MO834P/MC931A - Topics in Computing II

Institute of Computing — Unicamp
Instructors: André Grégio / Paulo Lício de Geus
E-mail: 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 aiming to compromise as many systems as it is possible. Cyber-attackers commonly make use of malicious programs to automate their operations and reach a broader range of victims whereas remaining anonymous. Therefore, the development of secure computer networks is very important to decrease the chance of successful attacks. However, to accomplish better security, it is essential to obtain, study and understand malicious programs.

This course will focus mainly on research about malware collection and analysis, and 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 and 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, 21-23pm at CC-51.
- Thursday, 19-21pm at CC-51

Prerequisites

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

Course Topics

Computers and networks attacks and defenses • honeypot • attack data collection • malicious programs • antiviruses • malware analysis • suspicious execution behavior • botnets and rootkits • bankers and Web malware • complex malicious software • mobile malware • detection techniques.

Grading

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

- Class participation: 5%
- Paper presentations: 20%
- Practical assignments: 35%
- Final project: 40%

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 Professional, 2007.
- Michael Ligh et al. *Malware Analyst's Cookbook*. Wiley, 2010.
- Michael Sikorski, Andrew Honig. *Practical Malware Analysis*. No Starch Press, 2012.

Academic Ethics

The student agree to behave honestly and do not cheat on the assignments and project. Moreover, students must follow an ethical and responsible conduct when learning about systems security.