​​​​​​​​​​**CpS 391 - Computer Security Fundamentals**

Fall 2020

|  |  |  |
| --- | --- | --- |
| C:\Users\ahughes\Desktop\Dr. Alan Hughes.jpg  ​Instructor: Dr. Alan Hughes | **Instructor:** | Dr. Alan Hughes |
| **Office:** | AL76  Alternatively, CS Lab (Mack Library, 2nd floor) |
| **Office Hours:** | M-F 10am electronic; or in person in CS Lab by appointment |
| **Email:** | [ahughes@bju.edu](mailto:ahughes@bju.edu) |
| **Telephone:** | Cell: 864-906-1024  Office: 86-242-4100 x​2274  ​ |

**Course Description:**

Introduction to computer security concepts, principles and practices, including but not limited to: authorization, attacks and attack prevention, infrastructure security, cryptography, controls, plans and procedures.

**Course Reading(s):**

Security+ Guide to Network Security Fundamentals, **6th** edition, Mark Ciampa, 2017, ISBN9781337289306.

**CompTIA Security+ Guide to Network Security Fundamentals, Lab Manual, 6th Edition,** Andrew J. Hurd, ISBN-13: 9781337288798

Other readings as assigned.

**Context:**

The faculty of the Computer Science department has aligned the computer science program with the goals of the Mathematical Sciences Division, the BJU Bible and liberal arts core objectives, and the BJU institutional goals. The goal of the Computer Science department is to align all courses in the Computer Science and Information Technology majors to support one or more of the following departmental goals. An asterisk indicates a specific goal fulfilled by this course.

1. Design and implement solutions to practical problems. \*
2. Demonstrate an ability to work effectively in teams. \*
3. Demonstrate an ability to communicate technological information effectively both in written and oral forms. \*
4. Demonstrate an ability to acquire new knowledge in the computing discipline. \*
5. Demonstrate an understanding of social, professional and ethical considerations related to computing. \*
6. Demonstrate understanding of fundamental concepts in the discipline. \*
7. Prepare students for graduate school or to secure employment in a related area. \*

**Course Goals:**

1. Design and implement solutions to practical problems.
2. Demonstrate an ability to work effectively in teams.
3. Demonstrate an ability to communicate technological information effectively both in written and oral forms.
4. Demonstrate an ability to acquire new knowledge in the computing discipline.
5. Demonstrate understanding of fundamental concepts in the student's discipline.
6. Provide the student a platform for continued learning and development of his God-given abilities.
7. Instill in the student a desire to use his abilities in service to Christ.

**Learning Objectives:**

At the end of the course, students should be able to:​

|  |  |
| --- | --- |
| **Learning Objectiv​e** | **Assessment Tools​** |
| 1. Understand the major issues in information security, including malicious software threats, intrusion detection and prevention, and social engineering. | Writing Assignments, Quizzes, Tests |
| 2. Understand the common attacks on computer networks, and the methods used to detect and prevent those attacks. | Writing Assignments, Quizzes, Tests |
| 3. Understand the basic principles of information system security. | Writing Assignments, Quizzes, Tests |
| 4. Evaluate and articulate information security procedures and practices. | Writing Assignments, Quizzes |
| 5. Design and implement information security procedures and practices. | Writing Assignments and Lab Projects, Quizzes, Tests |
| 6. Understand the major points of an information security policy and how they apply to a particular business. | Writing Assignments (security policy development), Quizzes, Tests |

​​**Course Policies:**

**Qualifications**

CpS 110 is a pre-requisite for CpS 391.  (Non-IT majors, see or email Dr. Hughes for pre-requisite waivers)

**Absences, lateness, and makeup opportunities**

1. The overarching guide for class attendance is the [BJU Class Attendance Policy](http://home.bju.edu/life/policies/class-attendance-policy.php).
2. For planned absences, please email me one week in advance.
3. Written assignments should be submitted before your planned absence.
4. Scheduled tests and quizzes should be taken before your planned absence; please contact me to make arrangements for doing so.
5. For absences due to incapacitating illness or emergency, you should contact me as soon as you are able to return to class in order to make arrangements for making up any graded work without penalty.
6. In other circumstances, tests and quizzes may be made up within one week of your return, with a 10 percent grade penalty for that test or quiz.
7. Leaving class early without prior arrangement will constitute an absence.

**Late Work**

1. Assignments must be submitted using the electronic submission system before midnight on the day due.
2. The use of the submission system will be explained during the first week of class.
3. Only work missed for legitimate reasons may be made up without penalty. Legitimate reasons include illness, a death in the family, or a BJU sanctioned tour.
4. You must make up late work according to the number of days missed - that is, missing one day of class gives you one extra day to turn in your work.
5. Any other late work will receive a 20% grade penalty.
6. All late work must be made up within one week in order to receive a non-zero grade.

**Grade appeals**

1. Grading appeals must be made by email only no later than one week after the grade was assigned.
2. Appeals will be automatically denied if the student attempts to make the appeal verbally.
3. Email grading appeals should be made respectfully and logically ("My grade should be increased because.....").

**Academic Integrity**

1. The overarching guide for academic integrity is the [BJU Academic Integrity Policy](http://home.bju.edu/academics/integrity.pdf).
2. Cheating on assignments and tests is a form of deception and stealing, and as such, is prohibited   
   by Scripture and will incur academic penalties.
3. All work is to be done individually unless Mr. Hughes gives permission for group work.
4. In general students are encouraged to assist one another in the lab environment, *but must exercise care when seeking assistance while completing labs*.
5. **The goal is for each student to become familiar with information security, and be able to work effectively on his or her own. Therefore, please do not copy work from another person, as this constitutes cheating.**

**Class Participation**

1. Compliance with student handbook policies, including the dress code, is expected during class.
2. Class participation grades are based upon actively participating in lecture class discussions, working diligently on course assignments in lab classes and being respectful to the rest of the class and the instructor.
3. Class participation grade will include in-class assignments throughout the semester that will be individually graded.
4. Playing games, electronic messages, working on other subjects, etc. is a demonstration of disrespect for both the instructor and other students, and is not allowed during lecture and lab classes.
5. Professional dress required for any presentations.

**Instructor Help outside of class**

You are encouraged to use **email** or the telephone to ask Dr. Hughes for assistance.

**Copyright Policy**

Copyright 2009-2020, Alan Hughes, as to this syllabus and all lectures. Students are prohibited from selling (or being paid for taking) notes during the course to, or by any person, or commercial firm without the express written permission of the professor teaching the course.​

**COVID Disclaimer**

In the event of a COVID outbreak, or other significant event, appropriate changes will be made to the course to facilitate finishing the semester. Students will be apprised in a timely manner should such an event occur.

**Schedule** (may be modified as needed during semester)

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Day** | **Class** | **Assignment** **Due** |
| **Week 1** |  |  |  |
| Aug 19 | W | Introduction and Syllabus; BJU Online; Introduction to Security – Chapter 1 | Chapter 1; Review Syllabus |
| Aug 21 | F | Chapter 1 – Intro to Security | Chapter 1; Quiz 1 (Sat) |
| **Week 2** |  |  |  |
| Aug 24 | M | Chapter 2 - Malware and Social Engineering Attacks | Read Chapter 2; Lab 1 |
| Aug 26 | W | Chapter 2 - Malware and Social Engineering Attacks |  |
| Aug 28 | F | Chapter 2 - Malware and Social Engineering Attacks | Lab 1; Quiz 2 (Sat) |
| **Week 3** |  |  |  |
| Aug 31 | M | Chapter 3 - Basic Cryptography | Chapter 3; Lab 2 |
| Sep 2 | W | Chapter 3 - Basic Cryptography |  |
| Sep 4 | F | Chapter 3 - Basic Cryptography | Quiz 3 (Sat) |
| **Week 4** |  |  |  |
| Sep 7 | M | Chapter 5 - Network Attacks | Chapter 5; Lab 3 |
| Sep 9 | W | Chapter 5 – Network Attacks |  |
| Sep 11 | F | Chapter 5 – Network Attacks | Quiz 4 (Sat) |
| **Week 5** |  |  |  |
| Sep 14 | M | Chapter 6 – Network Security Devices, Design, Technology | Read Chapter 6; Lab 4 |
| Sep 16 | W | Chapter 6 – Network Security Devices, Design, Technology |  |
| Sep 18 | F | Chapter 6 – Network Security Devices, Design, Technology | Quiz 5 (Sat) |
| **Week 6** |  |  |  |
| Sep 21 | M | **Test 1 - Ch 1-3,5,6; work on Security Policy** | **Test 1;** Read Chapter 7; Lab 5 |
| Sep 23 | W | Chapter 7 - Administering a Secure Network |  |
| Sep 25 | F | Chapter 7 - Administering a Secure Network | Quiz 6 (Sat) |
| **Week 7** |  |  |  |
| Sep 28 | M | Chapter 8 – Wireless Network Security | Read Chapter 8; Lab 6 |
| Sep 30 | W | Chapter 8 – Wireless Network Security |  |
| Oct 2 | F | Chapter 8 – Wireless Network Security | Quiz 7 (Sat) |
| **Week 8** |  |  |  |
| Oct 5 | M | Chapter 9 – Client and Application Security | Read Chapter 9; Lab 7 |
| Oct 7 | W | Chapter 9 – Client and Application Security |  |
| Oct 9 | F | Chapter 9 – Client and Application Security | Quiz 8 (Sat) |
| **Week 9** |  |  |  |
| Oct 12 | M | Chapter 10 - Mobile and Embedded Device Security | Read Chapter 10; Lab 8 |
| Oct 14 | W | Chapter 10 - Mobile and Embedded Device Security | All your devices can be hacked video |
| Oct 16 | F | Chapter 10 - Mobile and Embedded Device Security | Quiz 9 (Sat) |
| **Week 10** |  |  |  |
| Oct 19 | M | Chapter 11-12 – Authentication, Account, Access Management | Read Chapter 11-12; Lab 9 |
| Oct 21 | W | Chapter 11-12 – Authentication, Account, Access Management |  |
| Oct 23 | F | Chapter 11-12 – Authentication, Account, Access Management | Quiz 10 (Sat) |
| **Week 11** |  |  |  |
| Oct 26 | M | Chapter 13 – Vulnerability Assessment and Data Security | Read Chapter 13; Lab 10 |
| Oct 28 | W | Chapter 13 – Vulnerability Assessment and Data Security | Read Chapter 13 |
| Oct 30 | F | Data Center Visit | ISACA discussion; Quiz 11 (Sat) |
| **Week 12** |  |  |  |
| Nov 2 | M | **Test 2 – Ch 7-12; work on security policy** | **Test 2 (Ch 7-12);** Read Chapter 14-15; Lab 11 |
| Nov 4 | W | Chapter 14 – Business Continuity | DRII |
| Nov 6 | F | Chapter 14 – Business Continuity | Quiz 12 (Sat) |
| **Week 13** |  |  |  |
| Nov 9 | M | Chapter 15 - Risk Mitigation | Quiz 13 |
| Nov 11 | W | Group work – Risk Mitigation Presentation |  |
| Nov 13 | F | Group work – Risk Mitigation Presentation | Quiz 14 (Sat) |
| **Week 14** |  |  |  |
| Nov 16 | M | Presentations | **Lab 12 9am (before class starts all presentations must be turned in (or counted late)).** |
| Nov 18 | W | **Day of Rest** |  |
| Nov 20 | F | Presentations | **Information Security Policy, with Biblical Principles of Security component** |
| **Exam Week** |  |  |  |
| Nov 21 | Sat | 8-9:10am- **Final Exam**  **Note:** If you pass the CompTIA Security+ certification exam before the final, you are exempt from taking it (given that you have done all the other required work for the course with good quality (B- or better)). | Chapters 13-15 |

**Grading​**

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Item** | **Pts.** | **Total** |
| 14 | Quizzes | 40 | 520 |
| 12 | Labs | 30 | 360 |
| 2 | Tests | 100 | 200 |
| 1 | Final Exam | 120 | 120 |
| 1 | Completed Security Policy | 100 | 100 |
| ​1 | ​Biblical Principles of Security Paper | ​100 | 100 |
| 1 | Risk Presentation (team) | 100 | 100 |
| 1 | Class Participation | 100 | 100 |
| ​ | **TOTAL** | ​ | 1600 |

**Grading Scale**

|  |  |
| --- | --- |
| A | 90-100 |
| B | 80-89 |
| C | 70-79 |
| D | 60-69 |
| F | < 60​​ |

