COMP 7/8327: Network and Internet Security Spring'22

Instructor: Dipankar Dasgupta Class: UM GLOBAL (M50)

COURSE MOTIVATION & OBJECTIVES:

As the cyber become mainstream in our day-to-day activities and cyber criminals are increasingly launching sophisticated multi-stage targeted attacks to disrupt, gain access, exploit systems, services and information. Internet access mobility, its openness, anonymity allowing underlying unsecure technology to be abused for fraud, identity theft, data breach and ransom attacks in businesses, social media, e-government and other cyber-enabled services.

The course covers both the principles and practice of the Internet and Network security; help students to understand complex attack paths and countermeasures not only for a specific system but also for a class of computing systems with different hardware/software components and architecture. This course provides some hands-on experience in security-related tools and technologies. One of the important components of the course is a term project that will allow students to do extensive study/research on current topics in network and Internet security.

PREREQUISITES: COMP 7120 / COMP 6410 and COMP 6310 or permission of the instructor.

Course Syllabus (The following topics will be covered through teaching, selected reading and project activities subject to availability of time):

- **Quick Review** of Cryptography, Networking, Virus & Worms, basic security issues and countermeasures; **Communication Security**: IP Concepts, Protocols (IPv4, v6), Mobile IP, Covert Channels and DNS.
- **Defense in Depth techniques & tools:**
  * Authentication, Authorization, Access Control, Password Management and user Attribution, etc.
  * Intrusion Detection and Prevention Systems, Monitoring & Response
  * Virtualization and Cloud Security, Moving Target Defense, Zero-Trust Architecture, etc.
  * Firewall, Filtering and Proxying Tools, Virtual Private networks (VPN)
  * Security Risk Management and Responses: Vulnerability analysis techniques
- **Various Internet Security topics:** Wireless Security, Advanced Persistent Threats (APTs), Insider Threats
- Security Policy, Risk Analysis, Security Metrics, Incident Response, Security visualization
- Topics on Computational Intelligence (AI/ML) in Cyber Security

Suggested Textbooks/References:

1. **Network Security Essentials: Application and Standards (6th edition) by William Stallings. Pearson 2017**
2. **Computer Security: A Hands-On Approach, Wenliang Du, October 2017**
3. **Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization Nov 24, 2014 by Tyler Wrightson**
4. **Moving Target Defense II: Application of Game Theory and Adversarial Modeling (Advances in Information Security, by Sushil Jajodia and Anup K. Ghosh, Oct 15, 2014**
5. **Internet Security: How to Defend Against Attackers on the Web, by Mike Harwood, 2nd edition 2016 ISBN: 978-1-284-09055-0**
6. **Rootkits and Bootkits: Reversing modern malware and Next Generation Threats by Alex Matrosov, Eugene Rodionov, and Sergey Bratus Spring 2016, 304 pp. ISBN: 978-1-59327-716-1**
7. **Selected Reading**

COMP 7/8327 **Network & Internet Security** **Spring 2022**

Instructor: Dr. Dipankar Dasgupta
Email: dasgupta@memphis.edu

Room: Virtual/M50

Evaluation:

Students are expected to login to class every day and check the discussion boards and the assignments and activities mention weekly. The evaluation process will include paper presentations, assignments, software testing, tests (or quizzes), and a term project to make sure that you have integrated the material into your general practice of secure computing. Students registered for COMP 8327 will have to do some additional work.

Your final grade for the course will be based on the grades in the following course-related activities (given in percentages):

Grading:

Presentations	10%
Tests/quizzes/Exams	40%
Experiments/Assignments	25%
Final project + proposal	25%

Grading Scale:

A+	95.1-100	**B+**	85.1 - 88	**C+**	76.1 – 79	**D+**	60.1-66
A	90.1 – 95	**B**	82.1- 85	**C**	70.1 – 76	**D**	50 - 60
A-	88.1 – 90	**B-**	79.1 - 82	**C-**	66.1 – 70	**F**	< 50

Term Project:

The project (on cyber security) is one of the important components of the course. The topic/problem needs to be approved by the instructor. This individual project needs to be completed into three phases:

Phase 1:
Submission of the project proposal:

A one-page proposal (identifying techniques/software/methods to solve the given security problem, provides references) of worth 5% (of the project's grade) must be submitted to the instructor for approval. There will be one student for each project.
Due date: (2/26/2022).

Phase 2:
Project Progress Presentation (on Implementation of the project): March 26th

Phase 3:
Final Demo and report of the project:

Your final project report should be 6 to 8 pages long. You must implement the approved project. You need to search on the web for the references and for further resources. Also, feel free to think and propose others (new ideas) that may better solve the problem.

Due date: Project presentation/demo on the last day of class. It will be extremely difficult to get any extensions, so plan on finishing by the due date.

Ethical behavior/ Academic Integrity/Plagiarism:

Ethical behavior is an important part of this course. Since some of the methods, codes and tools that will be discussed and experimented in the course can be very harmful, if abused, it is expected that students will behave in a responsible fashion. In particular, always ask your local site administrator for permission before experimenting with security-related tools. In-class discussions of techniques for exploiting potential security threats and risks do not imply to use them! You will be sole responsible for any such violation.

The Office of Student Accountability provides university's academic integrity policy to promote academic integrity and prevent academic misconduct specifically in the online learning environment.

Plagiarism or cheating behavior in any form is unethical and detrimental to proper education and ***will not be tolerated.*** All work submitted by a student (projects, programming assignments, lab assignments, quizzes, tests, etc.) is expected to be a student's own work. The plagiarism is incurred when any part of anybody else's work is passed as your own (no proper credit is listed to the sources in your own work) so the reader is led to believe it is therefore your own effort. Students are allowed and encouraged to discuss with each other and look up resources in the literature (including the internet) on their assignments, but ***appropriate references must be included for the materials consulted***, and appropriate citations made when the material is taken verbatim.

If plagiarism or cheating occurs, the student will receive a failing grade on the assignment and (at the instructor's discretion) a failing grade in the course. The course instructor may also decide to forward the incident to the University Judicial Affairs Office for further disciplinary action. For further information on U of M code of student conduct and academic discipline procedures, please refer to: **http://www.memphis.edu/studentconduct/pdfs/csrr.pdf** and the student handbook and planner **.**

"Your written work may be submitted to Turnitin.com, or a similar electronic detection method, for an evaluation of the originality of your ideas and proper use and attribution of sources. As part of this process, you may be required to submit electronic as well as hard copies of your written work, or be given other instructions to follow. By taking this course, you agree that all assignments may undergo this review process and that the assignment may be included as a source document in Turnitin.com's restricted access database solely for the purpose of detecting plagiarism in such documents. Any assignment not submitted according to the procedures given by the instructor may be penalized or may not be accepted at all." (Office of Legal Counsel, October 17, 2005.

==========

SPRING 2022 TENTATIVE SCHEDULE COMP 7/8327

Week 1: Course Aims & Agenda, Pre-requisite topics: review of basic security issues, cyber threads, Model for Network Security, Selected

reading (pre-requisite): Cryptography overview-DES, AES, MD5, Digital Signature, homomorphic encryption, etc.

Week 2: – Networking & security issues – Review IP concepts, network protocols, Mobile IP, DNS; Vulnerability-CVSS, CVE, etc.

First Assignment

Week 3: Intrusion Detection Systems (IDS): Host-based, Network-based and Application-based, Attack Taxonomy, Traffic analysis, security monitoring tools, etc. CI technique

Week 4: Authentication and Access control, Password and Attack methods, IP Security, Protocol security issues, CI technique

Lab Exercise/Second Assignment

Week 5: Scanning and sniffing tools, Security Policy, threat model and risk analysis, NMAP Experiments

Week 6: Advanced Malware, bugs, Virus and Worm, Antivirus tools, scanning and sniffing tools, Integrity checker: tripwire, etc.

Lab Exercise /
Submission of the project proposal

Week 7: Firewalls, Experimenting Security tools and software (**demo**)

Third Assignment/Lab Exercise

Week 8: {***Break***}

Week 9: Virtualization security, Cloud Security, APTs,

Week 10: Wireless Network Security: Wireless Threats, Wireless Security Protocols; sensor network security, Web, OS Security– Windows/Unix security, System log files, protocol, Insider Threat analysis, etc.

Reporting Project Progress

Week 11: Moving Target Defense, Experimenting Security tools and software, User Attribution and OSN Security and Privacy issues.

Week 12: Reverse engineering, Static and dynamic analysis, Basics of x86 Assembly language, Factors that limit static assembly

Lab Exercise/Fourth Assignment

Week 13: Intelligent Defense: Building a machine learning-based security solutions--Feature space and decision boundaries, Overfitting and underfitting

Week 13: Secure Software, Mobile code, NIST Guidelines, Govt. standards e.g. AR 25-2, INFOSEC 1-99, COMSEC Policy, ITSEC, Honeypots, Botnet

Week 14: ***Project Presentations:***
Give Presentation, Demo & Submission of Project Report

NOTE 1: We plan to have some Lab exercises and demo with various tool and Techniques. However, for any technical reason if the Lab session needs to be cancelled, we will have lecture session, or an alternative arrangement will be made.

NOTE 2: Tests/Quizzes/Exams will be scheduled in every week or alternate weeks, but students should come prepared (on previous lectures and topics covered) for Quiz in each class.

NOTE 3: All course-related information will be available from elearn.memphis.edu. Check the course Web page at http://elearn.memphis.edu for class notes and updated information.

NOTE 4: If I need to communicate with the class as a group, I'll be using elearn email. You may need to check your email regularly.

Important Web links:

- Internet Storm Center (SANS)
- United States Computer Emergency Response Team (US-CERT)
- Stay Safe Online.Org (National Cyber Security Alliance)
- http://sectools.org/
- National Vulnerability Database (NVD)
- DCN-Network Security
- NIST Publications

Suggested Project Topics:

• *Web Security*	• *IoT Security*
• *Cloud Security*	• *Moving Target Defense*
• *Mobile device security*	• *Social Networks security & Privacy issues*
• *Insider Threat detection*	• *Sensor Network Security*
• *Advanced Persistent Threats*	• *Smart Grid/City Security*
• *Continuous Authentication & Identity Management*	• *Packet Analysis or Malware Analysis*