COMPSCI 469  Computer Security

University of Wisconsin-Milwaukee
Fall 2019

Class meetings:
Lectures: Monday, Wednesday: 3:30pm - 4:45pm, EMS E180.

Instructor: Dr. Guangwu Xu;
Office: EMS 1239;
Phone: (414) 229-5731;
Email: gxu4uw@uwm.edu;
Office hours: 1:30pm-3:00pm, Monday, Wednesday (or by appointment).

Textbook:
Introduction to Computer Security
by M. T. Goodrich and R. Tamassia
Addison-Wesley (ISBN-10 0-321-51294-9)

Attendance Policy: Students are expected to attend every lecture.

Assignments: There will be a total of six assignments (five homework assignments and one programming assignment) in the course.

- Homework assignments will involve problem solving and algorithm analysis. These assignments cover material presented in lecture and the readings. They are to be completed individually.

- Programming assignment will involve implementation of some cryptographic routines in C/C++, or Java. Programs should be well designed, and use good coding practice.

- Late assignments are not accepted.

Exams: There will be a midterm test and a final exam. They are all closebook. The format of questions will be multiple choice and some longer problems. Exam questions will be based on material covered in the book and/or in lecture.
Midterm Test Date: Monday, October 21.
Final Exam Date Time: Monday, December 16, 3:00–5:00pm.
Grading:
For Undergraduate Students:
Assignments (40%), midterm test (28%), final exam (30%), attendance and participation (2%)

For Graduate Students:
Assignments (30%), project (10%), midterm test (28%), final exam (30%) (midterm and final will be different from that for undergraduate students), attendance and participation (2%)

Desired Outcomes:
Students will be

1. able to understand basic components of computer security
2. able to understand how security threats are classified and dealt with.
3. able to understand fundamentals of symmetric key, public key cryptography and hash functions; and able to implement simple primitives using C/C++ or Java.
4. able to understand protocols of security services.
5. familiar with network security design using available security solutions.
6. able to understand design issues and working principles of various system authentication methods.
7. able to understand principles for the design and implementation of security mechanisms.
8. able to explain and compare security mechanisms for conventional operating systems
9. able to understand how to classify and defend against computer viruses.
10. able to explain common vulnerabilities in computer programs.

Course Outline: This is a one-semester course covers basics of computer security. Specific topics are
<table>
<thead>
<tr>
<th>Area</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Fundamental concepts and security principles; access control models; crypto concepts; implementation and usability issues.</td>
</tr>
<tr>
<td>Operating System Security</td>
<td>OS concepts; processes, memory, and file system security; software security.</td>
</tr>
<tr>
<td>Cryptography</td>
<td>Symmetric key encryptions; public key encryptions, key exchange, and digital signatures; hash functions and message authentication codes.</td>
</tr>
<tr>
<td>Network Security</td>
<td>Network concepts; security issues for link layer, IP layer, and transport layer; firewall and intrusion detection; IPsec; wireless security; TLS protocols; web attacks.</td>
</tr>
<tr>
<td>Malware</td>
<td>Insider attacks; virus, worms Trojan horses; counter measures.</td>
</tr>
<tr>
<td>Other applications</td>
<td>Digital currencies; blockchain technology.</td>
</tr>
</tbody>
</table>

**UWM Policies:** Policies for students with disabilities, religious observances, incomplete, academic misconduct, grade appeal procedures, final examination policy, students called to military service, discriminatory conduct, and complaint procedures can be found at http://www4.uwm.edu/secu/news_events/upload/Syllabus-Links.pdf