CONESTOGA

COURSE OUTLINE

Course Systems Development: Computer Security (2015-2016)

Code / Version INFO2050 (100)

Total Hours 45

Credits 3

PreRequisite(s) PROG2230 (102) Programming: MS Web Tech
or PROG2230 (103) Programming: MS Web Tech

CoRequisite(s)

Course Description

In this course, students will investigate threats to computer business applications from a variety of sources, as well as strategies for handling those threats. Topics will include encryption, SQL injections, URL backdoors, malware, wireless and cloud computing vulnerabilities, code level security, physical security, disaster recovery and backup, and privacy considerations.

PLAR Eligible: Yes

Course Outcomes

Successful completion of this course will enable the student to:

1. Describe the various types of threats to which applications and interactive web sites are subject.
2. Explain the motivations for attacks on computer applications and use this knowledge to assess the likelihood of an attack on an application.
3. Determine where the use of encryption is appropriate in a computer application or in the infrastructure of an application.
4. Develop test plans to assess the vulnerabilities of computer applications to various types of attacks.
5. Evaluate the system development process of an organization for its attention to security issues.
6. Assess an organization’s business plan for its attention to security of its computer applications.
7. Develop a plan for the physical security, disaster recovery and backup of its business applications.
8. Develop a security plan for protecting applications managed in a cloud environment.
9. Explain the rights and obligations, both legal and ethical, of the managers and users of a social networking site.

Essential Employability Skills addressed in this course			Taught	Reinforced	Assessed
Communication	ⁿ	Communicate clearly, concisely and correctly in the written, spoken, and visual form that fulfills the purpose and meets the needs of the audience		X	X
	ⁿ	Respond to written, spoken, or visual messages in a manner that ensures effective communication		X	X
Numeracy	ⁿ	Execute mathematical operations accurately			
Critical Thinking and Problem Solving	ⁿ	Apply a systematic approach to solve problems	X		X
	ⁿ	Use a variety of thinking skills to anticipate and solve problems	X		X
Information Management	ⁿ	Locate, select, organize, and document information using appropriate technology and information systems	X		X
	ⁿ	Analyze, evaluate, and apply relevant information from a variety of sources	X		X
Interpersonal	ⁿ	Show respect for the diverse opinions, values, belief systems, and contributions of others		X	
	ⁿ	Interact with others in groups or teams in ways that contribute to effective working relationships and the achievement of goals		X	

Essential Employability Skills addressed in this course			Taught	Reinforced	Assessed
Personal	n	Manage the use of time and other resources to complete projects		X	
	n	Take responsibility for one's own actions, decisions, and consequences		X	

Unit Outcomes

Successful completion of the following units will enable the student to:

1.0 Security Management

- 1.1 Develop a high level business assessment of an organization’s security plans.
- 1.2 Develop a plan for incorporating security into the software development life cycle.
- 1.3 Develop policies and procedures to promote best security practices within an organization.

2.0 Social Activism and the Underground Economy

- 2.1 Identify the different motivations that lead to attacks on data, privacy and intellectual property of individuals and organizations.
- 2.2 Using knowledge of the underground economy for security breaches, evaluate the likelihood of attack on a business application.

3.0 Network and Wireless Security

- 3.1 Evaluate a wireless application for vulnerability to attack.
- 3.2 Develop strategies to deal with threats to wireless applications.
- 3.3 Describe potential threats based on computer infrastructure.
- 3.4 Describe how the use of network monitoring tools can be used to intercept tool data communications.
- 3.5 Describe the methods used to implement Direct Denial of Service (DDOS) attacks.

4.0 Threats to Web Applications

- 4.1 Evaluate the vulnerability of a site to SQL and other code injections.
- 4.2 Describe the principles of cross-site scripting.
- 4.3 Describe the methods by which web sites are attacked through URL manipulation.

5.0 Von Neumann Architecture

- 5.1 Describe the components of processing hardware of the computer as they relate to computer security.
- 5.2 Describe the architecture of current Operating Systems as they relate to computer security.
- 5.3 Describe memory models for computer applications as they relate to applications security.

6.0 Malware

- 6.1 Identify and describe the various types of malware.
- 6.2 Develop strategies for minimizing the risks from malware threats of users and organizations.

7.0 Encryption

- 7.1 Explain the basic principles of symmetric and asymmetric encryption, hashing and digital signing.
- 7.2 Evaluate an application to determine which of its components should be protected by encryption and the level of that encryption.
- 7.3 Explain the use and significance of encryption packages such as SSL, and explain the best practices they incorporate for combining different kinds of encryption and digital signing in order to provide secure data communications.

8.0 Privacy, the Law and Social Networking

- 8.1 Explain both the rights and the liabilities of the consumer in using a business application or a social networking site.

8.2 Assess an application for conformance to legal and accepted privacy standards.

8.3 Evaluate the threats to users of ecommerce, social media and other web sites resulting from unsavoury data collection practices.

8.4 Develop a plan for maintaining privacy of data in an application managed in a cloud environment.

9.0 Physical Security, Disaster Recovery and Backup

9.1 Prepare an audit plan to determine whether an organization is prepared for physical attacks and natural catastrophes, and to determine its effectiveness restoring applications and data.

9.2 Evaluate an application for vulnerability to use by unauthorized users who have penetrated its security system.

Required Student Resources

Optional Student Resources

Mark Ciampa. Security Awareness (4th). Cengage Learning.

Oram and Viega. Beautiful Security (1st). O'Reilly.

Language manuals, web sites, chat rooms and bulletin boards

Evaluation

The minimum passing grade for this course is 55 (D).

In order to successfully complete this course, the student is required to meet the following evaluation criteria:

Project Modules (7@4.3%)	30.00
Presentation	10.00
Midterm Exam	30.00
Final Exam	30.00
	100.00 %

Other

Conestoga College is committed to providing academic accommodations for students with documented disabilities. Please contact the Accessibility Services Office.

Prepared By Randall Kozak

School Information Technology

Date 2015-11-20