Instructor: Dr. Habib Louafi  
Email: habib.louafi@uregina.ca  
Office: CW 308.5  
Telephone: (306) 337-3144  
Office Hours: TBD  
Other times by appointment  

Calendar Description

This course presents the objectives and the fundamentals of computer and network system security: confidentiality, integrity, availability, authentication, and authorization. Common security concepts are detailed, such as cryptography, symmetric/asymmetric encryption, digital signature, certificate authority, hashing, communication protocol security, and audit. Mathematical foundations and applications of these methods will be explained.

Lectures: Tuesday & Thursday 10:00 AM – 11:15 AM  
Location: Research and Innovation Center, 208

Evaluation:  
Assignments (2 x 10%) 20%  
Labs (2-3 labs) 15%  
Research project 25%  
Final exam 40%  
Total 100%  
Instructor Discretion +/- 5%

Research Project Schedule

- Select a topic to develop (approved by the instructor)  
- Submit a description of the project, 2 pages max (20%)  
- Oral presentation in class, 20 min max (30%)  
- Submit your final report, 20 pages max (50%)

Final Exam: Apr 22, 2021, 9:00 AM – 12:00 PM
Course Outline

• **Introduction**
  • Terminology
  • Security Objectives
  • Obstacles of security
  • Types of attacks
  • Defense mechanisms
  • Trust concept

• **Basic concepts**
  • Symmetric encryption/decryption
  • Asymmetric encryption/decryption
  • Digital signature
  • Hashing

• **Symmetric encryption**
  • Encryption concept
  • Encryption algorithms
  • Performance comparison
  • Entropy

• **Asymmetric encryption**
  • Mathematical background
  • RSA-encryption/decryption/Signature
  • Rabin-Signature, Diffie-Hellman, El Gamal

• **Hashing: data integrity and authentication**
  • Hashing applications
  • Cryptographic hashing
  • Symmetric hashing
  • Attacks on hashing systems

• **Communication protocols**
  • Protocols
  • Key distribution
  • Authentication

• **Security of centralized systems**
  • Security levels and classification
  • Integrity models
  • Access control
  • Control granularity

• **Security of distributed systems**
  • Network threats/attacks
  • End-to-end encryption
  • Traffic control
  • Packet filtering

• **Audit**
  • Logging systems
  • Audit procedure
  • Attack mitigated by audit
Lecture Notes

PowerPoint slides made by the Instructor will be posted on UR Courses. The class instructor will not give out his slides.

Textbook:


Other References

- Selected research papers will also be used.

Contact Information

- The best way to contact me is by email using the address above. Note that I will deal only with emails sent from the University server (uregina.ca). This ensures that your email won’t be blocked by spam filtering.
- Check URCourses and your University email on a regular basis. Important announcements for this class will be made on URCourses. Other announcements and direct communication will be via email.
- If you need special accommodations, please contact the Center for Student Accessibility (http://www.uregina.ca/student/accessibility/).

Policies and Procedures

- Please read the sections of the University of Regina Undergraduate Calendar (see http://www.uregina.ca/gencal/ugcal) dealing with attendance, evaluation, discipline and appeals, especially those regulations regarding academic integrity and plagiarism. Cheating will not be tolerated. Co-operation on programming assignments is generally encouraged, but it must be limited to verbal discussion of concepts; not program code or any other written documentation that is submitted for grading. Copying of assignments or previous solution keys is plagiarism. Knowingly allowing an assignment to be copied will also be treated as plagiarism. The consequence of plagiarism or any other form of cheating (such as copying on a quiz or examination) may range from a zero grade, to failure in the class, to expulsion from the University. Please note that the Dean of your Faculty will be notified of any such incident, as per University regulations.
- Article 5.13.1.1 in the Undergraduate Calendar stipulates that students are to conduct themselves responsibly and with propriety both in their studies and in their general behaviour. Misconduct, which may be in general behaviour, is subject to disciplinary action. Any student disturbing the class meeting will be asked to leave the room immediately.
• If you have any concerns regarding a class mark, then take the following two steps:
  • clearly explain your concerns in an email;
  • send the email to the class instructor. You must send this email with your concern about a class mark within one week after receiving the class mark.
• There are no make-up assignments or exams. Students who miss any of the assignments or lab final must provide a valid reason with documentation. In such cases, marks for the missed quiz or examination will be reallocated to the final examination.
• Deferred final examinations can only be granted by the Associate Dean (Academic) (for Faculty of Science students), or by the Deans (and/or Associate/Assistant Deans) of other Faculties or Federated Colleges. Deferred final examinations cannot be granted by the course instructor.
• Special needs: Students in this course who may have need for specialized accommodations, should please discuss these accommodations with the class and lab instructors, and should also contact the Centre for Student Accessibility/Disability Resource Office (Riddell Centre, Room 251.15, 585-4631).