SYLLABUS
CPSC 4360/5360: Computer Security (Spring 2013)
Department of Computer Science
University of Arkansas at Little Rock

Instructor and Contact Information:
- Instructor: Mengjun Xie, Ph.D.
- Office: EIT 573, Phone: 501-569-8134, E-mail: mxxie@ualr.edu.

Time and Place: TR 1:40 pm – 2:55 pm, ETAS 355.

Office Hours: TR 9:30 am – 11:00 am (EIT 573) or by appointment.

TA and TA Office Hours: Liang Hao (lxhao@ualr.edu), 2:00 pm – 4:00 pm Wednesday.

Important Dates:
- 1/18 Late registration ends.
- 3/12 Last day to drop an individual class.
- 3/18 – 3/24 Spring break, no class.
- 5/6 Last day of classes/Last day to withdraw from classes.
- 5/9 Final exam (1:30 pm – 3:30 pm)

Required Text:

Additional Reading:

Prerequisite:
- CPSC 3371 (Net-centric Computing: Language Concepts) and 3482 (Computer Organization I), or
- Consent of instructor.

Course Description:
The increased use of networked computer systems in our infrastructures and daily lives requires serious considerations of computer security and research for further improvements. As these systems become part of the infrastructure necessary to carry out our daily lives, their importance increases. This course covers the concepts and principles of computer security. Definition of a “secure computer” and its relationship to requirements, distinction between security and cryptology, etc are within the focus of this class. This course offers students practical and theoretical knowledge and understanding of issues related to computer security.

Topical Outline:
The main topics in this class include
- Introductory Concepts
  - Fundamental Security Concepts (C.I.A., A.A.A, threats and attacks, ten security principles)
  - Access Control Models (ACM, capabilities, RBAC)
  - Cryptographic Concepts
  - Passwords, Usability Issues, Social Engineering
- Operating Systems Security
  - OS Concepts (kernel, input/output, processes, Linux/Windows, virtual machines, etc)
  - Process Security (monitoring and logging)
  - Memory Management and Memory Security
  - File System, Access Control, and FS Security
• Application Security (buffer overflow attacks, format string attacks)
  • Malware
    o Insider Attacks, Backdoors, Trojan Horses.
    o Computer Viruses, Worms, Rootkits, Botnets, Zero-Day Attacks
    o Privacy-invasive Malware
    o Countermeasures (antivirus, intrusion detection systems, best practices, economics of malware)
  • Cryptography
    o Symmetric Cryptography
    o Asymmetric Cryptography
    o Cryptographic Hash Functions
    o Key Management (Needham-Schroeder, Diffie-Hellman key exchange)
    o Digital Signatures, Digital Certificates
  • Network Security
    o Network Basics (network layers, protocols, network devices, new network technologies)
    o Link Layer Security (ARP spoofing)
    o Network Layer Security (IP and IP spoofing, packet sniffing)
    o Transport Layer Security (TCP/UDP, NAT, TCP session hijacking)
    o Network Denial-of-Service Attacks and Countermeasures
    o Application Layer Security (email spam, DNS attacks, DNSSEC)
    o Firewall
    o Tunneling (IPSec and VPN, SSL/TLS, SSH)
    o Intrusion Detection (Rule-based, anomaly detection, port scanning, honeypot)
    o Wireless Network Security (WEP, WPA)
  • Web Security
    o Web (HTTP, HTML, sessions, cookies, HTTPS)
    o Client-side Attacks (session hijacking, phishing, XSS, CSRF, defenses)
    o Server-side Attacks (server-side scripting, SQL injection, DoS attacks, etc)
  • Security Models and Practice
    o Security Models, Trust Management
    o Access Control Models (Bell LaPadula Model, RBAC)
    o Software Vulnerability Assessment (static/dynamic analysis, vulnerability scanning, CERT)
    o System Administration (OS and software patch/update, auditing)

**Learning Outcomes:**
Upon successful completion of this course, a student will be able to
• Explain basic concepts in information security, including security policies, security models, and security mechanisms.
• Explain basic concepts related to applied cryptography, including plain-text, cipher-text, techniques for crypto-analysis, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, cryptographic hash functions, and modes of encryption operations.
• Explain the concepts of malicious code (e.g., virus, Trojan horse, rootkit, bot, and worm) and use common tools for detecting malware.
• Explain common vulnerabilities in computer programs, including buffer overflow vulnerabilities, time-of-check to time-of-use flaws, incomplete mediation.
• Explain the concepts of security models and outline their applications.
• Explain the requirements and techniques for securing operating systems and networks and use appropriate tools to secure OS, applications, and networks.

**Teaching Methodology:** Lectures, discussions, and assignments. Materials will be assigned for reading, discussion, and examination. Preparation prior to the class is expected. Class lectures will be technical and will mostly follow the material presented in the book along with relevant papers from the literature.

**Technology Use:**
• **Blackboard:** Blackboard (BB) is used for course management. Class schedule, announcements, homework and lab assignments, as well as information related to the course will be posted there. Please make sure to check the course
page on BB regularly (at least once a day).

- **E-mail:** If you e-mail me at my UALR address and not through BB, please make sure you include “CPSC 4360/5360:” in the subject line. For example, you want to notify me that you are having a surgery and you will be missing the exam; your subject line could be “CPSC 4360/5360: surgery.”

**Journals on Information Assurance and Cyber Security:**
Many high-quality magazines and journals on Information Assurance and Cyber Security can be accessed for free through UALR library databases. The following journals are highly recommended if you are interested in in-depth study and research in the area of computer security and information assurance.

- **IEEE Xplore Digital Library**
  - IEEE Security & Privacy (Magazine)
  - IEEE Transactions on Information Forensics and Security (Journal)
  - IEEE Transactions on Dependable and Secure Computing (Journal)
  - IEEE Symposium on Security and Privacy (Conference Proceedings)

- **ACM Digital Library**
  - ACM Transactions on Information and System Security (Journal)
  - ACM Symposium on Information, Computer and Communications Security (Conference Proceedings)
  - ACM SIGSAC Conference on Computer and Communications Security (Conference Proceedings)
  - ACM Conference on Security and Privacy in Wireless and Mobile Networks (Conference Proceedings)
  - ACM Conference on Data and Application Security and Privacy (Conference Proceedings)

- **ScienceDirect**
  - Elsevier Computers and Security (Journal)
  - Elsevier Journal of Information Security and Applications (Journal)
  - Elsevier Network Security (Journal)

- **SpringerLink**
  - International Journal of Information Security (Journal)
  - Security Informatics (Journal)

- **Wiley Online Library**
  - Security and Communication Networks (Journal)

**Academic Misconduct:** Any form of academic misconduct will NOT be tolerated. Please be advised that turning in someone else’s assignment/code is a form of academic misconduct. Cheating could, at the minimum, result in an “F” as the final grade for the course. You are required to read “Code of Student Rights, Responsibilities, and Behavior” in the Student Handbook. You must comply with the UALR Academic Integrity Policy as described at [http://ualr.edu/policy/index.php/50113/](http://ualr.edu/policy/index.php/50113/).

**Grading:**

<table>
<thead>
<tr>
<th>Assignments (Labs + HW):</th>
<th>40%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Midterm exam</td>
<td>20%</td>
</tr>
<tr>
<td>Final exam</td>
<td>35%</td>
</tr>
<tr>
<td>Attendance and Participation</td>
<td>5%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>[90, 100]</td>
</tr>
<tr>
<td>B</td>
<td>[80, 90)</td>
</tr>
<tr>
<td>C</td>
<td>(70, 80)</td>
</tr>
<tr>
<td>D</td>
<td>[60, 70)</td>
</tr>
<tr>
<td>F</td>
<td>[0, 60)</td>
</tr>
</tbody>
</table>

**Regulations for Assignments**

- Assignments consist of both labs (two) and homework assignments (around four).
- Each of the assignments is due at the start of class (i.e., 1:40 pm sharp) on the dates specified in the assignments. Anything that comes in after 1:40 pm will be considered late. The assignments must be submitted as described (paper copy, electronic copy, or both).
- Assignments that come in late (up to a maximum of five calendar days) will be given a late penalty (10% penalty per day). Assignments received later than five calendar days following the due date will not be graded.
- Your homework assignments must be typeset. No handwritten assignments will be accepted.
- I will not answer any question regarding a homework assignment on the due day.
• You may consult with each other, with me, with texts, papers, or any published material, but the final written solution you turn in for the assignment must be composed by you without the help of others. This means that you may neither look at the written solution of another student, nor show another student your written solution. Exchanging final solutions electronically also will be a violation.
• An “empty hands” policy must be observed when you meet with your classmates to discuss the problems on a homework assignment. You are free to discuss homework assignments, but you must leave the meeting without any record of these discussions.
• If you discuss a homework assignment with other students in the course, you are required to list their names when you turn in the assignment.
• If you have any questions about whether a particular source is considered to be published material, you are obligated to clear the source with me before consulting it. In general, searching for a solution on the web--and then submitting it as your answer for a homework assignment--will be considered a violation.
• If you have any questions about whether a consultation with a source might constitute a violation, you are required to ask me for permission before you are allowed to engage in such a consultation.

Extra Credit: You can earn extra credit (up to 10 points in final grade) during the semester by completing certain tasks/projects that are mentioned but not assigned as compulsory class work. One example would be doing an independent research project related to the course contents.

Exams
• The midterm exam will be on 2/28 (tentative) and the final exam will be on 5/9. They are in-class, open-book, and closed-notes exams.
• There will be no alternate time for the final exam. Make sure that you can attend the final exam at the specified time before enrolling in the class.
• You are required to take the midterm exam during the scheduled time period. Barring extreme situations such as a serious illness or a death in the family with legitimate supporting documents, I will neither allow anyone to take the midterm exam early nor schedule any make-up midterm exam.
• NO collaboration is allowed in the exams.
• NO electronic devices except calculator are allowed.

Students with Disabilities: Your success in this class is important to me, and it is the policy and practice of the University of Arkansas at Little Rock to create inclusive learning environments consistent with federal and state law. If you have a documented disability (or need to have a disability documented), and need an accommodation, please contact me privately as soon as possible, so that we can discuss with the Disability Resource Center (DRC) how to meet your specific needs and the requirements of the course. The DRC offers resources and coordinates reasonable accommodations for students with disabilities. Reasonable accommodations are established through an interactive process among you, your instructor(s) and the DRC. Thus, if you have a disability, please contact me and/or the DRC, at 501-569-3143 (V/TTY) or 501-683-7629 (VP). For more information, please visit the DRC website at www.ualr.edu/disability.

Modifications to Syllabus: This syllabus may be modified at the discretion of the instructor or in the event of extenuating circumstances. Students will be notified in class of any changes to the syllabus.