Instructor: Dr. Arslan Munir, Scrugham Engineering and Mines 206, Email: arslan@unr.edu

Lecture Hours: Monday & Wednesday 1:00 PM - 2:15 PM

Office Hours: Monday & Wednesday 12:15 PM - 12:45 PM, 2:15 PM - 2:45 PM, and by appointment, Room: SEM 206


Supplementary Material:


Prerequisites:

- CS 219 Computer Organization

Course Objectives: Security in computing systems has gained paramount significance as an increasing amount of sensitive and private data is being stored in computers (embedded or desktop or server). Furthermore, many computing systems need to operate reliably and dependably to meet application requirements. The course elaborates essential reliability and security primitives in computing systems and motivate students for considering security and reliability in the design of computing systems.

Course Description: The course emphasizes on cryptography (encryption, hash functions and message authentication), hardware-based security and trust, and hardware/software fault tolerance.
Course Outline and Topics:

Introduction to cryptography & data security ........................................ Week 1
Data encryption standards (DES, AES) & block ciphers ........................... Week 2
Introduction to public-key cryptography & RSA cryptosystem ................. Week 3
Elliptic curve cryptosystems & digital signatures ................................. Week 4
Hash functions, message authentication codes & key establishment .......... Week 5
Hardware metering & digital watermarking ............................................ Week 6
Security based on physically unclonable functions (PUFs) ...................... Week 7
Physical attacks, side-channel attacks and countermeasures .................. Week 8
Hardware Trojan ..................................................................................... Week 9
True random number generators & hardware security in contactless tokens Week 10
Hardware-based security architectures & trusted platform module .......... Week 11
Introduction to reliability & fault tolerance ........................................... Week 12
Hardware fault tolerance ........................................................................ Week 13
Software fault tolerance ........................................................................ Week 14

Grading Policy—CS 454:

• Exam 1: 30%
• Exam 2: 30%
• Exam 3: 30%
• Homework assignments and class participation: 5%
• Selected topic class presentation: 5%

Grading Policy—CS 654:

• Exam 1: 25%
• Exam 2: 25%
• Exam 3: 25%
• Homework assignments and class participation: 5%
• Course technical report: 15%
• Course technical report and/or research topic class presentation: 5%

Grading Scale:

• A-: 87.00 - 89.99; A: 90.00 - 100
• B-: 75.00 - 79.99; B: 80.00 - 83.99; B+: 84.00 - 86.99;

*Course calendar is subjected to change depending on the progress of the class.
Supplemental Instructions for Graduate Students (CS 654) The work load and evaluations for CS 654 students are more demanding than CS 454 students as summarized above in the grading policy of CS 654. Below are supplemental instructions for CS 654 students.

- Graduate students will achieve deeper understanding of the material presented to the combined group by being given:
  - Additional readings
  - Additional assignments
- Some of the assignments will have additional questions for graduate students. The additional work will be clearly identified in the assignments. The graduate students will also have a technical report due at the end of the course and will comprise 15% of total grade.
- The additional reading assignments and course technical report will potentially inspire graduate students for research. The students will be provided an opportunity to discuss with the instructor interesting research problems relevant to their technical reports. Furthermore, students demonstrating research potential in their technical report will be provided an opportunity to pursue an independent study with the instructor.
- The graduate component of some assignments and course technical report will promote additional synthesis experience for graduate students.
- As indicated in the course syllabus, the graduate student taking the course will be required to do additional work that will be indicated clearly on assignments. Graduate students who will demonstrate research potential and will be interested in pursuing research in the area will be provided independent study opportunities.
- Graduate students will be required to do additional work for some assignments, which will be clearly indicated on the assignment. Graduate students who will not complete the additional graduate component (when specified) of the assignment will get a lower grade for the assignment. Furthermore, graduate students will be required to submit a technical report at the end of the course comprising 15% of the total grade.
- The additional reading, assignment work, course technical report and greater opportunities for interaction with instructors for possibilities of an independent study will provide greater academic value for graduate students.

Course Technical Report: For the course technical report/paper, please select a topic related to security or reliability of computing systems. Students are encouraged to do some research/small project (not mandatory though) for the technical paper. Students can form a team of two or three if undertaking a research project for the technical report. If not doing a research project for the technical paper, students are expected to do a comprehensive survey of the topic, provide some analysis, key insights, and future research directions in the selected topic's area. The technical paper should be formatted like an IEEE/ACM conference/journal publication. All written materials

---

1 No rounding up will be done for the final grades, no exceptions (i.e., 90.99 is still an A-, 86.99 is still B+ and so on). Students will have one week to appeal for their grades after the graded assignments/exams are returned if they think there is a problem/issue with the grading.
should be prepared and presented in a structured, polished, and professional manner. The project grade will be determined based on the ratio of the challenge and quality of the work versus the size of the team (in case of undertaking research project).

**Course Policies:**

- All course materials will be posted on the WebCampus.
- Unless instructed otherwise, use of electronic devices including laptops and cell phones is not allowed during lectures.
- Students are expected to demonstrate professionalism and courtesy by either silencing or turning off all cell phones and/or other alarm or audible indicator devices.
- No pets are allowed in the classroom.
- There will be three exams for this course. Students should plan on taking the exams on the scheduled times. Permission to take exams on other dates than scheduled will not be given, except for extreme medical emergencies. In case of any emergency situation, a student needs to provide a convincing documentation for it. The exams will be closed books and closed notes. The use of electronic devices such as laptops and cell phones, etc., are prohibited during exams.
- Students are expected to attend, and be on time, for every class. This demonstrates professionalism and consideration for your fellow students and your Instructor. While the course does not have an attendance policy, students who miss class and/or are late for class may experience an impact on their grade by missing classroom activities and/or quizzes.
- Students are expected to turn in all assigned materials in a timely manner.
- The Instructors reserve the right to add to, and/or modify any of the above policies as needed to maintain an appropriate and effective educational atmosphere in the classroom. In case of any change in the course policy, all students will be notified in advance of the new and/or modified policy.

**Important Dates:**

- First Day of Classes .......................................................... January 19
- Add Deadline (without permission from instructor) ........January 25
- Add Deadline (with permission from instructor) .............January 28
- Drop Deadline (with “W” received) ................................. March 29
- Final class meeting week begins ................................. May 5
- Final grades available to students in MyNevada ............. May 18

**Academic Integrity:** Students are encouraged to study together, however each student must individually prepare his/her solutions. Cheating or plagiarism is not permitted and will be sanctioned according to the UNR policy on Academic Standards. Students should carefully read the section on Academic Dishonesty found in the UNR Student Handbook.

**Homework Policy:** Late homework will be accepted for at most 70% credit. Students are encouraged to study together, but each person must prepare his or her solutions and have a firm understanding of any work turned in. When you put your name on your homework, you are stating that it is your own work and not the work of another person. As a reminder of UNR academic

---

Please check UNR academic calender to verify these dates.
standards, please read UNR policies and guidelines. Specifically, the following: “Plagiarism is defined as submitting the language, ideas, thoughts or work of another as one’s own; or assisting in the act of plagiarism by allowing one’s work to be used in this fashion.” This means that if another student asks to borrow your work to copy - JUST SAY NO - or you are participating in plagiarism.

Learning Outcomes:

Learning Outcome A: Students will be able to describe the security primitives in computing systems.

Learning Outcome B: Students will be able to apply cryptographic algorithms to secure and authenticate data.

Learning Outcome C: Students will be able to describe different approaches for hardware-based security and trust.

Learning Outcome D: Students will be able to describe reliability measures and approaches to incorporate reliability and fault tolerance in computing systems.

Learning Outcome E: Students will enhance their ability to communicate effectively with a range of audiences.

Student Outcomes and Course Outcomes: The course outcomes are skills and abilities students should have acquired by the end of the course. These outcomes determine how the general CSE Student Outcomes apply specifically to this course. These outcomes are defined in terms of the ABET Accreditation Criterion 3: Student Outcomes. All CSE Student Outcomes are listed in the next subsection and those relevant to this course are identified in Table 1.

CSE Student Outcomes:

1. an ability to apply knowledge of computing, mathematics, science, and engineering.
2. an ability to design and conduct experiments, as well as to analyze and interpret data.
3. an ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs, within realistic constraints specific to the field.
4. an ability to function effectively on multi-disciplinary teams.
5. an ability to analyze a problem, and identify, formulate and use the appropriate computing and engineering requirements for obtaining its solution.
6. an understanding of professional, ethical, legal, security and social issues and responsibilities.
7. an ability to communicate effectively with a range of audiences.
8. the broad education necessary to analyze the local and global impact of computing and engineering solutions on individuals, organizations, and society.
9. a recognition of the need for, and an ability to engage in continuing professional development and life-long learning.
10. a knowledge of contemporary issues.
11. an ability to use current techniques, skills, and tools necessary for computing and engineering practice.
12. an ability to apply mathematical foundations, algorithmic principles, and computer science and engineering theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices.
13. an ability to apply design and development principles in the construction of software systems or computer systems of varying complexity.
<table>
<thead>
<tr>
<th>CSE Student Outcomes</th>
<th>Description of CSE Course Outcomes</th>
<th>Course Strategies &amp; Assessment Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Students will be able to demonstrate an ability to apply knowledge of computing, mathematics, science, and engineering</td>
<td>Assignments and exam questions</td>
</tr>
<tr>
<td>2</td>
<td>Students will be able to manifest an ability to design and conduct experiments, as well as to analyze and interpret data</td>
<td>Assignments, course technical paper, and exam questions</td>
</tr>
<tr>
<td>3</td>
<td>Students will be able to exhibit an ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs, within realistic constraints specific to the field</td>
<td>Assignments, course technical paper, and exam questions</td>
</tr>
<tr>
<td>9</td>
<td>Students will be able to acknowledge a recognition of the need for, and an ability to engage in continuing professional development and life-long learning</td>
<td>Study of different cryptographic algorithms and hardware-based security methods</td>
</tr>
<tr>
<td>10</td>
<td>Students will be able to demonstrate a knowledge of contemporary issues</td>
<td>Exam questions</td>
</tr>
</tbody>
</table>

**UNR Athletics:** If you are involved with any university-sponsored athletic activities that will have an impact on your attendance, please provide your Instructor with a letter from your coach and/or the UNR Athletic Department as soon as possible, but no later than the end of the second week of classes. This should include the official schedule of your activities which will impact your attendance throughout the semester.

**Academic Success Services:** Your student fees cover usage of the Math Center, Tutoring Center, and University Writing Center. These centers support your classroom learning; it is your responsibility to take advantage of their services. Please keep in mind that seeking help outside of class is the sign of a responsible and successful student.

**Disability Statement:** If you have a disability for which you will need to request accommodations, please contact me or someone at the Disability Resource Center (Thompson Building, Suite 101), as soon as possible to arrange for appropriate accommodations.

**Class Recording:** Surreptitious or covert video-taping of class or unauthorized audio recording of class is prohibited by law and by Board of Regents policy. This class may be videotaped or audio recorded only with the written permission of the instructor. In order to accommodate students with disabilities, some students may have been given permission to record class lectures and discussions. Therefore, students should understand that their comments during class may be recorded.