MO834D/MC931B - Topics in Computing II

Institute of Computing — Unicamp
Instructors: Diego F. Aranha / André Grégio
E-mail: dfaranha@ic.unicamp.br, gregio@lasca.ic.unicamp.br
Site: http://www.lasca.ic.unicamp.br/~gregio/MO834/

Course Overview

Network-connected systems are under siege by legions of motivated attackers. These attacks may be either directed to a specific target, or a massive spread whose goal is to compromise as many systems as it is possible. Cyber-attackers commonly make use of malicious programs and codes to automate their operations, reaching a wider range of victims while remaining anonymous. Therefore, the development of secure systems is very important to decrease the chance of successful attacks. However, to accomplish better security, it is essential to deeply understand how malicious programs work.

Furthermore, protecting against these threats involves both defensive programming techniques and a development methodology oriented in terms of security testing and validation. To gain knowledge about common shortcomings in current programming languages, operating systems, and the Web is also essential for adopting adequate countermeasures. Critical portions of software security, such as the choice and implementation of cryptographic algorithms, require further attention.

This course will focus mainly on malware analysis and malicious code-based attacks, with strong emphasis on defensive technologies and software security. It will be based on selected papers published in top security venues (conferences and journals). Each student will present at least one lecture in a seminar format to promote the discussion about the chosen topic. Moreover, each student will be required to research a relevant security problem, as well as to propose a practical solution (including related work, solution details, tests, results and limitations) in a conference paper format by the end of the term.

Location and Time

- Tuesday, 19-21pm at CC-52.
- Thursday, 21-23pm at CC-52.

Prerequisites

Students attending this course should be familiar with basic systems security, operating systems, networking concepts, and programming languages such as C and Python.

Course Topics

Attack: attacks against computer systems • malicious programs • botnets and rootkits • packers and obfuscation • bankers and Web malware • malware analysis • antiviruses • sophisticated malware • mobile devices insecurity.

Defense: principles of computer security • secure development • memory corruption • race conditions • code review and security testing • basic cryptography • authentication methods • Web vulnerabilities • information leaks and side-channel protection.

Grading

Students will be evaluated using the following criteria. A minimum of 60% is required for the student's approval:

- 5 practical assignments (undergrad/grad): 40%
  - **Deadlines**: Sep 1, Sep 15, Sep 29, Oct 27, Nov 3.
- 2 paper presentations per student (grad only): 20%
- 1 exam on September 29^{th} (undergrad only): 20%
- 1 final project (undergrad/grad): 40%
- Supplementary exam (undergrad, December 10^{th}, 2015)

Recommended Readings

The course will be based on articles from top conferences and magazines covering hot research about this course's selected topics. There will be no specific textbook for this course. However, the books listed below can help the student to better understand the topics.

- Peter Szor. *The Art of Computer Virus Research and Defense*. Addison-Wesley Professional, 2005.
- Niels Provos, Thorsten Holz. *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Addison-Wesley Prof., 2007.
- Michael Ligh et al. *Malware Analyst's Cookbook*. Wiley, 2010.
- Michael Sikorski, Andrew Honig. *Practical Malware Analysis*. No Starch Press, 2012.
- Gary McGraw, *Software Security: Building Security In*, Addison-Wesley Prof., 2006.
- Michael Howard, David LeBlanc, John Viega, *24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them*, McGraw Hill, 2009.
- Robert C. Seacord, *Secure Coding in C and C++*, 2^a ed., Addison-Wesley Prof., 2013.
- Matt Bishop. *Introduction to Computer Security*, Addison-Wesley, 2004.

Academic Ethics

The student agree to behave honestly and not to cheat on the assignments and project. Moreover, students must follow an ethical and responsible conduct when learning about systems security. Whoever engages in cheating will have the grade **zeroed**.