

Course web page:
<http://ugweb.cs.ualberta.ca/~c299/W08/B1/index.shtml>

CMPUT 299 B1 Security in a Networked World Course Syllabus

Date and Time: MWF at 1:00-1:50pm
Location: TEL 134
Number of credits: 3

Instructor:

Ioanis Nikolaidis <yannis@cs.ualberta.ca> Office: ATH 3-22, Phone: 492-5757, Office Hours: MW 2pm-3pm or e-mail for appointment

Note:

to arrange meetings outside the two hours indicated, I prefer that you contact me by e-mail to set up a meeting time which is mutually convenient. This allows me also to group meetings in consecutive time slots. By default, I assume a 15 minute slot. If you anticipate that a 15 minute meeting is not enough, then please let me know in advance.

Teaching Assistants: Jianzhao Huang <jianzhao@cs.ualberta.ca> Reza Sadoddin <sadoddin@cs.ualberta.ca>

Note:The Lab facility that will be used is CSC 235. Time in the Lab will be allocated on-demand as the term progresses. Labs will also be the place to meet and consult the TAs about assignments. TAs are not obliged to have additional office hours beyond the hours that they provide assistance during the labs. Also, on occasion, TAs present valuable information of tutorial value during the lab sessions. Such presentations are announced in advance (this is one good reason to check your e-mail, the course newsgroup, and the course web pages on a daily basis).

Newsgroup: ualberta.courses.cmput.299

Note:

Use the usual posting etiquette for newsgroups, but also pay particular attention to (a) not giving away answers that compromise the assignments (e.g., supplying source files etc.) and (b) not expecting to use the newsgroup as a means to get a quick solution to a technical problem you are facing (as it usually happens a few hours before an assignment deadline). We will do our best to answer questions posted in the newsgroup within a working day, and sometimes we will answer very quickly, but this is not a guarantee that the newsgroup will provide you the solutions you need in real-time. During weekends, we reserve the right to rest (including not responding to the newsgroup postings) and you should try to rest as well!

Overview

The course provides an introduction to the security issues related to the design and operation of networked information systems. The network under study is our familiar TCP/IP-based Internet. We also consider specific end-user network access technologies, such as wireless local area networks. The systems studied provide services running on network nodes (web, login/shell, file sharing, etc.) that interact with other servers at other nodes, or, directly, with the end-users. We define the usual information assurance objectives (confidentiality, integrity, and authentication) and describe how they can be implemented. We review the sources of existing vulnerabilities, and the tools and techniques used to fix them, or to minimize their impact. Essentially the course presents concepts of TCP/IP networking, basic Operating System capabilities, and cryptography, that, when combined appropriately, provides the security objectives of large networked systems. The course is both an examination of the "arms race" of measures and counter-measures in the world of security, as well as an extensive introduction into what are current good practices for building secure systems.

Objectives

The purpose of the course is to familiarize you with the multiple facets of security in large interconnected networks, such as the Internet. At the end of the course, a student will be able to (a) identify the security requirements of a system (at the network protocol, OS, application, and user level) and whether example systems provide the required assurances, (b), select the

appropriate tools that allow the study of security vulnerabilities of systems, (c), recommend the right fixes to safeguard vulnerable systems using mostly existing technologies, e.g. firewalls, (d) recognize at a conceptual level what would be the value of cryptography to achieve particular security requirements in a system, and (e) be familiar with some of the current best practices for developing secure systems.

Pre-requisites

CMPUT 201 is a *recommended* pre-requisite or co-requisite because material related to certain vulnerabilities is best illustrated through the use of C as the programming language of choice. Note that CMPUT 313 is *not* a pre-requisite. The intention of the course is to be accessible to a wider audience than just Computing Science majors. For more information contact the instructor.

Course Topics

- Definitions and Terminology
- Host Security (authentication and authorization techniques)
- Review of Shared Key Cryptography & Hash Functions
- Basic Public Key Cryptography (DH, RSA, CAs, PKI)
- Introduction to the TCP/IP Stack
- Network Security (ports & protocols)
- Firewalls and Firewall Rules
- Application Security (vulnerabilities of programming/scripting languages)
- Malicious Code (virii, worms, malware)
- Securing Services (shells, e-mail, web servers)
- Identifying Vulnerabilities (tools & techniques)
- Intrusion Case Studies
- Wireless Security
- Basics of Intrusion Detection

The topics are not presented in the exact sequence listed above. In fact some (e.g., case studies, or, identifying vulnerabilities) are interleaved as needed with the other topics.

Since this is the first time the course is offered, the instructor will rely on student *feedback* throughout the term for appropriately pacing and tuning the topics.

Course Work and Evaluation

Course Work	Date	Weight
Assignment 1	February 5th	12%
Assignment 2	March 11th	15%
Assignment 3	April 3rd	15%
Midterm Exam	February 27th	18%
Final Exam	April 18th (2pm)	40%
Deferred Exam	April 28th (9am)	(40%)

Please double check the Final Examination date and time by consulting the *Official Fall 2007 / Winter 2008 Exam Planner* (<http://www.registrar.ualberta.ca/ro.cfm?id=360>). In case of disagreement between the contents of this syllabus and the official exam planner, the official exam planner will be the authoritative source.

All assignments are to be submitted no later than **6:59pm** on the due date. Late submissions are **not** accepted.

Grading System

The course is marked according to the grade distribution of 3rd year undergraduate courses. I try to interpret "61.6 *University*

of *Alberta Marking and Grading Guidelines*" as faithfully as the situation allows. Occasionally, adjustments (to the benefit of the students) are made when it is evident that a course component (e.g. a midterm) was "harder" than expected. No absolute totals are required for passing the course. However, experience shows that the class average (if 100% is perfect score) tends to be close to the mid-60% and the failing grade is close to the 30%. Both types of components, i.e., assignments and exams, matter. The somewhat larger contribution of the exam scores suggests a somewhat more prominent role of the exams in the total mark. The key to success in this course is the proper organization of your time. It never, repeat: NEVER, works to wait with an assignment until a few days before the deadline.

Deferred Exams

The deferred examination date is April 28th, 2008 at 9am. You can take the deferred final exam *only if* the Faculty grants you an excused absence from the final examination.

Re-evaluation

Any questions or concerns about marks on a particular assignment or exam must be brought to my attention within 10 days of the day you are notified about your mark for the assignment/exam. After 10 days, I will not consider remarking or re-evaluating the work. Note that what counts as notification is either an e-mail message to your CCID account, OR a newsgroup announcement instructing you on how to access your mark or marking sheet. Make sure you check daily your CCID e-mail account *and* the course newsgroup.

Important:

If you have a question or concern about marks on a particular assignment, your first point of contact is the TA (or TAs) that marked the assignment in question. Since the question/concern must be brought to the instructor's attention within 10 days of the day you are notified about your mark for the assignment/exam, the best way to initiate the process of possible assignment re-evaluation is (within the 10 day period) to send the TA an e-mail and to cc- to the instructor. This approach lets the instructor know that you are actively pursuing a re-evaluation and that you are in discussions with the TA. If after contacting the TA, you still think the assignment should be re-considered, then you should contact the instructor directly

Course Materials

Required textbook: W. R. Cheswick, S. M. Bellovin, and A. D. Rubin, **Firewalls and Internet Security**, 2nd Edition, Addison-Wesley, 2003. (ISBN 0-201-63466-X).

Supporting (Online) Book: A. Lockhart, **Network Security Hacks**, 2nd Edition, O'Reilly, 2006. (ISBN 0-596-52763-2) [FREE access via UofA's Library site as part of *Safari Books Online*.]

Reference (Online) Book: A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, **Handbook of Applied Cryptography**, CRC Press, 1996. (ISBN 0-8493-8523-7) [FREE access to all chapters.]

General Interest Book: B. Schneier, **Secrets and Lies: Digital Security in a Networked World**, John Wiley & Sons, 2000. (ISBN 0-471-25311-1) [Not required for any component of the course, but it *did* inspire the title of the course.]

Additional materials to assist you in your study are made available as needed throughout the term in the **Resources** section and their availability is announced in class. Consult also the course schedule page for a weekly updated summary of what was covered in class (and an idea of what is planned next).

Policies

Course Outlines

Policy about course outlines can be found in Section 23.4(2) of the University Calendar.

Academic Integrity

The University of Alberta is committed to the highest standards of academic integrity and honesty. Students are expected to be familiar with these standards regarding academic honesty and to uphold the policies of the University in this respect. Students

are particularly urged to familiarize themselves with the provisions of the Code of Student Behaviour (online at www.ualberta.ca/secretariat/appeals.htm) and avoid any behaviour which could potentially result in suspicions of cheating, plagiarism, misrepresentation of facts and/or participation in an offence. Academic dishonesty is a serious offence and can result in suspension or expulsion from the University. (GFC 29 SEP 2003).

Collaboration

All course work should be individually completed. This includes any programs and/or documentation. Please exercise judgment when posting to the newsgroup to not disclose many implementation details that would allow your implementation to be easily replicated by others. If you need to use a non-trivial piece of source code that is available through the web, found in a textbook, or available in any other way, you need to first get the permission of the instructor in order to use it. Even when permission is given by the instructor, the use of source code from external sources (web, textbooks, etc.) should be cited the same way you would cite published works.

Note:

In the event of suspicion of collaboration, plagiarism, and cheating in general, the instructor and the TAs reserve the right to use automated means (e.g. software tools) that provide information about the extent to which two or more student submissions are similar.

Excused Absences

Assignments:

You can request the late submission of an assignment due to incapacitating illness, severe domestic affliction or other compelling reason, provided supporting documentation (e.g., a doctor's note) is provided within 48 hours of the assignment deadline (or later if warranted by the nature of the incapacitating event). In the case of a doctor's note, you must have been seen by the doctor on the date that the assignment was due. Requests may be denied by the instructor. If the request is accepted, then submission of the assignment up to 48 hours past the assignment's deadline will be accepted (without any penalty). If the nature of the incapacitating event is such that it is impossible to submit the assignment within 48 hours of its original deadline, then, if the request is accepted, the missed assignment's mark will be set to the average of the remaining two assignments. No more than one late assignment submission is granted per student over the entire term, regardless of excuse.

Midterm:

You can request consideration for excused absence from the midterm due to incapacitating illness, severe domestic affliction or other compelling reason, provided supporting documentation is provided within 48 hours of the scheduled midterm. In the case of the midterm, supporting documentation for illness must be in the form of a completed U. of Alberta Medical Statement Form (and you have to be seen by the doctor on the day of the midterm), or other appropriate documentation (consistent with Calendar section 23.4[3]). Requests may be denied by the instructor. If the request is accepted, then the weight of the midterm is added to the weight of the final exam (i.e., the final exam weight becomes 58%). Deferred midterms are *not* given.

Final: If you cannot take the final examination, the instructor has *no control* over the process of deferral. In this case, the student must formally apply for a deferred examination to the student's Faculty office within 48 hours. If the Faculty decides to grant you a deferred examination, it will inform the instructor. The date and time of the examination is as listed in the "Course Work and Evaluation Section" above.

Additional Policies

Except for the policies listed here, be certain that you are also aware of the Departmental Policies (e.g. as they pertain to Conditions of Use of facilities) as well as of the University Policies (e.g., Electronic Communication Policy, Code of Student Behaviour, Student Appeals, etc.)