Forensic Computing Prospectus Seminar[1]
(FCM 791, Spring 2008)

Research Project Title: Web 2.0 Services and Malware Propagation

Instructor: Prof. Douglas Salane

Graduate Student: Mark Frankel

Class Meetings: Section 01, Wed. 6:20-8:20 p.m. or by previous arrangement.

Office Hours: Tues. - period 5, and Thurs. - period 7

Course Description: The student will prepare his M.S. degree thesis. In a detailed research report the student will assess the use and exploitation of Web 2.0 services for malware propagation. In addition, he will propose new methods for deterring malware risks in this new environment.

Course goal and objectives: The Internet rapidly is moving beyond static web pages and controlled scripts executed on client machines. The Web now features highly interactive applications that involve the frequent exchange of active content (code) among many parties. The security weaknesses in these new systems already are being exploited to make possible novel criminal activities or provide new venues for traditional criminal activities, particularly fraud. Mr. Frankel's task is to write a report that summarizes the state of malware propagation in this new environment. In addition his report will recommend measures to deter malware in the so-called Web 2.0 environment. He will have to examine recent reports and scripts from various sources including private security companies, government and government sponsored security organizations, hacker sites and the published literature. Besides developing particular expertise in Web 2.0 security, he will develop new insights into sources of information in this area and thus enhance his capabilities for security research.

Exams/Grading: Grades will be based on a final student research paper, interim reports, and daily class participation that provides evidence of careful and thorough readings of selected papers and sources.

Responsibilities: The student is expected to meet weekly with the instructor. Interim reports and readings must be completed at the scheduled times. The student will be expected to conduct independent research and find new sources of information on the use of web 2.0 services to propagate malware.

[1] Development of this course is sponsored in part by NSF grants 043044 and 0619226

Suggested Text: The Web Applications Hacker's Handbook: Discovering and Exploiting Security Flaws. Dayfydd Stuttard and Marcus Pinto.

Resources: Most information is on the Web. Here are some useful sites: www.gnucitizen.org, www.openajax.org, www.whitehatsecurity.org. Additional security sites are available on the FCM course home pages at web.math.jjay.cuny.edu.

Laboratory facilities: Accounts on the Linux computers in the Forensic Computing Lab will be provided if the student's project requires these facilities. In addition, the student can get accounts to use computers in the 4301 Linux Lab, Departmental research database servers, and the Department's cluster computer.

Academic Integrity: The College web page on academic integrity (http://www.jjay.cuny.edu/academics/762.php) discusses the inappropriate use of another's work, especially when using materials available on-line. The Library Research Web page (http://www.lib.jjay.cuny.edu/research/) provides detailed information on the correct method to cite written and electronic research materials. The student should refer to both of these valuable resources.

Course Outline

The student will research the following topics:

Week 1. Cross site scripting worms and viruses.
Week. 2. Puppet Nets: Use of Web Browsers to build a distributed attack infrastructure
Week. 3. Social networking and malware propagation
Week. 4. Interim Report – I
Week 5. An overview of Asynchronous JavaScript and XML (AJAX)
Week 6. Web services and XML security
Week 7. Hardening web service servers and input validation
Week 8. Interim Report – II
Week 9. Google mashups and alerts to detect vulnerable systems
Week 10. RSS e-mail conversion services to control hacked computers
Week 11. Spreading malicious code through wikipedia
Week 12. Malware propagation on Myspace and Facebook
Week 13. Countermeasures for Web 2.0 Malware
Week 14. Final report and presentation of results