UNIVERSITY OF CALGARY
FACULTY OF SCIENCE
DEPARTMENT OF COMPUTER SCIENCE
COURSE OUTLINE

1. **Course:** CPSC 526, Network Systems Security -- Fall 2017

   Lecture 01: (TR, 14:00-15:15 in EEEL161)

Instructor Name	Email	Phone	Office	Hours
Pavol Federl	pfederl@ucalgary.ca	403-220-5103	ICT742	Friday 11:00 - 13:00

   Course Site:

   D2L: CPSC 526 L01-(Fall 2017)-Network Systems Security

   Department of Computer Science: ICT 602, 403 220-6015, cpsc@cpsc.ucalgary.ca

2. **Prerequisites:**

   See section 3.5.C in the Faculty of Science section of the online Calendar.

   Computer Science 441.
   Credit for both Computer Science 526 and 529 will not be allowed.
   Computer Science 329 and one of Pure Mathematics 329, Computer Science 418, or Pure Mathematics 418 are recommended as preparation for this course.

3. **Grading:**

   The University policy on grading and related matters is described in F.1 and F.2 of the online University Calendar. In determining the overall grade in the course the following weights will be used:

Component(s)	Weighting %
Assignments	90%
Final Exam (In Class Thursday December 7, 2017 in EEEL 161)	10%

   Each piece of work (reports, assignments, quizzes, midterm exam(s) or final examination) submitted by the student will be assigned a percentage score. The student's average percentage score for the various components listed above will be combined with the indicated weights to produce an overall percentage for the course, which will be used to determine the course letter grade.

   The conversion between a percentage grade and letter grade is as follows;

Letter Grade	A+	A	A-	B+	B	B-	C+	C	C-	D+	D
Minimum Percent Required	95	90	85	80	75	70	65	60	55	50	45

   In order to obtain a final grade of C- or better, and to pass the course, a student must achieve a C- or better in the final exam.

4. **Missed Components of Term Work:**

   The regulations of the Faculty of Science pertaining to this matter are found in the Faculty of Science area of the Calendar in Section 3.6. It is the student's responsibility to familiarize himself/herself with these regulations. See also Section E.3 of the University Calendar

5. **Scheduled out-of-class activities:**

   There are no out-of-class activities scheduled for this course.

6. **Course Materials:**

   Optional Textbook(s):

   Kaufman, Perlman, Speciner, Network Security: Private Communication in a Public World, 2nd Edition, Prentice Hall

   Lectures slides and other support material will be posted on D2L.

7. **Examination Policy:**

   Closed book. No aids are allowed on tests or examinations.

   Students should also read the Calendar, Section G, on Examinations.

8. **Approved Mandatory and Optional Course Supplemental Fees:**

   There are no mandatory or optional course supplemental fees for this course

9. **Writing across the Curriculum Statement:**

   In this course, the quality of the student's writing in the weighted components of the course will be a factor in the evaluation of these components. See also Section E.2 of the University Calendar.

10. **Human studies statement:**

    Students will be expected to participate as subjects or participants in projects.

11. **OTHER IMPORTANT INFORMATION FOR STUDENTS:**

    a. **Misconduct:** Academic misconduct (cheating, plagiarism, or any other form) is a very serious offence that will be dealt with rigorously in all cases. A single offence may lead to disciplinary probation or suspension or expulsion. The Faculty of Science follows a zero tolerance policy regarding dishonesty. Please read the sections of the University Calendar under Section K. Student Misconduct to inform yourself of definitions, processes and penalties.

    b. **Assembly Points:** In case of emergency during class time, be sure to FAMILIARIZE YOURSELF with the information on assembly points.

    c. **Academic Accommodation Policy:** Students needing an Accommodation because of a Disability or medical condition should contact Student Accessibility Services in accordance with the Procedure for Accommodations for Students with Disabilities available at procedure-for-accomodations-for-students-with-disabilities_0.pdf.

       Students needing an Accommodation in relation to their coursework or to fulfil requirements for a graduate degree, based on a Protected Ground other than Disability, should communicate this need, preferably in writing, to the Associate Head of Undergraduate Affairs of the Department of Computer Science, Nathaly Verwaal by email nmverwaa@ucalgary.ca or phone 403-220-8485.

    d. **Safewalk:** Campus Security will escort individuals day or night (www.ucalgary.ca/security/safewalk/) . Call 403-220-5333 for assistance. Use any campus phone, emergency phone or the yellow phones located at most parking lot pay booths.

    e. **Freedom of Information and Privacy:** This course is conducted in accordance with the Freedom of Information and Protection of Privacy Act (FOIPP). As one consequence, students should identify themselves on all written work by placing their name on the front page and their ID number on each subsequent page. For more information, see also www.ucalgary.ca/legalservices/foip.

    f. **Student Union Information:** VP Academic, Phone: 403-220-3911 Email: suvpaca@ucalgary.ca. SU Faculty Rep. Phone: 403-220-3913 Email: sciencerep@su.ucalgary.ca; Student Ombudsman, Email: suvpaca@ucalgary.ca

    g. **Internet and Electronic Device Information:** You can assume that in all classes that you attend, your cell phone should be turned off unless instructed otherwise. Also, communication with other individuals, via laptop computers, Blackberries or other devices connectable to the Internet is not allowed in class time unless specifically permitted by the instructor. If you violate this policy, you may be asked to leave the classroom. Repeated abuse may result in a charge of misconduct.

    h. **Surveys:** At the University of Calgary, feedback through the Universal Student Ratings of Instruction (USRI)

survey and the Faculty of Science Teaching Feedback form provides valuable information to help with evaluating instruction, enhancing learning and teaching, and selecting courses. Your responses make a difference - please participate in these Surveys.

i. **SU Wellness Center:** The Students Union Wellness Centre provides health and wellness support for students including information and counselling on physical health, mental health and nutrition. For more information, see www.ucalgary.ca/wellnesscentre or call 403-210-9355.

Department Approval: Electronically Approved **Date:** 2017-09-07 07:56

Course Outcomes

1. By the end of the course, students should demonstrate facility with the task of probing and monitoring a network to discover its topology and the set of services that hosts provide or advertise; this learning outcome is the basis of professional activities like security auditing and penetration testing.
2. Students should be able to demonstrate professional judgement by listing common applied cryptography pitfalls, protocol design pitfalls, and common "snake oil" techniques; students should be able to explain to another student the impact on trustworthiness that each of these pitfalls has; students should demonstrate this capability by examining source code implementations that use applied cryptography like SSL libraries and observing the (possibly inadequate) use of file hashes and signatures on open-source software distribution archives.
3. Students should demonstrate the ability to use standard message encryption and integrity protection protocols and standards; for example, students should be capable of sending and receiving encrypted email and describing the usability challenges of both these standards and the duties involved in key management for various services like PGP, VPN, SSL, and SSH; importantly, students should be capable of explaining the different security guarantees that each such approach provides compared to the others.
4. By the end of the course, students should be capable of using common network monitoring tools (e.g., tcpdump, Wireshark) to capture a significant amount of real network traffic and analyze the resulting trace; the students should be capable of mentally imposing structure on this opaque data artifact and demonstrate this ability by identifying suspicious packets and flows (i.e., collections of packets); students should also be able to explain the context and purpose of an arbitrary packet in such a trace after examining its fields and its relationship to other packets in the trace.
5. By the end of the course, students should be able to use common packet-crafting frameworks to generate arbitrary network messages and craft packets or sequences of packets that express common layer 2 and layer 3 network attacks (e.g., ARP spoofing, ARP poisoning, DHCP spoofing, IP address spoofing); this ability demonstrates knowledge of the "deception surface" and why standard networking protocols cannot be trusted to provide security.
6. By the end of the course, the student should be able to examine and analyze the steps of security protocol descriptions and identify common mistakes and weaknesses; they should demonstrate this knowledge partially by referring to the history of the development of public key cryptography, block ciphers, random number generation, and hashing mechanisms; they should be able to name the state-of-the-art algorithms and standards to use for each of these purposes.
7. At the end of the course, the student should be able to enumerate and explain the semantics of each step of common authentication and network security protocols; the student should be able to identify whether an arbitrary set of protocol messages expresses one of these common protocols; the student should be able to articulate this analysis either in technical prose or with reference to protocol analysis frameworks known in the research literature.