COMP430 Computer Security
Fall 2017
Syllabus

Catalog Description
Network security concepts and methodologies. Topics include: security concepts and services, physical, operational, and organizational security, the role of people in systems security compliance and operational security; threats and vulnerabilities; network security. Access control and identity management; cryptography will also be covered in this course. Labs and projects will focus on techniques and tools for vulnerability detection and defense. Lecture and mandatory one hour lab session per week.

Credits: 3

Course Objectives:
This course fulfills suggested curriculum requirements of ACM, IEEE, and the Computer Science Accreditation Board for Computer Science departments. The course will provide the student with an overview of the tools and techniques of:

- protecting information assets,
- determining the levels of protection and response to security incidents,
- and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features.

The purpose of the course is to provide the student with an overview of the field of information security and assurance. Students will be exposed to the spectrum of security activities, methods, methodologies, and procedures.

Professional Objectives
This course is designed specifically to prepare students to be proficient in various computer security activities, methods, methodologies, and procedures. Coverage will include inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post-incident procedures, technical and managerial responses, and an overview of the information security planning and staffing functions.

Student Learning Outcomes:

- Describe the different categories of network threats and attacks.
- Describe the architecture for public and private key cryptography and how public key infrastructure (PKI) supports network security.
- Describe virtues and limitations of security technologies at each layer of the network stack.
- Identify the appropriate defense mechanism(s) and its limitations given a network threat.
- Discuss security properties and limitations of other non-wired networks.
- Identify the additional threats faced by non-wired networks.

- Describe threats that can and cannot be protected against using secure communication channels.
- Summarize defenses against network censorship and diagram a network for security.

Course Format: Lectures and Labs

Instructor : Martin Dwomoh-Tweneboah
Office : Renshaw 209
Office Phone : (503)883-2426 E-mail : mdwomoh@linfield.edu
Office Hours : Daily 3:00 - 5:00PM or by appointment.

Textbook (*Required*): Exam 98-367 Security Fundamentals. J. Wiley Publishers
ISBN : 978-0-470-90184-7
Academic Learning Series Security+ Certification by Joern Wettern
McGraw Hill

Course Material: **Transcender** CompTIA Premium Solution for SY0-401
CompCert: Security+

Online Course Materials :
1. Online tutorials in computer security.
2. Certification Practice Exams Materials

Software: Windows Server 2012, Redhat Linux or CentOS, Ubuntu, and other online security utility software.

Grading
Grading for this course will be based on multiple quizzes, assignments, two midterm exams, and final exam. The total possible points at any given time in the course will divide your total points earned to-date, resulting in a percentage that will determine your grade according to the following table.

The performance level descriptions shown below generally identify computer program attributes necessary to achieve the associated point percentage and letter grade.

Quizzes	25%
Assignments	20%
Midterm Exams	25%
Final	30%

Grading Scale:

95 – 100	A
90 – 94	A-
85 – 89	B+
80 – 84	B
75 – 79	B-
70 – 74	C+
65 – 69	C
60 – 64	C-
50 – 59	D
Below 50	F

Assignments

General Information

Several short homework assignments will be given throughout the semester.

- Homework assignments will be posted on the course website.
- Except for occasional supplementary materials, hard copies of the assignments will not be provided.
- It is your responsibility to check the course web site for any materials relating to the course and to keep track of upcoming assignments, quizzes and midterms.
- Homework is due at the ***beginning*** of class on the due date.
    - You are expected to have completed the assignment before you arrive in class.
    - You will have a 30-minute window after the class during which you may turn in your assignment with no penalty.

Assignment Management

The curriculum is designed to produce graduates ready to function in the computer industry with the competencies, skills, and attitudes necessary for success in the workplace or graduate school. It forms the basis for continued career growth, life-long learning as a computer professional or a future graduate program. Among other important skills for administrators and managers are time management and resource allocation. Specifically, appropriate attention to time management and resource allocation will aid you in meeting task deadlines with available resources. These skills will be important to your success in administration or management and to your success in your degree program. This syllabus describes course assignments and defines assignment due dates. Your effective use of time management and resource allocation will be key in meeting the assignment deadlines for both individual and study group assignments. From my own experience, I offer the suggestion that your time management plan include time for yourself and your academic work.

Late Assignments

In the general case, late assignments will not be accepted for grading. ALL ASSIGNMENTS; IF A HARD COPY IS REQUIRED, MUST BE SUBMITTED IN CLASS ON THE DUE DATE. If you know you must be absent from a class session, you should take appropriate steps to ensure that your assignments are delivered on or before the scheduled due date and time. I will not accept any excuse for late delivery. In addition to submitting a hard copy, you must keep electronic copies of all assignments in a folder in your home directory on the server. If submission is electronic, it must be in your home directory on the server on or before the due date.

Assignment Format
Assignments should be neatly typed so that it is: (a) easy to grade, and (b) useful as a study aid. Assignments submissions that do not meet minimal standards for acceptability in the workplace (completeness, neatness, readability, etc.) will be returned ungraded.

Quizzes
Quizzes are conducted during the class meeting and at times as take-home. Quiz questions will often be selected from or derived from the questions found at the end of the assigned chapters and readings. I will not give make-up exams and quizzes.

Attendance
Attendance is mandatory.

Course Materials
All course materials, can be found on Blackboard at http://bblearn.linfield.edu. It is your responsibility to check the web page on regular basis for course materials and due dates.

Extra Credit Policy
There will not be any extra credit in this course. There are a lot of assessment exercises in this course for you to catch up with areas you don't perform well. Therefore, don't bank on extra credit to improve your grades.

Missed Classes
It is your responsibility to make arrangements to obtain materials distributed on class days when you miss a class. This can be done through contacting a classmate who was present or by contacting me during my office hours or other times. Missed or late quizzes cannot be made up under any circumstances but with good cause and adequate notice, an early quiz may be given. If you miss a class, make sure you go through all the lab work you missed because each lesson is built on the previous one.

Academic Integrity
Linfield College operates under the assumption that all students are honest and ethical in the way they conduct their personal and scholastic lives. Academic work is evaluated on the assumption that the work presented is the student's own, unless designated otherwise. Anything less is

unacceptable and is considered a violation of academic integrity. Furthermore, a breach of academic integrity will have concrete consequences that may include failing a particular course or even dismissal from the college, as published in the Linfield College Course Catalog.

Violations of academic integrity include but are not limited to the following:

Cheating: Using or attempting to use unauthorized sources, materials, information, or study aids in any submitted academic work.

Plagiarism: Submission of academic work that includes material copied or paraphrased from published or unpublished sources without proper documentation. This includes self-plagiarism, the submission of work created by the student for another class unless he or she receives consent from both instructors.

Fabrication: Deliberate falsification or invention of any information, data, or citation in academic work.

Facilitating Academic Dishonesty: Knowingly helping or attempting to help another to violate the college's policy on academic integrity.

Classroom and Group Discussions

Study groups are highly recommended for a course of this kind. However, copying someone's work for presentation will be treated as academic dishonesty. Active involvement of each student in class discussions and exercises are essential. Class attendance and active participation are expected and required in this course. Absences or lack of participation generally reduces a learner's aggregate point score and thus may affect a learner's final grade.

We must assume that we are all persons of intelligence and good will who are here to learn from each other in a team environment. Group discussions should not be a forum to impose our ideas on others. For the academic endeavor to succeed, we must treat each other with civility, courtesy and respect. Software development involves team work and all contributions by group members should be discussed and analyzed thoroughly.

Preparation for Classes

- Read the text chapter assigned per schedule.
- Visit the companion Web site on Blackboard and review the topic objectives and other materials, complete online study guide quizzes, and review other materials.
- Make note of any questions you may have to pose during class or via e-mail.
- Browse the PowerPoint presentation for the topic.
- Take notes in class.

Difficulties

If you find you are having problems with the class – the use of the software package, case tool, attendance, keeping up with the reading, fitting into a group, please let me know. I am always available to help you, but I have to know about the problem while it's going on and before the end of the course. The last few weeks to the end of the course is not the best time to ask for help.

Students with Disabilities

Students with disabilities are protected by the Americans with Disabilities Act and Section 504 of the Rehabilitation Act. If you are a student with a disability and feel you may require academic accommodations please contact Learning Support Services (LSS), as early as possible to request accommodation for your disability. The timeliness of your request will allow LSS to promptly arrange the details of your support. LSS is located in Melrose Hall 020 (503-883-2562). We also encourage students to communicate with faculty about their accommodations.

Students with documented disabilities who may need accommodations for taking quizzes and tests, who have any emergency medical information I should know of, or who need special arrangements in the event of an evacuation, should make an appointment with me as early as possible, no later than the second week of the semester.

CELL PHONE USAGE, EMAIL AND WEB BROWSING

All cell phones should be turned off during lectures. Unless otherwise instructed, all applications, including browsers and emails must be closed during lectures.

Course Outline

Control Fundamentals and Security Threats

Network Protocols, Attacks, and Defenses

Creating Secure Networks

Vulnerability Assessment and Penetration Testing

Authentication, Biometrics, and Security Controls

Securing a Networked Environment

Remote Access, Mobile, and Wireless Security

Cryptographic Methods and Public Key Infrastructures

Securing Applications, Virtualization, and the Cloud

Continuity, Disaster Recovery, and Computer Forensics

Note: The above schedule is subject to modification.