COMP 4/6420: Network and Mobile Security

Instructor: Dr. Kan Yang

Times: 1:00 pm – 2:25 pm | Days: T/R | Place: Fogelman Classroom Building 127

Contact Information:

Office: 305 Dunn Hall	Department Office: 375 Dunn Hall
Phone: 901-678-3139	Department Phone: 901-678-5465
E-mail: kan.yang@memphis.edu	URL: cs.memphis.edu
TA: TBD	
Course Website: https://www.cs.memphis.edu/~kanyang/COMP4420-fall22.html	

Office Hour: By appointment via email.

Course Description:

This course will discuss security issues and solutions in computer and mobile networks. Topics include Web Security (web security mode, web application security), Cryptography (symmetric cryptography, public-key cryptography, SSL/TLS, and other crypto tools), Network Security (security issues in network protocols, network defense tools, DoS attacks, etc.), Mobile Security (mobile platform security models, mobile threats and malware), and Cloud Security.

Why This Course?

Cyber security has become one of the most significant concerns in computer network and mobile systems, which have been widely used in our daily life. It helps businesses meet mandatory compliance regulations, protect customer data, and reduce the risk of legal action. It is vital for computer science students to gain the knowledge of analyzing security vulnerabilities and designing security solutions in today's network and mobile systems. In this course, students will be able to learn the fundamental security issues and defenses techniques in network and mobile systems.

Textbooks

Internet Security: A Hands-on Approach 3rd Edition (ISBN: 978-17330039-6-4), by Wenliang Du.
Amazon link: https://www.amazon.com/Wenliang-Du/e/B07R86172C

Evaluation:

Final Grade:
Homework/Lab: 40%, Attendance: 10%, Midterm: 20%, Final exam: 30%

Grading Scale (%):
A: 85 – 100, B: 75 – 84, C: 65 – 74, D: 55 – 64, F: 54 and below. **(**Plus/minus grading will be used).
The instructor reserves the right to lower the percentage threshold for letter grades as s/he sees fit (i.e., may make the grading scale better for you, but never worse).

Course Policies:

Late Policy: Without prior request, no late work will be accepted. All late submission maybe accepted at a penalty of 15% per day for no more than three days.

Testing Policy: All the midterm exams given are closed book/note/laptop/neighbor. But students are allowed to bring one cheat sheet (one piece of letter-size paper) for quick reference. Midterm exams are not cumulative. There will NOT be any makeup exams unless there is a documented emergency.

Homework Assignment and Project Report Policy: It is recommended that students use a word processing software (e.g., Word or LaTeX) to type their homework solutions or project report, then submit well-formatted PDF files.

Plagiarism/Cheating Policy: These are mandatory statements

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://libguides.memphis.edu/academicintegrity
http://www.memphis.edu/studentconduct/pdfs/csrr.pdf

Disability Notice:

Any student who anticipates physical or academic barriers based on the impact of a disability is encouraged to speak with me privately. Students with disabilities should also contact Disability Resources for Students (DRS) at 110 Wilder Tower (901-678-2880). DRS coordinates access and accommodations for students with disabilities (http://www.memphis.edu/drs/).

Class Schedule:

Lecture	Topic
1	Course Overview and Introduction
2	Security Introduction
3	Web Security Overview
4	Web Security – SQL Injection
5	Web Security – Cross-Site Scripting
6	Web Security – Cross-Site Request Forgery
7	Web Security – Session Management
8	Cryptography – Symmetric Cryptography I
9	Cryptography – Symmetric Cryptography II

10	Cryptography – Symmetric Cryptography III
11	Cryptography – Public Key Cryptography I
12	Cryptography – Public Key Cryptography II
13	Web Security – Https
14	Midterm Review
15	Midterm
16	Network Security – Network Overview
17	Network Security – Network Security Issues
18	Network Security – Firewall, VPN and IDS
19	Network Security – DNS Security
20	Network Security – DDoS
21	Network Security – Wireless Security
22	Mobile Security – iOS
23	Mobile Security – Android
24	Malware Overview
25	Final Review
26	Final

Labs:

Web Security:

1. Cross-Site Scripting Attack: https://seedsecuritylabs.org/Labs_20.04/Web/Web_XSS_Elgg/
2. Cross-Site Request Forgery Attack: https://seedsecuritylabs.org/Labs_20.04/Web/Web_CSRF_Elgg/
3. SQL Injection Attack: https://seedsecuritylabs.org/Labs_20.04/Web/Web_SQL_Injection/

Network Security:

4. IP Layer and Attacks https://seedsecuritylabs.org/Labs_20.04/Networking/ICMP_Redirect/
5. Packet Sniffing & Spoofing https://seedsecuritylabs.org/Labs_20.04/Networking/Sniffing_Spoofing/
6. TCP and Attacks 1: https://seedsecuritylabs.org/Labs_20.04/Networking/TCP_Attacks/
7. TCP and Attacks 2: https://seedsecuritylabs.org/Labs_20.04/Networking/Mitnick_Attack/
8. Firewall https://seedsecuritylabs.org/Labs_20.04/Networking/Firewall/
9. Virtual Private Network 1 https://seedsecuritylabs.org/Labs_20.04/Networking/VPN_Tunnel/
10. Tunneling and Firewall Evasion: https://seedsecuritylabs.org/Labs_20.04/Networking/Firewall_Evasion/
11. DNS and Attacks 1: https://seedsecuritylabs.org/Labs_20.04/Networking/DNS/DNS_Local/
12. DNS and Attacks 2: https://seedsecuritylabs.org/Labs_20.04/Networking/DNS/DNS_Remote/
13. DNSSEC: https://seedsecuritylabs.org/Labs_20.04/Networking/DNS/DNSSEC/

Mobile Security

14. Android Repacking Attack: https://seedsecuritylabs.org/Labs_20.04/Mobile/Android_Repackaging/
15. Android Device Rooting: https://seedsecuritylabs.org/Labs_20.04/Mobile/Android_Rooting/