

BA 632 INFORMATION SYSTEMS SECURITY

Instructor Information

Instructor: Prof. Khaled Falah

Websites: <http://cu.learninghouse.com/> – online class website

E-mail: kyfalah@campbellsville.edu - (All official email will be to/from this address)

Phone: (202) 509-6932 – Cell –

Office Hours: 6-10PM ET Daily

Course Information

Online Course

Textbook

Principles of Computer Security, Conklin and White, 4th Edition, McGraw-Hill Companies, 2016; ISBN: 978-0-07-183597-8.

Course Description

This course covers the common body of knowledge, skills, techniques, and tools in the domain of information technology security. Topics include threat management, risk diagnosis, accountability, security frameworks, enterprise security policy, encryption, wireless security, legal, and ethical issues.

Learning Outcomes

1. Recognize the management of common information security concerns.
(Assessed using quizzes, discussion, project, and individual assignments)
2. Illustrate and discuss the threats, risks, and assessments for an organization's information security program.
(Assessed using quizzes, discussion, project, and individual assignments)
3. Assess information security needs and policies.
(Assessed using quizzes, discussion, project, and individual assignments)
4. Analyze the tradeoffs between security and system functionality.
(Assessed using quizzes and individual assignments)
5. Examine the ethical and legal obligations related to information.
(Assessed using quizzes, discussion, project, and individual assignments)
6. Assess the need for disaster recovery and business continuity.
(Assessed using quizzes and assignments)

Maps to CompTia Security+ Exam SY0-401

By studying this textbook, students will be better prepared to take and pass the CompTIA Security+ Certification Exam. See Appendix A and B for more information. The textbook includes a CD which contains Practice Exam Software, a PDF copy of the textbook, and technical support information.

Style for Writing

Use the APA format for papers, etc. Use spell check, grammar check, etc., to make sure that your papers are submitted in professional form with no keyboarding or grammatical errors.

Resource: *Publication Manual of the American Psychological Association*. 6th edition. ISBN 13: 978-1-4338-0561-5. ISBN 10: 1-4338-0561-8. **References are required in your papers.**

Suggested Membership

Student membership in the Association for Computing Machinery www.acm.org for online access to research materials and tutorials.

Additional Materials Needed

Computer access – you will need access to a computer with MS Word and PowerPoint installed. Your computer should be reliable and accessible. **You MUST have a plan of action in the event your primary computing resources become unavailable to you.** Sources for an alternative may include using a family or friend's computer or access through a local library or public access system. You are responsible for having a backup plan. There is no excuse for not submitting your work on time because your computer is not working.

Title IX Information

Campbellsville University and its faculty are committed to assuring a safe and productive educational environment for all students. In order to meet this commitment and to comply with Title IX of the Education Amendments of 1972 and guidance from the Office for Civil Rights, the University requires all responsible employees, which includes faculty members, to report incidents of sexual misconduct shared by students to the University's Title IX Coordinator.

Title IX Coordinator:

Terry VanMeter

1 University Drive

UPO Box 944

Campbellsville, KY 42718

Administration Office 8A

Phone 270-789-5016

Email: twvanmeter@campbellsville.edu

Information regarding the reporting of sexual violence and resources that are available to victims of sexual violence is set forth at: www.campbellsville.edu/titleIX.

Course Policies

- Students should read assigned materials before class. Chapter objectives are provided at the beginning of each chapter in the text to help guide your reading.

- Changes in the syllabus may occur during the term to adjust the course requirements to best meet our learning objectives. Any changes will be announced online. It is the responsibility of the student to keep abreast of any changes.
- Check your e-mail daily for any announcements.
- All assignments are due based on Eastern Daylight Time.
- All work submitted must be your own. Plagiarism is not tolerated.

Attendance and Participation Policy

You will be expected to participate actively in class discussions and class activities **on time**. You will be considered absent each week that you do not answer the discussion question for the week. If you do not answer the discussion for one week, your lack of participation (absence) will be reported. If you do not answer the discussion for two total weeks, you will be withdrawn from the class with a “WA” grade, which is calculated as a “F” grade.

Late work, including DQ responses and written assignments are considered late if posted after the due date. **Points will be deducted for late work:**

5 point deduction after due date

10 point deduction after the first week late

15 point deduction after the second week late

20 point deduction after that point in time

No points will be given for late replies to fellow students. You must post the replies in the week they are due. Replies are awarded 5 points if posted on time.

Written Assignment penalties for Weeks 2, 4, 6, and 8 assignments:

One Week Late: 2 point deduction

Two Week Late: 4 point deduction

Three Week Late: 6 point deduction

Four Weeks or more: 8 point deduction

Less than a week late deduction at the discretion of the faculty instructor

No late work will be accepted without prior approval of the instructor. In addition, **NO WORK** will be accepted **after the close of the class** at the end of the session. The last day for acceptance of late work will be the last day of class.

Disability Policy

Campbellsville University is committed to reasonable accommodations for students who have documented physical and learning disabilities, as well as medical and emotional conditions. If you have a documented disability or condition of this nature, you may be eligible for disability services. Documentation must be from a licensed professional and current in terms of assessment. Please contact the Coordinator of Disability Services at 270-789-5192 to inquire about services.

Academic Honesty

Academic dishonesty (plagiarism and cheating) will not be tolerated. If you are caught engaging in any form of academic dishonesty, you will automatically fail the course.

Course Assessment

Weekly discussion questions (8 lessons x 30 points each)	240 points
Quizzes (8 lessons x 15 points each)	120 points
Lesson assignments (4 assignments x 20 points each)	120 points
Project paper on an information security topic (Any topic related to IT Security will be acceptable)	100 points
TOTAL POINTS	580 points

522-580	=	A
463-521	=	B
404-462	=	C
345-403	=	D
Below 344	=	F

Teaching Methods and Techniques

Online lectures, project assignment with paper and presentation, online activities, online discussion questions, quizzes, and individual assignments.

Tentative Course Schedule

WEEK	CHAPTER	TOPICS
Week 1	1, 2, 3	<p>Introduction and security trends General security concepts Operational and organizational security Chapter Objectives: 1—Student will describe various types of threats that exist for computers and networks. 2—Student will recognize some of the basic models used to implement security in operating systems. 3—Student will describe physical security components that can protect computers and network. LESSON READING ASSIGNMENT: Read Chapters 1, 2, 3 (Objectives 1, 2, 3) Go to the <i>Water Cooler</i> to introduce yourself to the Professor and to the class. LESSON QUIZ: Chapters 1, 2, 3 (Objectives 1, 2, 3) TERM PROJECT: Paper due at the end of Week 7</p>

Week 2	4, 5, 6	<p>Role of people in security Cryptography Public key infrastructure Chapter Objectives: 1—Student will recognize methods attackers may use to gain information about an organization. 2—Student will identify and describe the three types of cryptography. 3—Student will explain the relationship between trust and certificate verification. LESSON READING ASSIGNMENT: Read Chapters 4, 5, 6 (Objectives 1, 2, 3) LESSON WRITTEN ASSIGNMENT: IT governance plan analysis LESSON QUIZ: Chapters 4, 5, 6 (Objectives 1, 2, 3) TERM PROJECT: Paper due at the end of Week 7</p>
Week 3	7, 8, 9	<p>Standards and protocols Physical security Network fundamentals Chapter Objectives:</p>

		<p>1—Students will identify the standards involved in establishing an interoperable Internet PKI. 2—Students will describe steps that can be taken to help mitigate risks. 3—Students will define the basic network protocols. LESSON READING ASSIGNMENT: Read Chapters 7, 8, 9 (Objectives 1, 2, 3) LESSON QUIZ: Chapters 7, 8, 9 (Objectives 1, 2, 3) TERM PROJECT: Paper due at the end of Week 7</p>
--	--	---

Week 4	10, 11, 12	<p>Infrastructure security Authentication and remote access Wireless security and mobile devices</p> <p>Chapter Objectives:</p> <p>1—Students will describe the different types of storage media used to store information. 2—Students will identify the methods and protocols for remote access to networks. 3—Students will describe the different wireless systems in use today.</p> <p>LESSON READING ASSIGNMENT: Read Chapters 10, 11, 12 (Objectives 1, 2, 3) LESSON WRITTEN ASSIGNMENT: Text, page 334, Essay Quiz #2 (Objective 2) LESSON QUIZ: Chapters 10, 11, 12 (Objectives 1, 2, 3) TERM PROJECT: Paper due at the end of Week 7</p>
Week 5	13, 14, 15	<p>Intrusion detection systems and network security System hardening and baselines Types of attacks and malicious software</p> <p>Chapter Objectives:</p> <p>1—Students will determine the appropriate use of tools to facilitate network security. 2—Students will investigate group policies. 3—Students will describe various types of computer and network attacks, including denial-of-service, spoofing, hijacking, and password guessing.</p> <p>LESSON READING ASSIGNMENT: Read Chapters 13, 14, 15 (Objectives 1, 2, 3) LESSON QUIZ: Chapters 13, 14, 15 (Objectives 1, 2, 3) TERM PROJECT: Paper due at the end of Week 7</p>

Week 6	16, 17, 18	<p>E-mail and instant messaging Web components Secure software development Chapter Objectives: 1—Students will describe security issues associated with e-mail. 2—Students will explain web applications, plug-ins, and associated security issues. 3—Students will describe the major types of coding errors and their root causes. LESSON READING ASSIGNMENT: Read Chapters 16, 17, 18 (Objectives 1, 2, 3) LESSON WRITTEN ASSIGNMENT: Text, page 529, Lab Project 16.2. (Objectives 1, 2) LESSON QUIZ: Chapters 16, 17, 18 (Objectives 1, 2, 3) TERM PROJECT: Paper due at the end of Week 7 NEXT WEEK!</p>
Week 7	19, 20, 21	<p>Business continuity, disaster recovery, and organizational policies Risk management Change management Chapter Objectives: 1—Students will describe the various components of a business continuity plan. 2—Students will explain the differences between qualitative and quantitative risk assessment. 3—Students will identify the essential elements of change management. LESSON READING ASSIGNMENT: Read Chapters 19, 20, 21 (Objectives 1, 2, 3) LESSON QUIZ: Chapters 19, 20, 21 (Objectives 1, 2, 3) TERM PROJECT: Paper due at the end of Week 7 THIS WEEK!</p>
Week 8	22, 23, 24	<p>Incident response Computer forensics Legal issues and ethics Chapter Objectives: 1—Students will identify the differences among user, group, and role management. 2—Students will identify the rules and types of evidence. 3—Students will identify the laws that govern computer access and trespass.</p>

		LESSON READING ASSIGNMENT: Read Chapters 22, 23, 24 (Objectives 1, 2, 3) LESSON WRITTEN ASSIGNMENT: Text, page 694, Essay Quiz #3. (Objective 2) LESSON QUIZ: Chapters 22, 23, 24 (Objectives 1, 2, 3)
--	--	---

Project Written Report and Presentation

You will choose any information security topic from our textbook and/or discussions to write a paper and develop a PowerPoint presentation. The final report should be 10-12 pages, 12 font size, 1" margins, double-spaced, including figures, tables, etc. Follow the current APA format guide for your report. Use spell check, grammar check, etc. to make sure that your report is written in professional form with no keyboarding or grammatical errors. No abstract is required. However, a cover page and a reference page are required. Make sure the cover page and reference page are also in current APA format.

Your project paper will be assessed as follows:

- Is the paper of optimal length?
- Is the paper well organized?
- Is the paper clear and concise?
- Is the title appropriate
- Are individual ideas assimilated well?
- Are wording, punctuation, etc. correct?
- Is the paper formatted correctly?
- Is the paper well motivated?
- Is an interesting problem/issue addressed?
- Is knowledge of the area demonstrated?
- Use of diagrams or other graphics?
- Have all key references been cited?
- Are conclusions valid and appropriate?

You will need to develop a PowerPoint presentation to summarize your final report. Use transition and animation in your slides. Ten to twenty slides are required to highlight your project.

Discussion Questions and Online Netiquette

Listed below are the discussion (essay) questions that we will cover. Make sure that your response reflects an understanding of the situation and the reading materials. Each answer/response should be supported with research unless the question is opinion oriented. Answer my question by 11 p.m. on Wednesday evening (minimum 250 word response); and give a response to one classmate between 1 a.m. on Thursday and 11 p.m. on Saturday evening (minimum 125 word response to each classmate). Do not give both responses on Wednesday.

Your class participation will be evaluated on the following criteria:

- Discussion contributions reflect thorough preparation.
- Ideas offered are usually substantive and provide good insight and sometimes direction for the class.
- Class comments and demeanor support an open and encouraging class environment.
- Arguments are usually well supported and often persuasive.
- Comments usually help others improve their thinking.
- Students are required to post one original response for each discussion question, as well as a response to one classmate. Original responses should not be a word for word rehashing of what is stated in the readings, but rather an integration of the concepts and additional insights, either from real world experience or additional sources. It should be a 250 word response to my question each week by 11 p.m. on Wednesday evening. Your primary posting may end with a tag-line or a related question of your own. Between 1 a.m. on Thursday and 11 p.m. on Saturday, you should have done your secondary posting. Your secondary posting is a response to one classmate's post. Each answer/response should be supported with research unless the question is opinion oriented. Responses to classmates should not be "I agree" or "I like the way you stated that." These responses should again be insightful, offering an opinion or facts based on your research and experiences. The response to one classmate should be a minimum of 125 words. See APA criteria for citing resources.

Week 1 Discussion Question

Your boss mentions that recently a number of employees have received calls from individuals who didn't identify themselves and asked a lot of questions about the company and its computer infrastructure. At first, he thought this was just a computer vendor who was trying to sell your company some new product, but no vendor has approached the company. He also says several strange e-mails requesting personal information have been sent to employees, and quite a few people have been seen searching your company's trash dumpsters for recyclable containers.

Your boss asks what you think about all of these strange incidents. Respond and be sure to provide a recommendation on what should be done about the various incidents.

Week 2 Discussion Question

Perform a search on the Web for articles and stories about social engineering attacks or reverse social engineering attacks. Find an attack that was successful and describe how it could have been prevented.

Week 3 Discussion Question

Discuss why your company or organization needs more user education about security. What topics should be included in security education and training?

Week 4 Discussion Question

What concerns should be understood about data communications being sent over wireless networks? Discuss the pros and cons of one method of transmission, such as Wireless Application Protocol (Search the Internet for help in wireless networks).

Week 5 Discussion Question

Describe the best practice to employ to mitigate malware effects on a machine

Week 6 Discussion Question

Much has been made of the new Web 2.0 phenomenon, including social networking sites and user-created mash-ups. How does Web 2.0 change security for the Internet? How do secure software development concepts support protecting applications?

Week 7 Discussion Question

Describe and discuss at least two backup strategies. Discuss the use of cloud backup strategies, as well?

Week 8 Discussion Question

Discuss one of the most important things you will take from this course. You do not have to document your sources for this question. It is an opinion question

BOOKS RECOMMENDED BY OUR TEXTBOOK AUTHORS

Computer Forensics: A Beginner's Guide. McGraw-Hill ISBN: 978-0-07-174245-0.

Security Metrics: A Beginner's Guide. McGraw-Hill ISBN: 978-0-07-174400-3.

Web Application Security: A Beginner's Guide. McGraw-Hill ISBN 978-0-07-177616-5.

Wireless Network Security: A Beginner's Guide. McGraw-Hill ISBN 978-0-07-176094-2.