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

1. **Course:** CPSC 626: Network Systems Security
   Lecture Sections:
   L01, TR 14:00-15:15, Pavol Federl, ICT 742, 220-5103, pfederl@ucalgary.ca
   Office Hours: MW 12:00-13:00

   Course Website: http://pages.cpsc.ucalgary.ca/~pfederl/cpsc526w17

   Computer Science Department Office, ICT 602, 220-6015, cpsc@cpsc.ucalgary.ca

2. **Prerequisites:** Consent of Department
   (http://www.ucalgary.ca/pubs/calendar/current/computer-science.html#3620)

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

Research Project	100%

   This course **will not** have a Registrar's Scheduled Final Exam.

   Special Regulations affecting Final grade: None..

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. Section 3.6. It is the student's responsibility to familiarize theirself with these regulations. See also Section E.6 of the University calendar.

5. **Scheduled Out-of-Class Activities:** REGULARLY SCHEDULED CLASSES HAVE PRECEDENCE OVER ANY OUT-OF-CLASS-TIME ACTIVITY. If you have a clash with this out-of-class activity, please inform your instructor as soon as possible so that alternative arrangements can be made.

6. **Course Materials:**
   Network Security: Private Communication in a Public World 2nd Edition, Charlie Kaufman, Radia Perlman and Mike Speciner, Prentice Hall

   Online Course Components:
   Lecture slides will be posted on the course website.

7. **Examination Policy:** None. Students should also read the Calendar, Section G, on examinations.

8. **Approved Mandatory and Optional Course Supplemental Fees:** None.

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. See also Section E.5 of the University Calendar.

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

a) **Misconduct:** Academic misconduct (cheating, plagiarism, or any other form) is a very serious offense 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 which can be found in each classroom and building.

c) **Student Accommodations:** 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 http://www.ucalgary.ca/policies/files/policies/procedure-for-accommodations-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 Computer Science.

d) **Safewalk:** Campus Security will escort individuals day or night (http://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 http://www.ucalgary.ca/secretariat/privacy

f) **Student Union Information:** VP Academic (403) 220-3911 suvpaca@ucalgary.ca SU Faculty Rep (403) 220-3913 science1@su.ucalgary.ca, science2@su.ucalgary.ca and science3@su.ucalgary.ca, Student Ombuds Office: (403) 220-6420 ombuds@ucalgary.ca, http://ucalgary.ca/provost/students/ombuds

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. All communications with other individuals via laptop computers, cell phones or other devices connectable to the internet in not allowed during 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) **U.S.R.I.:** At the University of Calgary feedback provided by students through the Universal Student ratings of Instruction (USRI) survey provides valuable information to help with evaluating instruction, enhancing learning and teaching, and selecting courses (www.ucalgary.ca/usri). Your responses make a difference – please participate in USRI surveys.

Department Approval_____ Date_____

Faculty Approval for
out of regular class-time activity: _____
Date:_____

Faculty Approval for
Alternate final examination arrangements: _____
Date:_____

A signed copy of this document is on file in the Computer Science Main Office

CPSC 626 Syllabus

Review of networking concepts and basic protocols, OSI reference model, IEEE 802.3, UDP, TCP, IP, ICMP, ARP, DNS, SMTP, HTTP

Internet routing, forwarding, BGP, OSPF

Basic cryptographic concepts, constructs, and terminology

Block ciphers

Stream ciphers

Cipher modes (ECB, CBC, OFB, CFB, CTR)

Secret key / symmetric key cryptography

Public key / asymmetric key cryptography

Hash algorithms and message authentication codes (HMAC, MD)

DES, 3DES, AES

MD2,MD4,MD5, SHA-1, SHA-2

Review of Mathematical concepts underpinning public key cryptography

RSA

Diffie-Hellman

Authentication Protocols, Attacks and Defenses

Secure Protocol Design, Concepts and Implementations

Password authentication schemes, strong password protocols

Security handshakes and protocol primitives

SSH

IPsec

SSL/TLS

Kerberos v4 and v5

Certificates and PKI

Network Defense: Attacks and Countermeasures

Packet Crafting

Sniffing

Intrusion Detection

DoS, DDoS

Legal and ethical issues involved in network monitoring

Secure email, PGP

Firewalls, tunnels

Web Security

Folklore and security protocol design advice

Learning Outcomes:

By the end of the course, students will:

• 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.
• 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.
• 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.
• 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.
• 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.
• 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.
• 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.

Allowable Sources:

No Restrictions on source material.

Cited Sources:

If you used an article, book, function or algorithm that you did not create for this course you must cite it. (This means you may have to cite yourself!) Use APA for citations in a report, paper or in the header documentation of computer code you submit. If citing a website, make sure you include the date you accessed the website. Don't forget to cite code that you used, even if you modified the code.

Level of Collaboration between Students:

You may discuss the assignments with other students in the class but do NOT share any code, do not ask others to provide you with code and do not show code that you have created for assignments to other students.

Disclosure Policy

If you discuss the assignments with others, make sure to cite these discussions.