

CSC 570: Computer Viruses and Worms

Summer 2014

General Information

Professor: Sviatoslav (Svet) Braynov

Office: UHB 3117

Email: sbray2@uis.edu (for a faster response please put "CSC570" in the subject)

Course Overview

The purpose of this course is to demonstrate the current state of the art of computer viruses/worms and to teach the methodology of virus/worm analysis and protection. Students will learn malware strategies for infection, in-memory operation, self-protection, payload delivery, exploitation, and more. Previous programming experience is not required.

Course objectives

The goal of this course is to give the students theoretical knowledge of computer viruses and worms, specifically, how they function and how they can be prevented. The course begins with a short introduction, followed by more in-depth coverage of different virus and worm types. Upon completion of the course, students should be able to demonstrate knowledge of the technologies behind viruses and worms; and should be able to analyze and evaluate protection measures.

Textbook

Peter Szor, The Art of Computer Virus Research and Defense, Addison Wesley (Symantec), 2005. ISBN: 0-321-30454-3



Other useful textbooks (optional):

John Aycock, Computer Viruses and Malware, Springer, 2006.

Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard, Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, Wiley, 2010.

Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams, Gray Hat Hacking The Ethical Hackers Handbook, 3rd Edition, McGraw-Hill Osborne Media, 2011.

Bill Blunden, The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System, Wordware Pubising. 2009.

Michael Sikorski and Andrew Honig, Practical Malware Analysis, No Starch Press, 2012.

Expected Topics (time permitting)

- History of self-replicating malware and basic malware terminology
- Malicious code environments
- In-memory strategies of malware
- Self-protection strategies of malware
- Payload
- Advanced code evolution
- Anti-virus defense strategies
- Memory scanning and disinfection
- History of computer worms
- Worm components
- Superworms
- Botnets
- Conficker
- Zeus and ZitMo
- Stuxnet
- TDL-4
- Flame
- Mobile Worms

Useful resources

- Virus Bulletin: <http://www.virusbtn.com/index>
- SecurityFocus: <http://www.securityfocus.com/virus>
- Symantec Security Response : <http://securityresponse.symantec.com>
- VirusList: <http://www.viruslist.com>
- CERT: <http://www.cert.org>
- NIST Virus Information: <http://csrc.nist.gov/archive/virus/index.html>
- TrendMicro Virus Encyclopedia: <http://threatinfo.trendmicro.com/vinfo/virusencyclo/default.asp>
- IBM Antivirus Research: <http://www.research.ibm.com/antivirus/SciPapers.htm>
- Microsoft Malware Protection Center: <http://www.microsoft.com/security/portal>
- ICSA Labs: <https://www.icsalabs.com>
- McAfee Virus Information: <http://home.mcafee.com/VirusInfo/Default.aspx>
- CNET Security Center: <http://www.cnet.com/internet-security>

- Overview of Computer Viruses and Antivirus Software by Bob Kanish: www.hicom.net/~oedipus/virus32.html
- F-Secure: <http://www.f-secure.com/v-descs/new.shtml>
- Lookout: <https://www.mylookout.com/>
- Virus Myths: <http://vmyths.com/>
- Sophos: <http://www.sophos.com>
- About.com: Anti-Virus Software : <http://antivirus.about.com/?once=true>
- Computer Associates' Virus Information Center : <http://www.ca.com/us/anti-virus.aspx>
- European Institute for Computer Anti-Virus Research (EICAR) : <http://www.eicar.org/>
- Hideaway.Net : <http://www.hideaway.net/>
- WildList Organization International : <http://www.wildlist.org/>
- Hoax Busters: <http://hoaxbusters.ciac.org/>
- FreeByte: <http://www.freebyte.com/antivirus/>
- FredCohen & Associates: <http://all.net/>
- Vesselin Bontchev: <http://www.people.frisk-software.com/~bontchev/>
- Eugene H. Spafford: <http://spaf.cerias.purdue.edu>

Course Assignments

The course assignments include multiple quizzes and a couple of homeworks. There will be no programming assignments. The homeworks will typically ask you to research a topic and write a short paper. One homework will include a dissection of a virus code. In addition, there will be a blackboard discussion forum on a specific topic.

Final exam

Because the course is short-term and condensed, there will be no midterm exam. The final exam will consist of 40 multiple-choice/multiple-answer/true-false questions, and will be offered online. All students must take it at the scheduled date and time (because of the time difference, the time of the exam might not be convenient to you). The exam will be open-book, open-notes. It will last 40 minutes. To take the final exam, you do NOT need to have a proctor.

Course Format

The course is organized around the following pattern:

1. You read the assigned material (a chapter in the textbook or a paper)
2. You read the PowerPoint slides corresponding to the chapter.
3. You take an online, open book quiz on the chapter.
4. You do a homework assignment and turn in your answers.

The Course Calendar

The COURSE CALENDAR is very important because it tells you what to do on a day-by-day basis. You are REQUIRED to check that calendar each week day. There may be changes to what is up there from day to day. Read any course announcements first, and then check the COURSE CALENDAR. Most weekdays there will be a calendar entry.

The good thing about online courses is that you have time flexibility: you can work on assignments at different times of the day. This, however, does not mean that you can procrastinate. You have to be on schedule and do all necessary work. Late assignments will receive 0 points.

Most assignments will be due on midnight of a certain day. Remember that it is your responsibility to check the COURSE CALENDAR and the course announcements.

Some of the material in this course can be complicated. If you cannot understand some topic, read the text several times. If necessary, check previous chapters. Read the lecture slides. It usually helps. You have to read the textbook word for word, do not skip. If you still do not understand, then email me with a SPECIFIC question about what you are confused about. Do not write me "I cannot understand Chapter 3 at all" is not a specific question and I cannot answer it.

Checking your email regularly

You should check your UIS email frequently, preferably each week day. UIS sends you official mail at that email address. When I send the class an email using Blackboard, the default email address it uses for you is that official UIS email address. Do not forget to check your course announcements and the course calendar on a day-by-day basis.

Grading

The grading breakdown is the following:

Quizzes	40%
Homeworks	30%
Final exam	30%

F	D	C	B	A
< 60	61-70	71-80	81-90	91-100

Where and When to Turn in Homeworks

Each assignment must be prepared with a word processor. I'll take ASCII text documents (like those prepared with NOTEPAD), MS Word documents, HTML pages, and PDF. Any other formats you should clear with me in advance.

When you prepare your assignments do not try to make them super fancy. The focus is not on the form, but on the content. "Typewriter graphics" are fine. You can scan handwritten diagrams or figures as far as they are readable. Scanned handwritten text is not acceptable. If I cannot read something, I will assume that it is wrong.

Acceptable Use Statement

Since the course covers technologies that can be abused to commit computer crimes, every student must sign and turn in the Acceptable Use Statement. Students whose statements do not arrive by June 13th will be removed from the class. There will be no exceptions.

Plagiarism

All academic work must be your own. Plagiarism, defined as copying or receiving materials from a source or sources and submitting this material as one's own without acknowledging the particular debts to the source (quotations, paraphrases, basic ideas), or otherwise representing the work of another as one's own, is never allowed. Collaboration, usually evidenced by unjustifiable similarity, is never permitted in individual assignments. Any submitted academic work may be subject to screening by software programs designed to detect evidence of plagiarism or collaboration.

Getting outside help on your homework: it is not allowed. Unless it is otherwise stated in an assignment, you are not to get help on your homework from anyone except me (Svet Braynov, your instructor). You also aren't supposed to use email or the web to find someone else's answers to these questions, or to copy material which is posted on the web. If you are using external material, you have to make it clear by explicitly marking the external material and acknowledging the source. Copying material from the web without making it clear is considered cheating

The UIS Academic Integrity Policy (AIP) covers all academic misconduct, but three common violations are cheating, plagiarism, and facilitating violations of academic dishonesty. The UIS AIP is available at: <http://www.uis.edu/academicintegrity/policy/index.html>

"Academic integrity is at the heart of the University's commitment to academic excellence. The UIS community strives to communicate and support clear standards of integrity, so that undergraduate and graduate students can internalize those standards and carry them forward in their personal and professional lives. Living a life with integrity prepares students to assume leadership roles in their communities as well as in their chosen profession. Alumni can be proud of their education and the larger society will benefit from the University's contribution to the development of ethical leaders. Violations of academic integrity demean the violator, degrade the learning process, deflate the meaning of grades, discredit the accomplishments of past and present students, and tarnish the reputation of the University for all its members." (UIS Academic Integrity Policy)

Academic sanctions range from a warning to expulsion from the university, depending on the severity of your violation and your history of violations. Whatever the sanction, I will file a report of academic dishonesty to the Office of the Provost.

If you have any doubts about what is cheating or plagiarism, please contact me before submitting your work.

Any student accused of a violation of academic integrity will receive an F for the course .

No Extra Credit Work

Students sometimes ask for some extra credit work near the end of the semester in an attempt to bring up sagging grades. No extra credit work will be given to any student on an individual basis.

Late Policy

Late homework and missed quizzes will not be accepted, unless the student is ill. If you are traveling, you need the instructor permission for late quiz or homework. If a student misses an exam or a quiz, he/her will receive a zero for that portion of the grade. There are no makeup exams or assignments.

Illness

In the event of an illness or other mishap, get proper documentation (e.g., medical certificate). I accept medical documentation issued by US doctors only.

Students with disability

Reasonable accommodations are available for students who have a documented disability. Please notify the instructor during the first week of class of any accommodations needed for the course. Late notification may cause the requested accommodations to be unavailable. All accommodations must be approved through the Office of Disability Services (ODS) in the Human Resources Building (HRB), Room 80, 217-206-6666.