1. **Course:** CPSC 525: Principles of Computer Security  
   CPSC 625: Principles of Computer Security  
   **Lecture Sections:**  
   L01, TR 12:30-13:45, ICT 114, Philip Fong, ICT 640, 210-6229, pwlfong@ucalgary.ca  
   Office Hours: TR 16:00-17:00  
   **Course Website:** http://www.cpsc.ucalgary.ca/~pwlfong/525  
   http://www.cpsc.ucalgary.ca/~pwlfong/625  
   **Computer Science Department Office, ICT 602, 220-6015, cpsc@cpsc.ucalgary.ca**

2. **Prerequisites:** CPSC 525: CPSC 457 and either MATH 271 or 273  
   CPSC 625: Consent of the 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:

<table>
<thead>
<tr>
<th>CPSC 525</th>
<th>CPSC 625</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignments</td>
<td>45%</td>
</tr>
<tr>
<td>Project Proposal</td>
<td>5%</td>
</tr>
<tr>
<td>Project Report</td>
<td>50%</td>
</tr>
<tr>
<td>Project Report</td>
<td>50%</td>
</tr>
</tbody>
</table>

   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 themself 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 assignments can be arranged.

6. **Course Materials:**  
   None.

   **Online Course Components:**  
   Lecture slides and reading materials will be made available on the course webpage.

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](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 fulfill 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/](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](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](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 ([http://www.ucalgary.ca/usri](http://www.ucalgary.ca/usri)). Your responses make a difference – please participate in USRI surveys.

Department Approval__________________________________________Date__________________________

Associate Dean’s Approval for
out of regular class-time activity: __________________________________Date:__________________________

Associate Dean’s Approval for
Alternate final examination arrangements: __________________________Date:__________________________

*A signed copy of this document is kept on file in the Computer Science main Office ICT 602*
<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>95-100</td>
</tr>
<tr>
<td>A</td>
<td>90-94</td>
</tr>
<tr>
<td>A-</td>
<td>85-89</td>
</tr>
<tr>
<td>B+</td>
<td>80-84</td>
</tr>
<tr>
<td>B</td>
<td>75-79</td>
</tr>
<tr>
<td>B-</td>
<td>70-74</td>
</tr>
<tr>
<td>C+</td>
<td>65-69</td>
</tr>
<tr>
<td>C</td>
<td>60-64</td>
</tr>
<tr>
<td>C-</td>
<td>55-59</td>
</tr>
<tr>
<td>D+</td>
<td>50-54</td>
</tr>
<tr>
<td>D</td>
<td>40-49</td>
</tr>
<tr>
<td>F</td>
<td>0-39</td>
</tr>
</tbody>
</table>
Tentative Topics Covered


Learning Outcomes:

By the end of the course: students will:

- By the end of the course, students should be able to use their knowledge of evaluation standards, the Security Mindset, and analysis tools to produce a security review of a product, protection technique, or security mechanism.
- By the end of the course, students should use common debugging and program analysis tools and frameworks to explain the internal state of programs and systems to an observer and hypothesize how the program or system reached that state, including identifying any cross-layer interactions, composition of trust relationships in the software, and the efficacy or influence of countermeasures.
- By the end of the course, students should be able to list three major security models (Biba, Bell-LaPadula, and Clark-Wilson), enumerate the rules defining each model, and identify the standard purpose of each model.
- Using the Security Mindset, students should be able to critique an arrangement of protection mechanisms, or a system, or program logic; the student demonstrates the validity of such a critique by offering evidence that their crafted input has some correlation with the perceived coding mistake.
- By the end of the course, students should be able to apply the Security Mindset: a way of thinking about systems that envisions how they can be made to fail by supplying unanticipated input or environmental conditions; the advanced student should be able to hypothesize how such failure states could be customized for external control of the compromised application.
- By the end of the course, the student should demonstrate the operation of common access control mechanisms in operating systems, among others; in addition, students should be able to offer a critique of common access control models like RBAC.
- By the end of the course, students should be able to list common static analysis techniques and tools and demonstrate the ability to run such tools on real, large software code Students should also be able to list common (e.g., NIST) security evaluation standards; the advanced student will be able to list specific evaluation criteria from the appropriate model.
- By the end of the course, students should be able to explain how coding mistakes lead to specific classes of code injection vulnerabilities; students should be capable of both purposefully writing and exploiting such a weakness; students should be able to list common, deployed countermeasures to code injection attacks.
- By the end of the course, students should be able to explain the genesis of the field of computer systems security by referencing the seminal security literature elucidating those models in addition to the seminal work on protection domains; the students should be able to map the memory protection concepts in the research literature circa 1970 to the memory protection techniques used in modern processors.