# **Previous Report**

#### **Course Outline**

Engineering and Applied Science

Faculty of Science

SENG 4220 - **3.00** - Academic

Software Security Engineering

#### Rationale

GET analysis has identified that this course meets the Knowledge ILO criteria. See attached foci tool and notes under Educational Objectives/Outcomes.

### **Calendar Description**

Students explore the various software security issues in the context of software development lifecycle. Students are introduced to set of processes, policies, and techniques that are appropriate for software security management, maturity, and risk tolerance. Students learn how to incorporate practical security techniques into all phases of the development lifecycle. Students learn writing secure software application by exploring various commonly known security flaws.

#### **Credits/Hours**

**Course Has Variable Hours:** No **Credits:** 3.00 **Lecture Hours:** 3.00 **Seminar Hours:** 0

# **Current Report**

#### **Course Outline**

#### **Engineering**

Faculty of Science

SENG 4220 - **3.00** - Academic

Software Security Engineering

### Rationale

The proposed course outline for Software Security Engineering has been revised to address the escalating importance of secure coding practices and the evolving landscape of software vulnerabilities. The recent security concepts and tools related to PKI, internet security, and emerging technologies like blockchain have been incorporated into the course.

# **Calendar Description**

Students explore the various software security issues in the context of software development lifecycle. Students are introduced to a set of processes, policies, and techniques that are appropriate for software security management, maturity, and risk tolerance. Students learn how to incorporate practical security techniques into all phases of the development lifecycle. In addition, students will examine fundamental security principles, cryptographic building blocks, authentication methods and protocols, software exploits, privilege escalation, and malicious software. The course also includes public-key infrastructure (PKI), web and browser security, and network security. Students learn to write secure software applications by exploring various commonly known security flaws.

# **Credits/Hours**

**Course Has Variable Hours:** No **Credits:** 3.00 **Lecture Hours:** 3.00 **Seminar Hours:** 0 **Lab Hours:** 2.00 Lab Hours: 2.00 Other Hours: 0 *Clarify:* Total Hours: 5.00 Delivery Methods: (Face to Face) Impact on Courses/Programs/Departments: Software Engineering Program Repeat Types: A - Once for credit (default) Grading Methods: (S - Academic, Career Tech, UPrep)

# **Educational Objectives/Outcomes**

 Understand software security issues in various phases of software development lifecycle.
Analyze the processes, policies, and techniques in managing software security in various contexts of application domains.
<del>Capture requirements for secure software applications.</del>
Understand common software code vulnerabilities.
Apply security principles in designing secure software architecture.
<del>This course meets the Knowledge criteria</del>. <del>See attached foci tool demonstrating the match.</del>

# Prerequisites

SENG 3210-Applied Software Engineering A minimum of grade "C" or better in prerequisite course.

# **Co-Requisites**

**Recommended Requisites** 

### **Exclusion Requisites**

# **Texts/Materials**

#### Textbooks

1. **Required** Allen, J H, Barnum S, Ellison R J, McGraw G, Mead N R. *Software Security Engineering: A Guide for Project Managers* Addison-Wesley Professional, 2008, ISBN: 10:032150917X.

2. **Required** David LeBlanc, Michael Howard. *Writing* Secure Code, 2nd ed. Microsoft Press, ISBN: 0735617228.

### **Student Evaluation**

Other Hours: 0 *Clarify:* Total Hours: 5.00 Delivery Methods: (Face to Face) Impact on Courses/Programs/Departments: Software Engineering Program Repeat Types: A - Once for credit (default) Grading Methods: (S - Academic, Career Tech, UPrep)

# **Educational Objectives/Outcomes**

 Understand software security issues in various phases of software development lifecycle.
Analyze the processes, policies, and techniques in

managing software security in various contexts of application domains.

3. <u>Apply cryptographic techniques to protect data</u> <u>confidentiality and integrity, including encryption, hashing,</u> <u>digital signatures, and key management.</u>

4. Understand common software code vulnerabilities.

5. Apply security principles in designing secure software architecture.

6. <u>Understand web and browser security implementations</u> and how internet security works.

# Prerequisites

SENG 3210-Applied Software Engineering A minimum of grade "C" or better in prerequisite course.

# **Co-Requisites**

### **Recommended Requisites**

# **Exclusion Requisites**

# **Texts/Materials**

#### Textbooks

1. **Required** Paul C. van Oorschot. *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin*, Second ed. Springer, 2021, ISBN: 978-303083410.

# **Student Evaluation**

<u>The Course grade is based on the following course</u> evaluations. Assignments and Labs (20.00%) Two Mid

The Course grade is based on the following course

<u>Term Exams</u>	( <u>30.00%</u> )	Project	( <u>15.00%)</u>	Final	<u>Exam</u>
<u>(35.00%)</u>		-			

#### **Course Topics**

Topics	Textbook Mapping		
	Chapter #	Book	
Why Is Security a Software Issue?	1	B1	
What Makes Software Secure?	2	B1	
Requirements Engineering for Secure Software	3	B1	
<del>Secure Software Architecture and</del> <del>Design</del>	4	B1	
<del>Considerations for Secure Coding and Testing</del>	5	B1	
Security and Complexity: System Assembly Challenges	6	B1	
<del>Governance, and Managing for More</del> <del>Secure Software</del>	7	B1	
<del>Public Enemy #1: The Buffer</del> <del>Overrun</del>	5	<del>B2</del>	
<del>Determining Appropriate Access</del> <del>Control</del>	6	<del>B2</del>	
Running with Least Privilege	7	<del>B2</del>	
Protecting Secret Data	9	<del>B2</del>	
All Input Is Evil!	10	<del>B2</del>	
Canonical Representation Issues	11	<del>B2</del>	
<del>Database Input Issues</del>	12	<del>B2</del>	

#### Methods for Prior Learning Assessment and Recognition

As per TRU Policy.

Last Action Taken

# **Course Topics**

Topics	Textbook Mapping	
	Chapter #	Book
Introduction to Software Security	1	B1
Software Security Background	1	B1
<u>Cryptographic Building Blocks</u>	2	B1
User Authentication	3	B1
Authentication Protocols and Key Establishment	4	В1
<u>Software Security - Exploits and</u> <u>Privilege Escalation</u>	6	B1
Malicious Software	7	B1
Public-Key Certificate Management and Use Cases	<u>8</u>	B1
Web and Browser Security	9	B1
Code Injection and Clickjacking	9	B1
Firewalls and Tunnels	10	B1
Anonymity and Intrusion Detection	11	B1
<u>Network Security</u>	12	B1
Bitcoin, Blockchains and Ethereum	<u>13</u>	B1

#### Methods for Prior Learning Assessment and Recognition

As per TRU Policy.

### Last Action Taken

Default by HOLD TRU Conversion

Implement by Submission	Drovious Subce	mmittoo Chair
implement by Submission	rieview Subce	Jinninee Chair
Shelley Church		

# Awaiting Action

Awaiting Action by Dean(s)

Current Date: 16-May-25

Current Date: 16-May-25