Malicious Code and Digital Forensics

Description and Policies

Spring 2004

Description

Current Catalog Description
This course will study the motivations of malicious code developers and the common weaknesses exploited by such code. The course will then move in to a forensics analysis of techniques for protection and recovery from such malicious code.

Warning/Disclaimer
You are not permitted to write, experiment or distribute malicious code or programs in this course. Viruses, worms, trojans and other forms of malicious code can be extremely dangerous and have destroyed data, caused downtime and cost billions of dollars. You are liable for damages caused by malicious code you intentionally or unintentionally write and/or release. Malicious code writers and those who spread have been fined and jailed for the damage caused by their creations.

Prerequisite by Topic
  • Assembly Language Programming
  • C/C++ Language Programming
  • Compiler Design
  • Intro to database or file management
  • Operating Systems

Course Goals
Students are expected to gain insights into the field of computer forensics, specifically approaches for the identification and remedy of malicious code.

Textbook
Major Topics Covered in the Course

• Computer virus infection and replication techniques.
• Detecting Malware.
• Malware quarantine techniques Removing malware.
• Hardware and file features exploited by malware.
• Techniques for minimizing malware exposure.

Laboratory Projects

1. Familiarization with file formats and opportunities for malware exploitation.
2. Development of a malware detector with the possibility of adding a malware remover, time permitting.

Social and Ethical Issues

Ethical implications of developing and releasing malware.

Theoretical Content

• Security implications of design trade-offs.
• Programming language facilities that enhance or retard malware transmission.
• Theoretical techniques for identification and removal of malware.
• Problem Analysis
• Analysis of hardware and software features that enable malware.
• Techniques for minimization of exposure due to these features.

Solution Design

Design of techniques for discovery, removal, and mitigation of malware.

Policies

Material in addition to the textbook and assigned paper readings is covered in the course lectures. Students are responsible for anything that transpires during a class - therefore if you’re not in a class, you should get notes from a colleague or the course staff (not the instructor).

Assignments are due prior to the beginning of the class period. Late assignments will not be accepted. If an extraordinary situation (for example hospitalization) prevents you from working for a period of time, contact me as soon as possible to discuss your situation and arrange a special schedule. Unless you are unconscious (medically speaking), I need to hear from you before the deadline for any exceptions to be granted.
Requests for regrading must be submitted to the instructor in writing within one week of the time the graded assignment was made available for pickup. You must be specific in saying why you feel your answer deserves additional credit. A request for regrade may result in a re-evaluation of the entire assignment and your total grade may increase or decrease as a result.

Makeup exams will only be given in cases of severe medical or family emergencies. You must contact the instructor to arrange for a special circumstance. Note: personal or business travel is not considered a valid excuse for missing an exam.

Passing the course requires a grade of at least 33/100 on every graded assignment. Any student scoring less than 33/100 on an assignment will receive a grade of F for the course.

Academic Honesty

Students are prohibited from handing in work as their own which they did not create. This includes handing in assignments in which substantial amounts of the material was done by someone else. Students need to be especially careful that in the process of discussing problems with other students they do not inadvertently end up using someone else’s work. Similarly, failing to cite a source that contributed substantially to the solution of a problem is also considered to be cheating. Any literature consulted should be referenced precisely. Posting project solutions to the web or the class mailing list, or making them available to other students in the class, will be considered cheating. Any student who makes their work available to another student to copy, whether knowingly or through negligence, will be penalized for academic misconduct.

In the event a case of cheating is discovered, the student will receive a score of zero (0) for that assignment or exam.

Acknowledgements

Mark Morrissey, Michael Pak, and Dr. Karen Karavanic for their contribution and advise making this course possible.