



CMPT 320 Intranet and Internet Security SYLLABUS

General information (SPRING 2010)

CMPT 320-01	Monday AND Wednesday	1:00 – 2:15 pm	RI 376
CMPT 320-02	Wednesday	5:30 – 8:00 pm	RI 376

Instructor: Dr. Stefan A. Robila Phone: (973) 655-4230
Office: 312 Richardson Hall Email: robilas@mail.montclair.edu
Office Hours: Monday 10:30-11:30am, Wednesday 4:00-5:00pm or by appointment

Purpose of the course

An overview of the fundamental problems of computer security, followed by an in-depth analysis of the current solutions including encryption, public key schemes, testing and analyzing current network and Internet architectures based on security considerations. The general objective of this course is to introduce students to the current paradigms in intranet and internet security and to develop basic skills for applying that knowledge in practice. Students will learn fundamental concepts of security that can be applied to many traditional aspects of computer programming and computer systems design as well as in dealing in day to day activities such as accessing confidential information, protecting computer systems, etc.

Prerequisites

Knowledge of Discrete Mathematics on the level of CMPT 285 or MATH 501 is expected. A programming proficiency at the CS II (CMPT 184) level or equivalent is expected. Basic understanding of computer organization, and programming is assumed.

Promises

On Monday, January 5, 2009, Twitter.com disclosed on their blog that they "discovered 33 Twitter accounts had been "hacked" including prominent Twitter-ers like Rick Sanchez, (Britney Spears) and Barack Obama (who has not been Twittering since becoming the president elect due to transition issues). We immediately locked down the accounts and investigated the issue. Rick, Barack, and others are now back in control of their accounts."

(<http://blog.twitter.com/2009/01/monday-morning-madness.html>)

Hacking a Twitter, or any other social network account may not be a very significant action, however, given the high profile of the victims, it does raise a significant question: how safe is our information?

To answer this question, we should first understand how are we vulnerable and how can we protect ourselves. From this, we will learn how to help protect others' information. For this, we will try to achieve the following course outcomes:

- 1) *Investigate what the internet and intranet are. What types of networks do we have? Who owns them? How are they managed?*

- 2) *Discuss major issues concerning computer security. What does secure mean? What needs to be protected? For how long?*
- 3) *Learn how to write professionally about security using the terms of art. Is the government requiring us as professionals to do so? Why or why not?*
- 4) *Use and evaluate the security of commercial security products, organizational policies, and software designs. Out of so many, which should we adopt? How do we know they provide the 'protection' they claim or they need?*
- 5) *Identify security breaches in a computer network. What is a breach?*
- 6) *Study variety of cryptographic algorithms and protocols underlying network security applications.*

Does this mean that at the end of this course will we all become security experts? After all, we are vulnerable:

"On Sunday morning, security consultant Alan Shimel woke to discover that his personal blog, which is frequented by countless peers and reporters, was pointing to a website featuring explicit porn. Equally disturbing, he found someone had cracked open his Yahoo! Mail account and aired sensitive documents he filed with the Internal Revenue Service. Oh, and while the miscreants were at it, they sent crude pornographic images to parents on the Little League baseball team Shimel coached. The chief strategy officer for security firm StillSecure, Shimel is one of three high-profile researchers in the security world known to have been attacked by unknown criminals over the past week. A personal Gmail account belonging to Petko D. Petkov, of the GNUCitizen ethical hacking collective, was ransacked and 2GB of its contents made public. And logs believed to come from the home blog of Security-Protocols.com researcher Tom Ferris have also been exposed."

(August 13, 2008, http://www.theregister.co.uk/2008/08/13/security_researchers_targeted/)

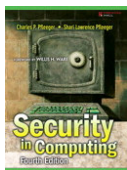
But an informed person can tackle problems better. After all knowledge and curiosity are powerful tools:

"And so it happened that on my second day at work, Dave wandered into my office, mumbling about a hiccup in the Unix accounting system. Someone must have used a few seconds of computing time without paying for it. The computer's books didn't quite balance; last month's bills of \$2,387 showed a 75-cent shortfall"... The phone's ringing. It's Lawrence Livermore Laboratory—a place I've stayed away from because they design nuclear bombs. A hacker's breaking into their computer. They want my help. They think I'm a wizard." Cliff Stoll. *The Cuckoo's Egg*. Simon & Schuster, Inc., New York, 1990

(http://www.ci.ulsu.mx/~elinod/docencia/herseg/cuckoo_egg.pdf)

How will you fulfill these promises?

To realize these promises, you MUST take responsibility for your own learning and participate as an active learner. Students of internet and intranet security have indicated that the best way to learn is by reading and experimenting. You are provided with a textbook as well as with other various reading material (in electronic form) that you will read, analyze, and think about between each class. The textbook is available through the University's bookstore as well as at various online retailers:



Charles P. Pfleeger, Shari L. Pfleeger, *Security in Computing*, 4th Edition, Prentice Hall, ISBN-10: 0-13-239077-9; ISBN-13: 978-0-13-239077-4; Published: Oct 13, 2006; Copyright 2007; Dimensions 7x9-1/4; Pages: 880; Edition: 4th.

Here is a list of additional materials that you have available:

- Robila, Notes available on Blackboard

- Robila, Collection of links available on Blackboard
- Textbook author supplements: <http://authors.phptr.com/pfleeger/security3e/>
- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001, available online at: <http://www.cacr.math.uwaterloo.ca/hac/>
- National Institute of Standards and Technology – Computer Security Division: <http://csrc.nist.gov/>

Use these readings to challenge yours and your colleagues beliefs. Discuss what you learn with your peers and your faculty and see if their understanding is different than yours. There are also plenty of other information sources that will help you understand better the course. A list of them will be provided and maintained on **Blackboard**. Feel free to email me additions to it.

The class format will be a sequence of presentations and discussions on security related topics. The presentations will be done by the instructor, students as well as invited guests. The class includes examinations, assignments and a project. The project includes a significant writing component that will be developed in multiple stages. The lecture materials, homework and project description are found online on **Blackboard**.

In addition, some of the class activities and assignment questions will involve hands on activities that will allow you to experiment with tools such as Hacme Bank, Nmap, and Paros Proxy. Such tools are used today by security professionals to evaluate computing environments. Learning how to use them will allow you to get a better understanding of the topics, and prepare you for being successful in your future career.

The goal for this class is to cover the following major topics:

- 1) cryptography techniques (encryption types, secret and public key methods, key exchanges, etc.)
- 2) network protection (topologies, types of threats, protection, etc.)
- 3) OS security (memory protection, file protection, users, trusted OS)
- 4) database security (reliability, sensitive data, etc.)
- 5) program security (viruses, buffer overflows, trapdoors)
- 6) enterprise security (policies, planning, etc.)
- 7) social engineering and other human aspects of security
- 8) basic security threats on networks connected to the Internet
- 9) security resources available for the Internet.
- 10) ethics in protection
- 11) pseudosecurity (steganography, watermarking. etc.)

How do we evaluate the progress

The grade for this course will assess your ability to analyze concepts and use tools appropriate to this field. To evaluate your progress we will look at the following items:

Homework (35%): Several homework assignments will be provided. They will cover the topics presented during the lectures and are to be solved individually by each student. While interaction with your colleagues is encouraged, by submitting individual work you push yourself to determine if you understood the concepts covered in the tasks.

Written Examination (25%): In many situations, a professional must provide a solution in a limited amount of time. A written examination will assess how well will you respond to such challenge. This course includes a one in class examination that will cover the topics on data encryption and network security.

Term Project (40%): As computing professionals we often embark on new and exciting initiatives. We start from a need then refine the requirements, investigate resources, craft an approach, test and revise. This is no longer a weeklong endeavor and requires reading and testing on your own. The term project for this class allows you to develop such skills. It includes choosing a topic (that YOU CARE ABOUT), gathering and analyzing data, writing a scientific paper and giving a short in class presentation. Each of the steps will be assessed individually and you will receive feedback. In addition, some of the projects may require software development. Projects can (and are encouraged to) be done in teams. However, as in real life, a larger team will require the topic and length of the project to be larger.

Based on the evaluation for each of the above items, we will compute a score, and the university requires that a letter grade be provided. No curve will be used in assigning the grades. Instead, here is how the grades will be determined:

Percentage of Total	90%-100%	75%-90%	60-75%	<60%
Grade	A-,A	B-,B,B+	C-,C,C+	D and lower

The splits between plus and minus grades varies depending on the actual distribution of the final averages. However, if your average is 95% or more, you are assured of A. A grade under 50% would amount to failure.

Important notes

It is University policy to provide, on a flexible and individualized basis, reasonable accommodations to students who have disabilities that may affect their successful participation in course activities or to meet course requirements. Students with disabilities are encouraged to contact their instructors to discuss their individual needs for accommodations.

Academic Honesty - Cheating and plagiarism will not be tolerated. Copying work from other students, presenting work not done by you as your own, or otherwise misrepresenting your work will result in penalties including a failing grade for the respective task. University regulations related to this topic will be strictly enforced. At the end of the day you must ask yourself: Why am I here? Will the grade by itself help me?

One Last Note:

When the mainstream media first announced Barack Obama's "victory" in keeping his BlackBerry, the focus was on the security of the device, and keeping the U.S. president's e-mail communications private from spies and hackers. The news coverage and analysis by armchair security experts thus far has failed to focus on the real threat: attacks against President Obama's location privacy, and the potential physical security risks that come with someone knowing the president's real-time physical location. (Chris Sogioian – Surveillance State Blog - http://news.cnet.com/8301-13739_3-10159055-46.html)