Network Security  
CS490-002 (CRN: 36350)/590-001 (CRN: 36795) - Fall 2019

Welcome to Network Security, Fall 2019!

Instructor: Dr. Hiroshi Fujinoki  
Office: EB 2034  
Office Phone: 650-3727  
E-mail: hfujino@siue.edu (specify "CS490" or "CS590" in the subject of your e-mail)  
Instructor's HP: www.siue.edu/~hfujino  
Office Hours: (1) Mondays: 1:30 - 3:30 P.M.  
              (2) Tuesdays: 10:00 - 11:00 A.M.  
              (3) Tuesdays: 2:00 - 3:30 P.M.  
              (3) Wednesdays: 1:30 - 3:30 P.M.  
              (4) Thursdays: on appointment  
              (4) Fridays: on appointment  

Class Meeting Room: EB-0140 (in the basement of the Engineering Building)  
Class Meeting Days: M, W, and F  
Class Meeting Time: 12:00-12:50 P.M.  

Note: item with "★" symbol means an important item.

★ Course Objectives:

This course addresses the fundamentals in computer network security especially to develop skills for prevention of security hazards and for protection of network systems from potential malicious software and users. The primary purposes in this course are to learn (1) what security threats are possible, (2) how the security threats are possible (how the attackers perform such attacks), (3) what solutions exist to prevent the security attacks, and (4) how the solutions work. This course will consist of the lectures to cover concepts of network security, discussions for past case studies of security incidents and possible solutions for protection, and literature reviews for on-going research activities in the today's frontline in network security. This course proposes to focus on practical aspects of network security as well as concepts and theories. The security threats and the solutions to be covered by this course are as shown in the following list:
Security Threats
- Reconnaissance (ping, port scan, network mapping)
- Password cracking (dictionary attacks)
- Viruses, worms, and spiders
- Trojan horses, backdoors and spyware (key loggers)
- Denial of service attacks (flooding and logic bomb)
- Phishing and URL-redirections
- Distributed Denial of Service Attacks and Bots
- Infrastructure attacks (black-hole routers and DNS contaminations)
- System vulnerabilities and Exploits (buffer overflow attacks, root kits, SQL injections and others)
- Intelligent middlemen (for instant messengers)
- Web securities (SQL-injections, cross-site scripting attacks, and HTTP session hijacking)

Solutions:
- Asymmetric cryptography
- Secure protocols (PGP, IPSec, SSL, etc.)
- Hash Digests (MD5 digest, etc.)
- Certificate
- Firewall
- Intrusion detections
- Honeypots and honeynets
- Multi-level security
- Access controls and user managements
- Secure systems (trusted OS, etc.)
- Security standards (ITUT-X800 standard)
- Cloud security
- Case-studies (IP-spoofing attacks, "DNS-reflector" DDoS attacks)
- SET (Secure Electronic Transaction) protocol

Grading (CS490-002):
- Quizzes (12 quizzes): 20% 100 - 90: A
- Survey Homework (six HW): 25% 89-80: B
- Midterm Exam: 25% 79-70: C
- Final Exam (Comprehensive): 30% 69-60: D
  Below 60: F

Grading (CS590-001):
- Quizzes (12 quizzes): 15% 100 - 90: A
- Survey Homework (six HW): 20% 89-80: B
- Research Project: 15% 79-70: C
- Midterm Exam: 20% 69-60: D
- Final Exam (Comprehensive): 30% Below 60: F
Exams:
- Exams will be closed textbook and closed notes (each exam consists of quiz (CAT. I) questions and the exercise (CAT. II) questions covered in the lectures).
- Makeup exam will be given only for medical emergency (with a written proof).
- If you need any special assistance you must contact Dr. Fujinoki at least one week before.

Quizzes:
- Quizzes cover reading assignment and other literature review in the course. The instructor will announce the coverage for each quiz a week before.
- Questions to appear in each quiz will be posted before each quiz.
- There will be 12 quizzes throughout the semester. If we cannot make all of the 12 quizzes in a semester, the average of each quiz (in percent) will be calculated.
- If you cannot take a quiz by some serious reason, you need to talk to the instructor at least one week before the quiz for a make up. However, the acceptable reasons are limited to serious reasons only. In case of medical emergency, you do not need prior notice to the instructor.

Survey Homework:
In this homework, each person in this course covers the security topics for enhancing your knowledge regarding the known existing security threats and solutions. You do not have to submit any report, but your learning will be measured by multiple-option questions after the due for the homework (the due date will be announced on the course home web site). Some sample questions for the homework will be posted to the course home. Out of the six homework, the lowest homework grade will be dropped from your homework grade. The survey homework covers the following five categories:
- Homework #1: Security Threats (Part I)
- Homework #2: Security Threats (Part II)
- Homework #3: Malwares
- Homework #4: Cryptography
- Homework #5: Security Protocols
- Homework #6: Firewalls

Note: for your survey homework, it is strongly suggested to keep the source of the information you used for preparing your solutions. Credit may be given
to some solutions that are not expected by the course instructor, if you can present the source of the information.

♦ Research Project (for CS590-001 students only):
  - Conduct a research on a specific topic(s) in network security to provide an opportunity to review the current state of network security in details. **This project will be an individual project.** Each individual (1) performs preliminary research to find a topic, (2) perform in-detail literature reviews, (3) organize major findings, as well as your analyses on the effectiveness of the existing solutions, and integrate them in a presentation and (4) present and peer-review other's work. The grade will be given in competition basis.

Attendance Policy:
  - Attendance will be taken at the beginning of each lecture (being late more than 5 minutes can be considered absence).
  - For the first three absences, no penalty will be applied. After the third absence, -2 points (100-point basis) will be applied to your next exam.
  - The above penalty will not apply to medical emergency (however, you need to provide written proof of medical service to waive the penalty).
  - There are special attendance policies for “Research Project”, which are applicable to both CS490-002 and CS590-001 students.

♦ Academic Dishonesty: Following activities will be considered academic dishonesty and final letter grade of F will be given:
  - Submitting (or presenting) work (such as homework assignments and projects) done by somebody else (this includes any human/electronic sources (such as web sites)) under your name.
  - Watching and copying your neighbors' solutions during exams.
  - Using materials not allowed in the course (this includes, exams, quizzes, homework and projects).

♦ Required Textbook:

Course Prerequisites:
  - CS447 (Data Communications and Networks) or equivalent
  - CS314 (Operating Systems) is preferred
• Basic knowledge in socket programming
• Basic knowledge of UNIX/LINUX operating systems
• Moderate fluency in C/C++ plus system programming (systems call, pointers and data structures)

✦ Other Notices:
• Every student is expected to check: www.cs.siue.edu/~hfujino/CS590_001_F19/CS590.html at least twice in a week.
• Important notices for that week will be posted every week. I assume each of you check the homepage at least twice, one of which should be Sunday night.
• The instructor is NOT responsible for the consequences if you do not regularly check the CS490-002/590-001 course home. Important information regarding important activities, such as exams and projects, will be posted at least 24 hours prior to the deadline unless otherwise announced (this means if posting any serious information is announced in the classroom, it can appear in the CS490-002/590-001 home even within 24 hours from the deadlines).
• Smart phones and any other hand-held devices are not allowed during the lectures, quizzes, and exams.
• Any grading problem should be reported within two weeks (14 days) after their grades are posted or the graded materials are returned in the classroom.
• E-mails sent to the course instructor during weekends and the break (spring break) may not be responded.

✦ Tentative Class Schedule:

This schedule is tentative and subject to change. However, any change will be announced in the class or noticed in the notice page of the instructor.

<table>
<thead>
<tr>
<th>Week #: Day</th>
<th>Topics</th>
<th>Materials Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1: August 19 (M):</td>
<td>Course description</td>
<td>Course Syllabus</td>
</tr>
<tr>
<td></td>
<td>Project description</td>
<td>Chapter 1</td>
</tr>
<tr>
<td></td>
<td>Introduction to network security</td>
<td></td>
</tr>
<tr>
<td>August 21 (W):</td>
<td>Framework of network security</td>
<td>Chapter 1</td>
</tr>
<tr>
<td></td>
<td>Introduction to network security (continued)</td>
<td></td>
</tr>
<tr>
<td>August 23 (F):</td>
<td>Types of possible network security hazards</td>
<td></td>
</tr>
</tbody>
</table>
Network security report from CERT

Week 2: August 26 (M): Quiz #1, Lecture note
Introduction of the major security threats ("what are they?")
August 28 (W): Symmetric cryptography and hash digest (Part I) Lecture note
August 30 (F): Symmetric cryptography and hash digest (Part II) Lecture note

Week 3: September 2 (M): Labor Day Holiday. University closed
September 4 (W): Quiz #2, Signature and security certificate (Part I) PPT Presentation
September 6 (F): Signature and security certificate (Part II) PPT Presentation

Week 4: September 9 (M): Quiz #3, Viruses, worms and spiders (Part I) Lecture note
September 11 (W): Viruses, worms and spiders (Part 2) Lecture note
September 13 (F): Security Firewall (Part I) PPT Presentation

Week 5: September 16 (M): Quiz #4, Security Firewall (Part 2) PPT Presentation
September 18 (W): Intrusion detections and intrusion sensors (Part I) PPT Presentation
September 20 (F): Intrusion detections and intrusion sensors (Part II) PPT Presentation

Week 6: September 23 (M): Quiz #5, Honeypots and Honeynets (Part I) Lecture note
September 25 (W): Honeypots and Honeynets (Part II) Lecture note
September 27 (F): Protocol-level security (Part I) PPT Presentation

Week 7: September 30 (M): Quiz #6, Protocol-level security (Part II) PPT Presentation
October 2 (W): Protocol-level security (Part III) PPT Presentation
October 4 (F): Denial-of-Service (DoS) attacks (Part I) Lecture note
• Logic attacks and flooding attacks

Week 8: October 7 (M): Midterm Exam (cover the materials from 1st to the 7th week)
October 9 (W): Denial-of-Service (DoS) attacks (Part II) Lecture note
• TCP SYN-flooding attacks and solutions
October 11 (F): DDoS (Distributed DoS) attacks Lecture note
• Bots
• DNS-reflection attacks

Week 9: October 14 (M): Infrastructure-oriented security hazards (Part I) Lecture note
• Security-hazards to the core routers and their impacts
• Black-hole routers and DNS contamination
October 16 (W): Web Security and secure online transactions (Part I) Chapter 7
October 18 (F): Web Security and secure online transactions (Part II) Chapter 7

Week 10: October 21 (M): Quiz #7, Web Security and secure online transactions (Part III) PPT presentation
October 23 (W): Web Security and secure online transactions (Part IV) PPT presentation
• SSL (Secure Socket Layer)
October 25 (F): IPsec (Part I) PPT presentation
Week 11: October 28 (M): Quiz #8, IPsec (Part II)  
October 30 (W): IPsec (Part III)  
November 1 (F): Other security threats (Part I)  
- Phishing and URL redirections

Week 12: November 4 (M): Quiz #9, Other security threats (Part II)  
- Vulnerabilities and exploits (buffer overflow attacks, root kits, SQL injections, backdoors, and others)
November 6 (W): Other security threats (Part III)  
- Intelligent middlemen for instant messengers
November 8 (F): Other security threats (Part III)  
- TBA

Week 13: November 11 (M): Quiz #11, TBA  
November 13 (W): Course project presentation and evaluation (Day 1)  
November 15 (F): Course project presentation and evaluation (Day 2)

Week 14: November 18 (M): Quiz #12, Course project presentation and evaluation (Day 3)  
November 20 (W): Course project presentation and evaluation (Day 4)  
November 22 (F): User management and access control (Part I)  
- Principles: user authentication and authorization  
- Role-based access control  
- multi-level security

Week 15: November 25 - December 1: Thanksgiving Break. Classes not in session.

Week 16: December 2 (M): User management and access control (Part II)  
December 4 (W): PGP (Pretty Good Privacy) and SSL  
December 6 (F): TBA

Final Exam Week: December 9 (Monday): 10:00-11:40 A.M. at EB-0140: Final Exam (comprehensive)