REQUEST FOR ADDITION OF NEW COURSE

Computer Science & Engineering

September 22, 2017

PROPOSED COURSE DESCRIPTION

Rubric & No. 4360

Title Malware Analysis and Reverse Engineering

Short Title (≤ 19 characters) M A L W A R E A N A L Y S E S

Semester Hours of Credit 3 credit hours

If combination course type, # hrs. of credit for

Repeat Credit Max. (if repeatable): credit hours Graduate Credit? Yes No

Credit will not be given for this course and:

Course Type (Indicate hours in the appropriate course type.)

Lecture Lab Seminar Recitation Lec/Rec Lec/Sem Lec/Lab Res/Ind Clin/Pract Intern

Maximum enrollment per section: (use integer, e.g. 25 not 20-30) 30

Grading System: Letter Grade Pass/Fail Final Exam: Yes _ No _

*(Attach justification if the proposed course will not hold a final exam during examination week.)*

Course Description:
(Concise catalog statement exactly as you wish it to appear in the General Catalog)

CSC 4360 Malware Analysis and Reverse Engineering (3)
Prereq.: CSC 4103 or equivalent. Legal and ethical issues; categorization of malware; static methods for malware analysis and reverse engineering, including disassembly and decompilation; dynamic analysis strategies including debugging, sandboxes, and binary instrumentation; circumvention of obfuscation and anti-analysis techniques.

BUDGET IMPACT (IF ANSWER TO ANY QUESTION IS "YES", ATTACH EXPLANATION).

If this course is approved, will additional staff be needed? Yes No X

Will additional space, equipment, special library materials or other major expense be involved? Yes No X

Academic Affairs Approval: (Date)

ATTACHMENTS (ATTACH THE FOLLOWING TO YOUR PROPOSAL)

JUSTIFICATION: Justification must explain why this course is needed and how it fits into the curricula. Will the course duplicate other courses?
SYLLABUS: Including 14 week outline of the subject matter; titles of text, lab manual, and/or required readings; grading scale and criteria
(For 4000-level, specify graduate student grading criteria if requirements differ for graduate and undergraduate students).

APPROVALS

Department Faculty Approval Date Feb. 24, 2017

Department Chair Signature (date) 10/31/2017

Graduate Dean Signature (date) 11/10/18

Coretta Douglas douglas@csc.lsu.edu

College Contact E-mail

College Faculty Approval Date 1/1/17

College Dean Signature (date) 1/11/17

Chair, FS C&C Committee (date) 1/18/17

Academic Affairs Approval (date) 1/12/18

Re'd 11/10/18

Revised Approval (date)
It was approved. I will check with Matt and get his approval as well as Dean Masse.

Thank you!

Andrea B. Abad
Academic Officer for Curricula and Course Management
Office of the University Registrar
Louisiana State University
112 Thomas Boyd Hall,
Office 225-578-4111
abode@lsu.edu | lsu.edu | lsu.edu/registrar

From: John B Hopkins
Sent: Tuesday, January 09, 2018 12:09 PM
To: Andrea B Abad
Subject: Re: CSC 4360 - Proposal Incorrectly Marked

Andrea

Has the original proposal been approved and signed off by Matt Lee? If so I don’t think its right to make a change at this point without his advanced approval. Please contact Anna and ask Matt if he is OK with us making this change.

If Matt Lee agrees, go ahead and make the change get graduate school approval and have AA initial the change.

john hopkins

From: Andrea B Abad
Sent: Monday, January 8, 2018 9:29 AM
To: John B Hopkins
Subject: CSC 4360 - Proposal Incorrectly Marked

Dr. Hopkins,
The attached proposal was submitted for CSC 4360. The department has informed me that they mistakenly marked this course as not for graduate credit but that is incorrect.

Based on the syllabus provided, is this acceptable or do they need to change the proposal and would this need to be returned to the committee to be reviewed again as a graduate level course? If it is acceptable, I will make the change and send it to the Graduate School for their approval.

Please let me know as soon as possible what they should do. They are hoping to teach this course this semester.

Thanks in advance,

Andrea B. Abad
Academic Officer for Curricula and Course Management
Office of the University Registrar
Louisiana State University
112 Thomas Boyd Hall,
office 225-578-4111
abode@lsu.edu | lsu.edu | lsu.edu/registrar
CSC 4360 Malware Analysis (3)

Prereq.: CSC 4103 or equivalent. Legal and ethical issues; categorization of malware; static methods for malware analysis and reverse engineering, including disassembly and decompilation; dynamic analysis strategies including debugging, sandboxes, and binary instrumentation; circumvention of obfuscation and anti-analysis techniques.

Justification:
Software reverse engineering is a critical area in cybersecurity, with applications in software patch verification, software interoperability, the analysis of malicious software, and cyberwarfare. Furthermore, reverse engineering skills are now routinely required in digital forensics investigation and incident response. There is a huge shortage not only in the US but also internationally of cybersecurity professionals with reverse engineering skills. Notably, the most prestigious NSA/DHS academic designations (e.g., Center of Academic Excellence in Cyber Operations or CAE-CO) require a malware reverse engineering course in a designated university's curricula.
CSC 4360
The Courses and Curriculum (C&C) Committee of the Division of Computer Science and Engineering (CSE), is currently discussing various approaches toward formalizing a curricula focus in cybersecurity. With the expected hiring of a CSE professor in the research area (interviews Spring 2018), we anticipate developing additional undergraduate courses related to the area. CSC 2700 Special Topics "Introduction to Cybersecurity" will be targeted as the 2nd undergraduate course offering to be refined and proposed for the catalog. Most prominent in the discussion has been the creation of a 5th concentration, "Cybersecurity"; initially, CSC 4360 will be required in the concentration as well as the 2000-level introductory course. Our timeline is for proposal in the catalog early fall 2018 for inclusion in the 2018-2019 catalog.

Cybersecurity is a critical area in technology development and software engineering. Breeches in security may have devastating results. Our Industry Advisory Council has strongly urged continued and increased emphasis on the topic. Students attending the recent Kick-off sessions demonstrate a marked increased interest in cybersecurity; the course offering is important toward recruitment and retention of our majors.
SYLLABUS

CSC 4360 Malware Analysis and Reverse Engineering

Catalog Description:
CSC 4360 Malware Analysis and Reverse Engineering (3 credit hours) Legal and ethical issues; categorization of malware; static methods for malware analysis and reverse engineering, including disassembly and decompilation; dynamic analysis strategies including debugging, sandboxes, and binary instrumentation; circumvention of obfuscation and anti-analysis techniques.

Prerequisites: CSC 4103 or equivalent course in operating systems. experience with assembler language is helpful.

Course Coordinator: Prof. Golden G. Richard III; golden@csc.isu.edu
Office Location: DMC 2020
Office Hours: Spring 2017: M 1:15-2:45, W 10-11:30a or by appt

Learning Objectives:

1. Have a firm understanding of the legal and ethical issues surrounding reverse engineering efforts
2. Understand the primary motivations for reverse engineering
3. Be familiar with the basic architectures of both historical and modern malware
4. Have a deep understanding of static and dynamic analysis techniques commonly employed to reverse engineer and understand malware
5. Thoroughly understand modern anti-analysis techniques and how to circumvent them
6. Be able to independently reverse engineer malware samples using state-of-the-art tools

Reference Text:

Suggested Reading:
Twitter: #dfir, #reverseengineering, #infosec; papers from reverse engineering/malware analysis conferences.

Software:

IDA Pro: https://www.hex-rays.com/products/ida/
Hopper: https://www.hopperapp.com/
Grading Scheme:

<table>
<thead>
<tr>
<th>Total Percentage Points:</th>
<th>Final Grading Scale:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Midterm:</td>
<td>A+ (98 and above)</td>
</tr>
<tr>
<td>35%</td>
<td>A (94% and above but &lt; 98%)</td>
</tr>
<tr>
<td>Reverse Engineering Assignments:</td>
<td>A (90% and above but &lt; 94%)</td>
</tr>
<tr>
<td>30%</td>
<td>B+ (87% and above but &lt; 90%)</td>
</tr>
<tr>
<td>Final Exam:</td>
<td>B (84% and above but &lt; 87%)</td>
</tr>
<tr>
<td>35%</td>
<td>B- (79% and above but &lt; 84%)</td>
</tr>
<tr>
<td></td>
<td>C+ (77% and above by &lt; 79%)</td>
</tr>
<tr>
<td></td>
<td>C (71% and above but &lt; 77%)</td>
</tr>
<tr>
<td></td>
<td>C- (68% and above but &lt; 71%)</td>
</tr>
<tr>
<td></td>
<td>D+ (65% and above but &lt; 68%)</td>
</tr>
<tr>
<td></td>
<td>D (62% and above but &lt; 65%)</td>
</tr>
<tr>
<td></td>
<td>D- (58% and above but &lt; 62%)</td>
</tr>
<tr>
<td></td>
<td>F (&lt; 58%)</td>
</tr>
</tbody>
</table>

Assignments:

This class involves a number of reverse engineering efforts, targeting both historical and modern malware. These assignments involve a combination of static and dynamic analysis strategies, to deobfuscate and fully document malware samples. Some of the classical malware samples that are provided for analysis include Michelangelo, SQL Slammer, Lucius, and others. Generally, students start with a binary malware sample and then perform a full reverse engineering effort, with the end product being a report containing full documentation of the sample's code and data.

Class Policy:
- All submitted work for grading is the work of each student, except when teams are explicitly allowed (e.g., for the semester project).
- Due dates are indicated on the assignment.
- Missed deadlines or tests are handled on an individual basis with the approval of the Dean’s Office.
- All problems with grading must be resolved within 3 class days of returning the work.
- If class is missed, detailed notes and class content must be acquired from a classmate.

Student Class Participation:
The class meets for a total of 3 hours per week, which constitutes a 3 hour credit course. While notes and reference materials may be posted via Moodle, the class is not designed to be online and students are expected to attend class. Absences should be rare and exceptional. Students are expected to have read the assigned chapters or supplementary reading materials prior to class and to participate in class discussions and think critically about the concepts addressed. Students should expect to spend at least six to eight hours outside of class each week reading and doing reverse engineering assignments.

LSU Student Code of Conduct:
The LSU Student Code of Conduct explains student rights, excused absences, and what is expected of student behavior. Students are expected to understand this code as described here: [http://students.lsu.edu/saa/students/code](http://students.lsu.edu/saa/students/code)

Any violations of the LSU Student Code will be duly reported to the Dean of Students.

Disabilities:
Louisiana State University is committed to providing reasonable accommodations for all persons with disabilities. If you have a disability that may have some impact on your work in this class and for which you may require accommodations, please see a staff member in Disability Services so that such accommodations can be considered. Students that receive accommodation letters, please meet with me to discuss the provisions of those accommodations as soon as possible.
**Major Topics and Schedule:**

- **Week # 1:**
  - Introduction to reverse engineering
  - Why is reverse engineering useful?
    - Interoperability
    - Security auditing
    - DRM
    - Analysis of malware
  - Legal Issues
    - Under what circumstances is reverse engineering legal?
    - When isn't reverse engineering legal?
  - Overview of important foundational knowledge
    - Important assembler languages
    - Popular programming languages for malware development
    - Operating systems internals
    - Hardware

- **Week # 2:**
  - Historical malware
  - MS-DOS malware case studies

- **Week # 3**
  - Overview of modern malicious software
    - Viruses
    - Worms
    - Trojans
    - Ransomware
    - Botnets

- **Week # 4:**
  - Polymorphic and metamorphic malware
  - Malware detection
    - Worm fingerprinting / signature generation
    - Behavioral approaches for detection of malware
    - Hardware agents for system integrity checking

- **Week # 5:**
  - Low level software
    - Compilation toolchains and impacts on reverse engineering
    - Representation of compiled high level language structures in assembler
    - Virtual machines for interpreted high-level languages

- **Week # 6:**
  - Static and dynamic reverse engineering techniques
    - System monitoring tools
    - System call, filesystem, and registry tracing
    - Debuggers
    - Disassemblers
    - Decompilers

- **Week # 7:**
  - Worm case study
    - Infection vectors
    - Target selection
    - Propagation
• Week # 8:
  o Executable file formats
    ▪ Portable Executable (PE) format
    ▪ ELF
    ▪ Mach-O

• Week # 9:
  o Encrypted virus case study
    ▪ Infection vector and propagation
    ▪ Obfuscation strategies
    ▪ Unpacking
    ▪ Effects

• Week # 10:
  o Advanced code obfuscation techniques
    ▪ Control flow obfuscation
    ▪ Opaque predicates
    ▪ Arithmetic obfuscation

• Week # 11:
  o Encrypted and packed executables
    ▪ Identifying packed executables
    ▪ Packing strategies
    ▪ Unpacking

• Week # 12:
  o Anti-debugging techniques
    ▪ Debugger detection
    ▪ Strategies for blocking debugger access

• Week # 13:
  o Anti-VM techniques
    ▪ Types of virtualization
    ▪ Detection of virtualization
    ▪ Exploiting runtime differences in physical vs. virtualized hardware

• Week # 14:
  o Memory forensics and reverse engineering
    ▪ Memory acquisition
    ▪ Malware detection using memory forensics
    ▪ Dumping process memory for analysis