Syllabus revised 2011-08-19

Administrative Information
Instructor: Dr. Aleksandar Lazarevich
Email: alazarev@gmu.edu subject=GMU-TCOM/CFRS 661-001_Your name
Phone: 703-393-2247
Office hours: By appointment
Teaching Assistant: TBD
Classes: Thursday, Innovation 320, 4:30 pm – 7:10 pm

Course Description

CFRS 780 - Advanced Topics in Computer Forensics – Counter Forensics (3:3:0)
Prerequisites: TCOM 548 and TCOM 556 or TCOM 562; a working knowledge of computer operating systems (e.g. CS 471 or equivalent) or permission from instructor. Teaches advanced topics from recent developments and applications in various areas of computer forensics. The advanced topics are chosen in such a way that they do not duplicate existing CFRS courses. Active participation of the students is encouraged in the form of writing and presenting papers in various research areas of the advanced topic. The course is designed to enhance the professional engineering community’s understanding of breakthrough developments in specific areas of computer forensics.

Textbooks
None

Potential topics
1. Digital Media wiping
2. Stegonography
3. Rootkits
4. Encryption
5. Metadata manipulation
6. S.M.A.R.T. manipulation
7. Audit/Log manipulation
8. Slack space manipulation
9. Secure Digest Collision generation
10. Memory manipulation
11. Misleading evidence
12. Forensic tool vulnerabilities
13. Obfuscation
14. Anonymizing
15. Flushable devices
16. Network manipulation

Grading
Grades will be assessed on the following components:
Research Papers (4@20% each) 80%
Class Presentation 20%
These components are outlined in the following sections.

**Research Papers**

Each student will prepare four research papers in APA format addressing a technique or tool used in counter/anti-forensics. They will be 7-10 pages in length with no less than 4 references. No more than 25% of the paper may be quotes. Papers will be randomly chosen for discussion in class.

Papers will be due in Weeks 5, 8, 11, and 15. Late reports will be assessed a penalty of 25% of the assignment grade for each week or part thereof it is late.

**Presentation**

Each student will select one of their research papers to present to the class in a one hour presentation that will include leading a discussion and a question and answer session. A soft copy of the PowerPoint (.ppt) file will be submitted prior to the presentation.

<table>
<thead>
<tr>
<th>Schedule</th>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
<th>Reading Assignments</th>
<th>Projects Due</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Week 1</td>
<td>9/1/2011</td>
<td>Introduction and overview of counter forensics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Week 3</td>
<td>9/14/2011</td>
<td>Review of digital media forensics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Week 4</td>
<td>9/21/2011</td>
<td>Counter forensic techniques</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Week 5</td>
<td>9/28/2011</td>
<td>Counter forensic tools</td>
<td></td>
<td>Paper 1 due</td>
</tr>
<tr>
<td></td>
<td>Week 6</td>
<td>10/5/2011</td>
<td>Student Presentations and paper discussions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Week 7</td>
<td>10/12/2011</td>
<td>Student Presentations and paper discussions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Week 8</td>
<td>10/19/2011</td>
<td>Student Presentations and paper discussions</td>
<td></td>
<td>Paper 2 due</td>
</tr>
<tr>
<td></td>
<td>Week 9</td>
<td>10/26/2011</td>
<td>Student Presentations and paper discussions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Week 10</td>
<td>11/2/2011</td>
<td>Student Presentations and paper discussions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Week 11</td>
<td>11/9/2011</td>
<td>Student Presentations and paper discussions</td>
<td></td>
<td>Paper 3 due</td>
</tr>
<tr>
<td></td>
<td>Week 12</td>
<td>11/16/2011</td>
<td>Student Presentations and paper discussions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Week 13</td>
<td>11/23/2011</td>
<td>Thanksgiving</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Week 14</td>
<td>11/30/2011</td>
<td>Student Presentations and paper discussions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Week 15</td>
<td>12/7/2011</td>
<td>Student Presentations and paper discussions</td>
<td></td>
<td>Paper 4 due</td>
</tr>
<tr>
<td></td>
<td>Week 16</td>
<td>12/14/2011</td>
<td>Student Presentations and paper discussions</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*This schedule is subject to revision before and throughout the course.*

Call 703-993-1000 for recorded information on campus closings (e.g. due to weather).
Important Dates

<table>
<thead>
<tr>
<th>Important Date</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last day to add classes</td>
<td>Tue. SEP 6</td>
</tr>
<tr>
<td>Last day to drop with no tuition liability</td>
<td>Tue. SEP 6</td>
</tr>
<tr>
<td>Last day to drop (33% penalty)</td>
<td>Mon. SEP 19</td>
</tr>
<tr>
<td>Last day to drop (67% penalty)</td>
<td>Fri. SEP 30</td>
</tr>
</tbody>
</table>

From [http://registrar.gmu.edu/calendars/2011Fall.html](http://registrar.gmu.edu/calendars/2011Fall.html)
See that Web page for more information.

**Attendance Policy**

Students are expected to attend each class, to complete any required preparatory work (including assigned reading) and to participate actively in lectures, discussions and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.

Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor if they miss any class without prior notice.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam may result in a grade of zero (0) for that exam.

**Communications**

Communication on issues relating to the individual student should be conducted using email or telephone. Email is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. Email messages from the Instructor to all class members will be sent to students' GMU email addresses – if you use another email account as your primary address, you should forward your GMU email to that account.

Lecture slides are complements to the lecture process, not substitutes for it - access to lecture slides will be provided as a courtesy to students provided acceptable attendance is maintained.

**Honor Code**

Students are required to be familiar and comply with the requirements of the [GMU Honor Code](http://example.com).

The Honor Code will be strictly enforced in this course.

All assessable work is to be completed by the individual student.

Students must **NOT** collaborate on the project reports or presentation without explicit prior permission from the Instructor.
Available at [http://catalog.gmu.edu/content.php?catoid=5&navoid=410#Honor](http://catalog.gmu.edu/content.php?catoid=5&navoid=410#Honor) and related GMU Web pages.