor
60-61	D-	
0-59	F	

The weights of each assignment for contributing to the final average are as follows:

Assignment	Weight in final grade
Five Labs	5 x 10% = 50%
Security of Cyberspace – Review Paper	10%
Paper	25%
Final Presentation	10%
Class Participation	5%

Assignments Delivery

The review paper is due a week it is assigned at 11:59 PM. The final paper is due to the end of the presentation weeks. The labs are due two weeks after each is assigned. I will accept late homework according the following schedule:

$$p = \log_2(2 - \frac{d}{14})$$

where *p* is the percentage applied to the earned grade and *d* is the number of days the homework is submitted late. The tentative dates are (subject of change, it will be dully communicated in class and through the D2L)

Assignment	Due Date (11:59 PM)
Security of Cyberspace – Review Paper	9/22/2016
Lab 1	10/13/2016
Lab 2	10/20/2016
Lab 3	10/27/2016
Lab 4.1	11/01/2016
Lab 4.2	11/03/2016
Final Presentation	11/03/2016
Lab 5	11/10/2016
Final Paper	11/15/2016

Laboratory Exercises

There will be five laboratory exercises corresponding to the course material and all of them can be carried out on your own machines (no physical lab needed). Contact me if you need any assistance in regards the lab setup or if you experience glitches while you are experimenting. Details on the lab environment setup, lab manuals, and the exercise reporting are provided in the D2L section “Laboratory Exercises”. These labs are designed for you to work individually, however, I encourage collaboration and working in groups. Your reports stay individual, though, and I expect to recognize clear engagement with the lab contents on your side.

Security of Cyberspace – Review Paper

You will have to choose one of the mid 2016 cybersecurity reports posted on D2L under the "Security of Cyberspace - Reports" section and write a critical review paper on the topic covered, your take on the report, and the perspectives on the overall state of cyberspace security. Not more than three students can pick the same report; you are encouraged to look online beyond the recommended ones and chose an appropriate report. Send me an email with your preference no later than the end of the first week and I will come back with the final report assignment for the entire class. For the paper formatting guidelines, see the section below.

Final Paper

There will be a final white/research paper due near the end of the course. This will be a paper on a topic of your choosing in the area of cybersecurity. You can provide detail analysis of a cybersecurity problem and available/potential solutions, survey current challenges and issues, or conduct an actual cybersecurity research and report the results. The topic has to be communicated with me no later than the second week of the semester in order to be approved. Working in groups not more than two are paper/project specific and require prior approval from me. To successfully complete this assignment, you will have to read and include content from published papers, books, and validated information sources outside of the reading material available for the course. Use DePaul's University Library as a rich repository for wide range of scientific papers and content available for free to you as students. There is no page/word count limit, however, the paper is expected to commensurate with an academic-level work. For the paper formatting guidelines and reference citation, see the section below.

Final Presentation

All students will create a slide show/web site on your final paper for the entire class. In addition, you will present your site/show sometime during the last week of class and finals week. There will be no final exam. This is the Doddle Poll for you to choose your presentation time slot [presentation time – 7 minutes]
http://doodle.com/poll/9yzrz5288yhffspa

[Online Students Only] - You will deliver your presentation for me to present in one of the final class presentations weeks. Subscribe to the poll as you prefer your presentation to be delivered [not all in the last week, have in mind I have to give your presentation].

Paper Formatting Guidelines

Papers have to be formatted and delivered according to the template under the "Paper Formatting" section in D2L course page. You can choose either IEEE or APA6 citation format. I encourage usage of citation software (Mendeley, Zotero, EndNote…). You can use a word processor of your choice. If you feel that you need help on the citation part, feel free to consult the citation materials provided, the *Publication manual of the American Psychological Association*, or any validated source on IEEE or APA6 citation. I strongly encourage you to pay a visit or schedule an appointment with the University Center for Writing-Based Learning: http://condor.depaul.edu/writing/

Attendance

I expect that you will attend every class; it is the single most important action you can take in mastering the course objectives. You are responsible for material covered, assignments delivered or received, and announcements made in class sessions or on the class web site.

Class Participation

I expect that you will actively participate in every class discussion; it is the one of the most important actions in mastering a critical cybersecurity thinking.

[Online Students Only] You will bring your comments on the D2L discussion forum for each topic we discuss in class.

Class Cancellation

Unless DePaul University closes because of weather, we will have class.

Incompletes

Students must formally request an incomplete by filling out an Incomplete Grade Request Form.

Academic Integrity

I expect that you have read and understood DePaul's policy on Academic Integrity (http://academicintegrity.depaul.edu/). It is part of this syllabus; follow it.

Changes to Syllabus

This syllabus is subject to change as necessary to better meet the needs of the students. Significant changes are unlikely, and will be thoroughly addressed in class. Minor changes, especially to the weekly agenda, are possible at any time. You will be informed of all such changes.

Online Course Evaluations

Evaluations are a way for students to provide valuable feedback regarding their instructor and the course. Detailed feedback will enable the instructor to continuously tailor teaching methods and course content to meet the learning goals of the course and the academic needs of the students. They are a requirement of the course and are key to continue to provide you with the highest quality of teaching. The evaluations are anonymous; the instructor and administration do not track who entered what responses. A program is used to check if the student completed the evaluations, but the evaluation is completely separate from the student's identity. Since 100% participation is our goal, students are sent periodic reminders over three weeks. Students do not receive reminders once they complete the evaluation. Students complete the evaluation online in CampusConnect.

Academic Policies

All students are required to manage their class schedules each term in accordance with the deadlines for enrolling and withdrawing as indicated in the University Academic Calendar. Information on enrollment, withdrawal, grading and incompletes can be found at: http://www.cdm.depaul.edu/Current%20Students/Pages/PoliciesandProcedures.aspx

Students with Disabilities

Students who feel they may need an accommodation based on the impact of a disability should contact the instructor privately to discuss their specific needs. All discussions will remain confidential. To ensure that you receive the most appropriate accommodation based on your needs, contact the instructor as early as possible in the quarter (preferably within the first week of class), and make sure that you have contacted the Center for Students with Disabilities (CSD) at: csd@depaul.edu.
Lewis Center 1420, 25 East Jackson Blvd.
Phone number: (312)362-8002
Fax: (312)362-6544
TTY: (773)325.7296

Tips

1. Writing a scientific paper is a time-consuming and intensive task. Don't procrastinate after we decided on your paper topics and wait until the last week to start searching for material and writing. Feel free to ask for suggestions during your researching and writing process, I am glad to help.

2. Don't be afraid to approach for help on any issue if you are experiencing any learning difficulties. I don't want you to gradually fall behind over the semester until things become untenable.

3. Participate actively in discussion sections. Developing critical thinking skills – essential for getting into the cybersecurity mindset – is through interactive learning and class discussions.