Cleveland State University
Department of Electrical Engineering and Computer Science

CIS 475 Introduction to Computer Security

Catalog Data: CIS 475 Introduction to Computer Security
Pre-requisites:CIS345 Operating System Principles or equivalent
This class covers the computer security principles, basic cryptography, authentication, program security, trusted operating systems, computer system attacks and intrusion detection. Linux and other modern operating systems will be used as examples to illustrate the concepts covered in class. Students will develop the skills in basic security system programming through a number of class projects. Basic operating system concepts are required. C/C++ programming skills are required.

Textbook

- Charles R. Pleeger and Shari Lawrence Pfleeger: *Security in Computing, Fourth Edition*. Prentice Hall (2006) ISBN: 978-0132390779
- Professor Avinash Kak Lecture notes on Computer and Network Security, Purdue University. Will be available for download on course blackboard.

Reference

- William Stallings: Computer Security: Principles and Practices, Prentice Hall
- Ed Skoudis with Tom Liston: *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall
- Ross Anderson: *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

Instructor: Mike Lin
Office phone: (216) 687-4783
Email: lin@cis.csuohio.edu

Expected Outcomes:

At the end of this course, the students will be able to 1) describe basic cryptography and security schemes, 2) identify the typical computer system security threats, 3) choose the appropriate security detection and prevention schemes. Students also will develop the security system programming skills.

Course Outline:

The schedule of topics and their order of coverage is given below. Every effort will be made to follow the schedule, but topics covered may vary depending upon the progress made.

Week	Topic	reading
1/12	Introduction	P&P Ch 1
1/14, 1/21	Cryptography: Classical Ciphers	KAK #2; P&P Ch2.1-2.4
1/26	Cryptography: Stream Ciphers	Readings on Wikipedia :One-Time Pad
1/28	Cryptography: Block Ciphers &	KAK #3; P&P Ch2.5
2/2	AES: the Advanced Encryption Standard	KAK #8; P&P Ch2.6
2/4	Using Black and Stream Ciphers for Secure wired and WiFi Communication	KAK #8 P&P Ch2.8
2/9	Finite Fields (Part 1)	KAK #4
2/11	Finite Fields (Part 1)	KAK #5
2/18	Finite Fields (Part 1)	KAK #6
2/23	Finite Fields (Part 1)	KAK #7
2/25, 3/2, 3/4	Public Key Encryption	P&P Ch2.7-2.8
3/8-3/15	Spring Recess	
3/16	Midterm Exam	
3/18	Program Security I	P&P Ch3.21-3.2; KAK#21
3/23	Program Security II	P&P Ch3.2-3.3, KAK #22
3/25	Program Security III	P&P Ch3.5-3.8
3/30	OS Review, Shell commands,	
4/1	Unix/Linux Access Control	
4/6	OS Security Basics I	P&P 4.1-4.2
4/8	OS Security Basics I	P&P Ch4.3-4.8
4/13	Trusted OS I	P&P Ch5.1-5.2
4/15	Trusted OS II	P&P Ch5.3-5.4

4/20	Trusted OS III	P&P Ch5.5-5.8
4/22	TCP/IP Vulnerabilities: IP Spoofing and	KAK #16, P&P Ch7-2
4/27	DNS and the DNS Cache Poisoning Attack	KAK #17
4/27	Packet Filtering Firewalls (Linux), Proxy-Server Based	KAK #18, 19, P&P Ch7.4
4/29	Port and Vulnerability Scanning, Packet Sniffing, IntrusionDetection, and Penetration Testing	KAK#23, P&P Ch7.5
5/1	Review	
5/4	Final Exam	

Grading:

The course grade is based on a student's overall performance through the entire Semester. The final grade is distributed among the following components:

Quizzes & Attendance	10%
Homework Assignments	10%
Projects	25%
Midterm Exam	25%
Final Exam	30%

Letter Grades:
A: [90.0, 100.0] A-: [88.0, 90.0) B+: [84.0, 88.0)
B: [80.0, 84.0) B-: [78.0, 80.0) C+: [74.0, 78.0)
C: [68.0, 74.0)
D: [60.0, 68.0)
F: [0.0, 60.0)

Method of Instruction:

This course will combine (a) traditional lectures based on recitation of the material, and (b) hands-on programming exercises on Linux systems.

Class Attendance Policy:

Students are required to attend every class. Quizzes will be given at the start of most class periods. The doctor's note is required for any absence due to sickness. No makeup quiz will be given.

Project assignments (Programming):

Hands-on practice is the essential for this class. Totally 6 programming projects will be assigned during the semester. The assignments will require students to develop software that performs/verifies specific security related functions. All assignments will be graded on correctness, clarity in design and proper documentation. All projects are to be completed by each student individually. While high level discussion between students is allowed, any collaboration by exchanging the code or any written description is a violation of the class rules and will result in an 'F' grade.

Penalty for late project submission:
The standard penalty is the reduction of the mark allocated to the project assignment, by 20% of the maximum mark applicable for the assessment item, for each day or part day that the item is late. Weekends (Saturday and Sunday) count as two days in determining the penalty. The submission more than 4 days after the due date without an approved extension will be awarded zero point.

Collaboration rule:
You may consult your classmates on general issues about this assignment, but your code remains private. You should neither show another your program nor permit another to look at your program. Beyond that, you should adopt an "empty hands" attitude toward collaboration: talk about the project as you wish, but leave the conversation with nothing written. You can expect that submissions will be screened for code-sharing by an automated service. It is your responsibility to keep your source protected and not readable by others.

Exams:
Midterm and final exams will be close book/notes written exams. However, students are allowed to bring a US-letter sized cheat sheet. During the exams: (1) the use of cell phones, calculators, or any electronic devices is prohibited, and (2) students must not share any materials. No makeup exams will be given unless notified and agreed to in advance. Requests will be considered only in case of exceptional demonstrated need. An absence will not be excused without a confirmed doctor's note.
Grade Dispute:
If students have different opinions on the grading, they have 3 days time frame to dispute their grades after the results are announced through email or distributed in class. No grade dispute will be accepted after 3 days.

Academic Honesty:
Students are expected to do their own work. Academic misconduct, student misconduct, cheating and plagiarism will not be tolerated. Violations will be subject to disciplinary action as specified in the CSU Student Conduct Code. A copy can be obtained at: http://www.csuohio.edu/studentlife/StudentCodeOfConduct.pdf or by contacting Valerie Hinton Hannah, Judicial Affairs Officer in the Department of Student Life (MC 106 email v.hintonhannah@csuohio.edu). For more information consult the following web page CSU Judicial Affairs available at http://www.csuohio.edu/studentlife/jaffairs/faq.html.

ADA Adherence:
If you need course adaptations or accommodations because of a disability, if you have emergency medical information to share with me, or if you need special arrangements in case the building must be evacuated, please make an appointment with me as soon as possible. My office location and hours are listed on top of this syllabus. If you need further information, please contact the Office of Disability Services (Main Classroom 147), phone number 216.687.2015, on the web at http://www.csuohio.edu/offices/disability/.

KAK #1	Introductory material, course administration handout, etc.	
2.	Classical Encryption Techniques	
3.	Block Ciphers and the Data Encryption Standard	
4.	Finite Fields (PART 1): Groups, Rings, and Fields	
5.	Finite Fields (PART 2): Modular Arithmetic	
6.	Finite Fields (PART 3): Polynomial Arithmetic	
7.	Finite Fields (PART 4): Finite Fields of the Form $GF(2^n)$	
8.	AES: The Advanced Encryption Standard	
9.	Using Block and Stream Ciphers for Secure Wired and WiFi Communications	
10.	Key Distribution for Symmetric Key Cryptography and Generating Random Numbers	
11.	Prime Numbers and Discrete Logarithms	
12.	Public-Key Cryptography and the RSA Algorithm	
13.	Certificates, Certificate Authorities, and Digital Signatures	
14.	Elliptic Curve Cryptography and Digital Rights Management	
15.	Hashing for Message Authentication	
16.	TCP/IP Vulnerabilities: IP Spoofing and Denial-of-Service Attacks	
17.	DNS and the DNS Cache Poisoning Attack	
18.	Packet Filtering Firewalls (Linux)	
19.	Proxy-Server Based Firewalls	
20.	PGP, IPSec, SSL/TLS, and Tor Protocols	
21.	The Buffer Overflow Attack	
22.	Malware: Viruses and Worms	
23.	Port and Vulnerability Scanning, Packet Sniffing, Intrusion Detection, and Penetration Testing	
24.	Dictionary Attacks and Rainbow-Table Attacks on Password Protected Systems	
25.	Security Issues in Structured Peer-to-Peer Networks	
26.	Small-World Peer-to-Peer Networks and Their Security Issues	
27.	Web Security: PHP Exploits and the SQL Injection Attack	
28.	Web Security: Cross-Site Scripting and Other Browser-Side Exploits	
29.	Bots and Botnets	
30.	Mounting Targeted Attacks with Trojans and Social Engineering --- Cyber Espionage	
31.	Filtering Out Spam	