CS 373 – Defense Against the Dark Arts

Credits: This course combines approximately 120 hours of instruction and programming work for 4 credits.

Terms Offered: Winter (On-campus and Ecampus)

Structure: Two 80-minute lectures per week
Note: Due to extensive programming assignments, this course has an implied, non-scheduled lab. The lab takes place on the students’ own times, and is not part of the official course schedule.

Instructor: Kevin McGrath

Prerequisites: CS344, CS340, CS372, knowledge of C

Courses that require this as a prerequisite: None

Catalog Description: Introduction to the current state of the art in anti-malware, computer forensics, and networking, messaging, and web security. Broad introduction to the field of computer security.

Course Content:
This course will cover multiple topics. These topics include, but are not limited to:
- Malware
- Forensics, methods and tools
- Malware defenses
- Vulnerabilities and exploits
- Windows kernel structures, drivers, and malware
- Network Security, methods and tools
- Web security, methods and tools
- Messaging security, methods and tools
- Mobile Security, methods and tools

Course-specific Measurable Student Learning Outcomes:
On completion of the course, students will have demonstrated the ability to:
1. Apply security knowledge to real world projects.
2. Demonstrate awareness of the current state of malware, adware, and crypto-ware.
3. Implement solutions to common attack vectors in multiple environments.
4. Implement spam identification tools.
5. Explain the nature and methods of rootkits.

Evaluation of Student Performance:
This is a very hands-on course, with weekly hands-on lab assignments. These labs make up the bulk of the grade, with a final project making up the remainder.

- Weekly labs and write-ups: 60%

August 5, 2016
- Final project: paper and presentation: 40%.

<table>
<thead>
<tr>
<th>%</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>93-100</td>
<td>A</td>
</tr>
<tr>
<td>90-92</td>
<td>A-</td>
</tr>
<tr>
<td>87-89</td>
<td>B+</td>
</tr>
<tr>
<td>83-86</td>
<td>B</td>
</tr>
<tr>
<td>80-82</td>
<td>B-</td>
</tr>
<tr>
<td>77-79</td>
<td>C+</td>
</tr>
<tr>
<td>73-76</td>
<td>C</td>
</tr>
<tr>
<td>70-72</td>
<td>C-</td>
</tr>
<tr>
<td>67-69</td>
<td>D+</td>
</tr>
<tr>
<td>63-66</td>
<td>D</td>
</tr>
<tr>
<td>60-62</td>
<td>D-</td>
</tr>
<tr>
<td>Below 60</td>
<td>F</td>
</tr>
</tbody>
</table>

**Learning Resources:**
This course covers a large number of topics, serving as an introduction to broad field of computer security. As such, a large number of books will be referenced and recommended:


**Students with Disabilities:**
Accommodations for students with disabilities are determined and approved by Disability Access Services (DAS). If you, as a student, believe you are eligible for accommodations but have not obtained approval please contact DAS immediately at 541-737-4098 or at [http://ds.oregonstate.edu](http://ds.oregonstate.edu). DAS notifies students and faculty members of approved academic
accommodations and coordinates implementation of those accommodations. While not required, students and faculty members are encouraged to discuss details of the implementation of individual accommodations.

**Link to Statement of Expectations for Student Conduct**, i.e., cheating policies
http://studentlife.oregonstate.edu/studentconduct/offenses-0