**The Villanova University**
Master of Science in Cybersecurity
Department of Electrical and Computer Engineering
**ECE 8489**
**Malicious Software Analysis and Defense**
January 12 - April 20, spring 2015

**Instructor**:
Dr. Charles Pak
Email: charles.pak@villanova.edu; charlespak@verizon.net
Email is the best way to contact me. Here is my cell number if needed: (443)610-7986

# General Course Information:

This is a graduate level class. Students are expected to apply time management skills to their work, home, and academic life. Any due dates for materials for these classes are designed to spread the workload over the semester. Material, such as reading assignments, with no due date given should be done as soon as possible by the student so the workload does not become overwhelming prior to the end of course.

# Course Description

Examine malicious software detection and defenses including tripwire, Bit9 and other software techniques (i.e., signature, hash algorithm). Explore Viruses, worms and Trojan horses, logic bombs, malicious CGI scripts, web server scripts or software. Study the anatomy of well-known viruses and worms to understand how they work. Examine mobile code issues as they apply to web and application technologies resulting insecurities. Review the underlying methodologies used by the anti-virus/spyware vendors and freeware offerings to protect electronic assets from harm or other compromise.

Students are reminded that it is a violation of Federal and some states' laws to attempt to gain unauthorized access to information assets or systems belonging to others, or to exceed authorized on systems to which they have been granted access. At no time in this class should any student violate either laws or confidences. Any violation of legal boundaries in the course of this class will be considered a violation of the class trust and will be subject to sanctions in grading.

# Course Objectives

Upon completion of this course, the student will be able to:

- Recognize malicious software
- Analyze different malicious software types
- Examine malicious software detection and defenses
- Explore software protection such as application signature
- Explore viruses, worms, Trojan horses, logic bombs, malicious CGI scripts, and web server attacks.
- Mitigate software vulnerabilities
- Monitor and Manage System Protection

# Required Reading Materials:

## *Books:*

Skoudis E. & Zeltser, L. (2004). "Malware: Fighting Malicious Code".
ISBN-10: 0131014056, ISBN-13: 978013014053, Prentice Hall
Grimes, R.(n.d.) Malicious Mobile Code: Virus Protection for Windows
ISBN: 978-1-56592-682-0 | ISBN 10: 1-56592-682-X

# Method of Instruction

The method of instruction will combine the following elements:
- Online Discussion
- Malicious Software Research Project

# Policy on Paper Submission

Papers are due on the date they are due. Up until midnight of that night, no penalty will accrue. Please note that life emergencies happen. Do NOT wait until the last moment to start on your paper. If you do that and something comes up to impede your progress, it will hamper your ability to turn in your paper on time. Papers MUST be submitted electronically via Blackboard.

All papers must include the following statement:
"This paper or presentation is my own work. Any assistance I received in its preparation is acknowledged within the paper or presentation, in accordance with academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I have cited the sources fully and completely in footnotes and bibliography entries. This includes sources that I have quoted or paraphrased. Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other class in this University or elsewhere, or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer reviewed journal, or professional conference. In adding my name following the word 'Signature', I intend that this certification will have the same authority and authenticity as a document executed with my hand-written signature.

Signature _____"

# Reading Assignments:

The scope of this course is very broad, and a large amount of reading is required. However, the relative importance of materials, as specified in the course outline, varies. Specifically assigned materials must be read in detail. Materials to which students are directed or for which copies are provided but which are not specifically assigned are recommended for added understanding of required material, but are optional in the sense that students will not be held explicitly responsible for anything that appears only in these materials. They are appropriate either for students who have difficulty with the subject matter based on the required readings or for those who want a deeper understanding of the material. Recommended background reading is valuable for overall understanding, may provide a technical depth beyond the requirements of the class, may provide valuable material for student research topics, and may be useful in responding to comprehensive essay questions.

Since much of what is happening in information security is happening now, current events will play a role in class discussions. As professionals, it is crucial for you to keep up with events as they unfold. There is no substitute for regular reading of business and technology news in a major newspaper, for following current journal articles, visiting key web sites, and for noting the direction of industry organizations such as the IEEE, IETF, and the ACM. You should constantly consider how what you read in such sources fits into the subject you are studying. Current articles, including Web articles, may be assigned as supplementary reading as the course progresses.

Students are encouraged to use as many and varied sources as possible in exploring the questions presented during the course, and to share those sources with their classmates. References to sources should be explicit in exchanges among the students and instructor, and will be considered in determining the extent to which each student participated for purposes of awarding grades.

# Grading Policy:

The overall course grade will be established as follows:

| Grading Criteria | Percentage |
|---|---|
| Discussion Participation | 20 |

| | |
|---|---|
| Malicious Software Research Paper | 25 |
| Cyber Vulnerability Analysis Paper | 25 |
| Malware Attacks on Critical Infrastructure Research Paper | 30 |
| **Total** | **100** |

http://www1.villanova.edu/villanova/enroll/registrar/policies.html#question_faq_5

| Letter Grade | Approximate percentage grade range | Grade Points |
|---|---|---|
| A | 95–100 | 4.00 |
| A− | 90 < 95 | 3.67 |
| B+ | 85 < 90 | 3.33 |
| B | 80 < 85 | 3.00 |
| B− | 75 < 80 | 2.67 |
| C+ | 70 < 75 | 2.33 |
| C | 65 < 70 | 2.00 |
| F | < 65 | 0.00 |

# Other Items of Importance

Don't ask for an incomplete for convenience. The University has very specific policy on when a grade of incomplete may be awarded. See the Bulletin for more information on grading policies.

***Writing and Speaking Standards:***

Written communication is an important element of the total communication process. This is a graduate program. **Students are assumed to have learned how to prepare academic papers in their earlier studies, including how to reference works used in preparation of their papers and presentations.** The University recognizes and expects exemplary writing to be the norm for course work. To this end, all papers, individual and group, must demonstrate graduate level writing and comply with and conform to standard academic format as specified in A Manual For Writers of Term Papers, Theses, and Dissertations by Kate L. Turabian, Seventh Edition. Points will be subtracted for format errors. Points will also be subtracted for spelling and grammatical errors. Use of Standard English ensures that your points will be both understood and correctly interpreted by all readers, a skill that will be vital to your success after graduation.

Effective managers, leaders, and teachers are also effective communicators. It is no understatement to say that effective speaking and writing skills are as important to career success as technical mastery of a subject. Speaking and writing effectively are a critical part of this course. Correct and graduate level Standard English must be used.

***Academic integrity*:**

Academic integrity is central to the learning and teaching process. Students are expected to conduct themselves in a manner that will contribute to the maintenance of academic integrity by making all reasonable efforts to prevent the occurrence of academic dishonesty. Academic dishonesty includes, but is not limited to, obtaining or giving aid on an examination, having unauthorized prior knowledge of an examination, doing work for another student, and plagiarism of all types.

Plagiarism is the intentional or unintentional presentation of another person's idea or product as one's own. Plagiarism includes, but is not limited to, the following: copying verbatim all or part of another's written work; using phrases, charts, figures, illustrations, or mathematical or scientific solutions without citing the source; paraphrasing ideas, conclusions, or research without citing the source; and using all or part of a literary plot, poem, film, musical score, or other artistic product without attributing the work to its creator. Students can avoid unintentional plagiarism by following carefully accepted scholarly practices. Notes taken for papers and research projects should accurately record sources of material to be cited, quoted, paraphrased, or summarized, and papers should acknowledge these sources.

## There is no such thing as "boilerplate" in academia.

If you don't understand what plagiarism is and how to avoid it, consult the University's academic integrity policy. See also http://www.prism-magazine.org/december/html/student_plagiarism_in_an_onlin.htm
This is a graduate program. Students are assumed to have learned how to prepare academic papers in their earlier studies, including how to reference works used in preparation of their papers and presentations.

The penalties for plagiarism include a zero or a grade of "F" on the work in question, a grade of "F" in the course, suspension with a file letter, suspension with a transcript notation, or expulsion. Students are not permitted to submit an assignment or paper that already has been submitted for another course at any institution, even if it is entirely their own work. This includes cutting and pasting portions of previous papers or other written assignments. The penalties will be the same as those listed above for plagiarism. Please check your work carefully. Turabian contains complete guidance on how to correctly reference all forms of material.

**There is no such thing as "boilerplate" or "standard language" in academia.** Students are expected to write their reports themselves. If it is necessary to use material from other sources, it is expected (and mandatory) that the standards of academic style and integrity will be followed. Every student is encouraged to visit these websites for interesting information regarding this issue:

- A true story about plagiarism gone awry
http://www.aweekofkindness.com/blog/archives/the_laura_k_krishna_saga/000023.html (May only be available in a Google Cache as Domain expired 2/23/2011).
- Goucher College's "Plagiarism-by-Paraphrase Risk Quiz"
http://faculty.goucher.edu/writingprogram/sgarrett/Default.html
- Copyright law, frequently asked questions, and other good stuff
http://www.copyright.gov/
- The Islam Online.net Fatwa on Plagiarism
http://www.islamonline.net/servlet/Satellite?pagename=IslamOnline-English-Ask_Scholar/FatwaE/FatwaE&cid=1119503549102

**Disabled Students:** Any student who has a disability and is in need of special consideration must inform the instructor of this need within the first week of class (or immediately if the disability appears after the first week of class) so that appropriate arrangements can be made. This includes students with reading or learning disabilities who may require extra time on tests. In all cases, the student must communicate with the Disability Services Center and have registered the disability with the University.

## Discussion Rubric

| Criteria | Non-compliant | Minimal | Compliant | Advanced |
|---|---|---|---|---|
| **One initial major response (minimum 125 words) to first discussion question** | Did not complete this portion of the assignment or most of the discussion points were inappropriate or were not identified. (1) | The discussion points were identified and described but with fair accuracy and some of the discussion points were inappropriate or were not identified. (3) | The discussion points were identified and described with good accuracy and appropriate information was identified and discussed. (6) | The discussion points were identified and described with high accuracy and all appropriate information was identified and discussed clearly. (10) |
| **Writing – grammar, sentence structure, paragraph** | 5 or more different errors in sentence structure, paragraph structure, spelling, punctuation, or APA | 3-4 different errors in sentence structure, paragraph structure, or APA usage. References are | 1-2 different errors in sentence structure, paragraph structure, spelling, punctuation, or APA usage. References | No errors in sentence structure, paragraph structure, spelling, punctuation or APA usage. References are expected. |

| Criteria | Non-compliant | Minimal | Compliant | Advanced |
|---|---|---|---|---|
| **structure, spelling, punctuation (APA required).** | usage. References are expected. (Major issues) (1) | expected. (Many issues) (3) | are expected. (Minor issues) (6) | (Minor issues) (10) |
| **Responding to other students.** | Did not respond to other students or responses were trite with no substance. (1) | Responded to other students but responses were trite with no substance. (3) | Responded to one other student, response was substantive. (6) | Responded to two or more other students, responses were substantive. (10) |
| **Frequency of responses.** | Did not post in the threaded discussion. (1) | Posted one message only 1 day of the week. (3) | Posted more than 1 message but only one day of the week. (6) | Posted on two or more different days of the week. (10) |

# Course Schedule

| Week | Date | Discussion Topic | Assignments Due |
|---|---|---|---|
| 1 | 1/12 | Ch1 – Introduction (Grimes)<br>Ch1- Introduction (Skoudis & Zeltser) | Discussion Participation |
| 2 | 1/19 | Ch2 – DOS Computer Viruses (Grimes)<br>Ch2- Viruses (Skoudis & Zeltser) | Discussion Participation |
| 3 | 1/26 | Ch3 – Windows Technologies (Grimes)<br>Ch3- Worms (Skoudis & Zeltser) | Discussion Participation |
| 4 | 2/2 | Ch4 – Viruses in a Windows World (Grimes)<br>Ch4- Malicious Mobile Code (Skoudis & Zeltser) | Discussion Participation |
| 5 | 2/9 | Ch5 – Macro Viruses (Grimes)<br>Ch5- Backdoors (Skoudis & Zeltser) | Discussion Participation<br>Malware Research Paper Due |
| 6 | 2/16 | Ch6 – Trojans and Worms (Grimes)<br>Ch6- Trojan Horses (Skoudis & Zeltser) | Discussion Participation |
| 7 | 2/23 | Ch7 – Instant Messaging Attacks (Grimes)<br>Ch7- User Mode Rootkits (Skoudis & Zeltser) | Discussion Participation |
| 8 | 3/2 | Ch8 – Internet Browser Technologies (Grimes)<br>Ch8- Kernel Mode Rootkits (Skoudis & Zeltser) | Discussion Participation |
| 9 | 3/9 | Ch9 – Internet Browser Attacks (Grimes)<br>Ch9- Going Deeper (Skoudis & Zeltser) | Discussion Participation |
| 10 | 3/16 | Ch10 – Malicious Java Applets (Grimes)<br>Ch10- Scenarios (Skoudis & Zeltser) | Cyber Vulnerability Analysis Paper |
| 11 | 3/23 | Ch11 – Malicious ActiveX controls (Grimes)<br>Ch11- Malware Analysis (Skoudis & Zeltser) | Discussion Participation |
| 12 | 3/30 | Ch12 – E-mail Attacks (Grimes)<br>Ch12- Conclusion (Skoudis & Zeltser) | Discussion Participation |
| 13 | 4/6 | Ch13 – Hoax Viruses (Grimes)<br>Ch14 – Defense (Grimes) | Discussion Participation |
| 14 | 4/13 | Review | |
| 15 | 4/20 | Final Week | Malware Attacks on Critical Infrastructure Research Paper |

**Malware Research Paper**

The student will research prevalent malicious software and write a paper.

1. Conduct a literature review on the latest malware attacks
2. Synthesize findings on these scholarly papers
3. Draw a conclusion on your findings.

**Cyber Vulnerability Analysis Paper**

The student will research cyber vulnerability scholarly papers and synthesize findings.

1. Conduct a literature review on cyber vulnerability
2. Synthesize findings on these scholarly papers
3. Draw a conclusion on your findings.

**Malware Attacks on Critical Infrastructure Systems Research Paper**

The student will research scholarly journal and conference papers and synthesize them to conclude his/her findings on the current malicious software attacks. The student will:

1. Identify current malicious software attacks.
2. Recommend how to prevent malicious software attacks.
3. Address how to protect national critical infrastructure systems against real-time threats, zero-day attacks, advanced persistent threats (APT), Cyberterrorism and other Cyber-attacks.
4. The paper should be in APA format, double spaced, in a minimum of 10 pages. Please use ACM/IEEE journal and conference papers for references.

**Research Paper Grading Rubric**

| **Criteria** | | | | | |
|---|---|---|---|---|---|
| | **Poor** | **Fair** | **Good** | **Excellent** | **Percent** |
| **Organization** | Sequence of information is difficult to follow. (0 – 7) | Reader has difficulty following work because student jumps around. (8 – 14) | Student presents information in logical sequence which reader can follow. (15 – 22) | Information in logical, interesting sequence which reader can follow. (23 – 30) | 30% |
| **Content Knowledge** | Student does not have grasp of information; student cannot answer questions about subject. (0 – 12) | Student is uncomfortable with content and is able to demonstrate basic concepts. (13 – 24) | Student is at ease with content, but fails to elaborate. (25 – 37) | Student demonstrates full knowledge (more than required). (38 – 50) | 50% |
| **Grammar and Spelling** | Work has significant spelling errors and/or grammatical errors. (0 – 2) | Presentation has several and/or grammatical errors. (3 – 4) | Presentation has a couple misspellings and/or grammatical errors. (5 – 7) | Presentation has no misspellings or grammatical errors. (8 – 10) | 10% |
| **APA Formatting** | Work has significant formatting errors (i.e. references page, title page, spacing, citations). (0 – 2) | Work has several formatting errors (i.e. references page, title page, spacing, citations). (3 – 4) | Work has a few formatting errors (i.e. references page, title page, spacing, citations). (5 – 7) | Work has no formatting errors (i.e. references page, title page, spacing, citations). (8 – 10) | 10% |