DO NOT TYPE IN THIS BOX

Bulletin #: 5

Academic Year: 2020-21

FLORIDA INTERNATIONAL UNIVERSITY
UNIVERSITY CURRICULUM COMMITTEE
Proposal for a Course Change

PART I. FILL OUT THIS SECTION COMPLETELY

1. **School/College** Engineering and Computing

   Div./Dept. in Which Taught School of Computing and Information Scienc

2. | CEN | 5 | 079 | C | 3 |
   |---|---|---|---|---|
   | Alpha Prefix | 1st Digit | Last 3 Digits | "C"-lec-lab "L"-Lab | Cr. Hrs. |

3. **Present Course Title** Secure Application Programming

PART II. FILL OUT CHANGE INFORMATION ONLY

Change Effective 08 / 01 / 2021

4a. **New Course Title** Software Vulnerabilities and Security

b. **New Abbreviated course Title** *(for computer class schedules, transcripts)* Software Security

LIMITED TO 25 Characters *(including spaces)*

5a.

New Alpha Prefix	New 1st Digit	New Last 3 Digits	Change "C"-lec-lab "L"-Lab

5b. Change Credit Hours: From _____ To _____

6. **New Catalog Description/Major Topics** *(not to exceed 200 characters including spaces)*
   College of Medicine and College of Law: Attach description not exceeding 1,000 characters including spaces.

7. **New Prerequisite(s):** _____

8. **New Corequisite(s):** _____

9. **Explain Reclassification Request:**

   The new name will more accurately reflect the syllabus. No change to the syllabus is proposed. The course will be included in the Systems focus

10. **Does this proposed change impact the assessment process of a program or certificate? If yes, then send notification to assessment@fiu.edu.**

PROPOSAL REQUESTED BY:

Faculty Contact Amin Kharaz (Type name) — Amin Kharaz (Signature) — 01 / 30 / 2021

ak@cs.fiu.edu (Email address) — 339-224-3351 (Phone number)

Chairperson (Dept./Div.) Jason Liu (Type name) — (Signature) — 02 / 01 / 2021

Chairperson (Curr. Comm.) Wei-Chiang Lin (Type name) — (Signature) — 02 / 10 / 2021

College/School Dean John Volakis (Type name) — Anthony McGoron Digitally signed by Anthony McGoron Date: 2021.02.16 08:38:09 -05'00' (Signature) — ____ / ____ / 20____

Submit one original form. Attach one copy of the Course Justification and Course Syllabus: Course Description, Objectives, Learning Outcomes, Major Topics and textbooks.

Justification

Amin Kharraz is an assistant professor at the department of Compute and Information Sciences. He holds a Ph.D. degree in cybersecurity from Northeastern University. Before joining FIU, he was a postdoctoral research associate at the University of Illinois at Urbana-Champaign where he led projects to rigorously analyze Internet scale online attacks and develop defense mechanisms to mitigate these attacks in a scalable and reliable manner. Amin Kharraz has over 12 years of experience in systems security, software engineering, and vulnerability analysis. His work has helped develop techniques to protect users from important security problems, including ransomware, web attacks, and guide the design of new defense systems and incident response platforms. Before that, he was a senior security engineer leading projects on IT audit and compliance, security investment consulting, infrastructure, applications and incident response.

He has also taught multiple graduate and undergraduate-level security courses at Northeastern University, where he incorporated the results of proposed research to educate students about modern attacks and defenses that they can use in practice. For instance, the course Software Vulnerabilities and Security covered the fundamental concepts of systems security, network and web security, operating systems security, intrusion detection, and recent topics such as malware. Amin Kharraz served on program committees of numerous well-known international security conferences and workshops.

Course Objective Metrics:

This course aims to make students “security aware”, and grain an in-depth understanding about security issues. The goals of the course are the following:

1 - Study common programming, configuration, and design mistakes in various software domains and levels of the software stack.

Amin Kharraz has developed several security systems to perform static and dynamic analysis in the area of web application security and malware detection. He designed and developed instrumentation frameworks for JavaScript and Windows binaries to analyze memory corruption and dynamic vulnerability discovery, and exploit analysis.

2- Understand approaches for detecting the presence of vulnerabilities during development and deployment.

Amin Kharraz has several years of experience in vulnerability detection and analysis. He has a strong background on software fuzzing, code debugginging, and reverse engineering Windows executables and Java applications. His area of research includes vulnerability analysis in a wide range of software systems such as Web applications, Web browsers, unix-based and Windows operating systems

3- Gain hands-on experience in attacking and defending vulnerable software systems.

Amin Kharraz has a strong background in developing system-oriented assignments to put the studied subjects into practice. He has designed several course challenges that are based on Capture The Flag (CTF) challenges which usually requires students to write tools to discover security flaws in different software

systems such as databases and remote servers, and devise code to exploit the target vulnerabilities.

Last Update

Amin Kharraz, 01/30/2021

CIS 5375 Software Vulnerabilities and Security

Catalog Description

Gain practical knowledge of common security vulnerabilities, such as buffer overflow, SQL injection, memory corruption, binary analysis, web attacks, and the corresponding defense mechanisms. The emphasis of this course is to develop an in-depth understanding about common software security issues and ways to detect and prevent them. (3 credits)

Prerequisites

SCIS Graduate Standing

Type

Required for MS in Cybersecurity (the system track)

Course Objectives

Internet security has become part of everyday life where security problems impact practical aspects of our lives. Even though there is a considerable corpus of knowledge about tools and techniques to protect systems, information about what are the actual vulnerabilities and how they are exploited is not generally available. This situation hampers the effectiveness of security research and practice. Understanding the details of attacks is a prerequisite for the design and implementation of secure systems.

This course deals with common programming, configuration, and design mistakes and ways to detect and avoid them. Examples are used to highlight general error classes, such as stack and heap overflows. Possible protection and detection techniques are examined. The course includes a number of practical lab assignments where participants are required to apply their knowledge as well as a discussion of the current research in the field. Students will learn how the security of systems can be violated, and how such attacks can be detected and prevented. The course aims to make the students "security aware", and gain an in-depth understanding about security issues.

Topics

- Operating system security and vulnerability
- Stack and heap overflows
- Memory corruption
- Reverse engineering and binary analysis
- Static and dynamic analysis
- Malicious code (Ransomware, Botnet, APTs, Botnets)
- Breach detection and analysis
- Programming language security
- Software penetration testing
- Web Security
- Capture the Flag (CTF) challenges

Prerequisites

- Significant programming experience
- Knowledge of C/C++, shell scripting, scripting languages such as Python
- Basic SQL knowledge and web programming

Textbooks

There is no official textbook for this course.

Last Update

Amin Kharraz, 01/30/2021