



**FLORIDA INTERNATIONAL UNIVERSITY  
UNIVERSITY CURRICULUM COMMITTEE**  
*Proposal for a Course Change*

<b>DO NOT TYPE IN THIS BOX</b>	
Bulletin #:	<u>3</u>
Academic Year:	<u>2021-2022</u>

**PART I. FILL OUT THIS SECTION COMPLETELY**

1. School/College College of Engineering and Computing
- Div./Dept. in Which Taught KFSCIS
2. 

<u>CIS</u>	<u>5</u>	<u>374</u>	<u>N/A</u>	<u>3</u>
Alpha Prefix	1st Digit	Last 3 Digits	"C"-lec-lab "L"-Lab	Cr. Hrs.
3. Present Course Title Information Security and Privacy

**PART II. FILL OUT CHANGE INFORMATION ONLY**

Change Effective 08 / 01 / 2022

- 4a. New Course Title Security and Privacy: Attacks and Defenses
- b. New Abbreviated course Title (for computer class schedules, transcripts) Sec & Priv: Attacks, Defs  
LIMITED TO 25 Characters (including spaces)

- 5a. 

<u>C</u>	<u>5</u>	<u>374</u>	<u>N/A</u>
New Alpha Prefix	New 1st Digit	New Last 3 Digits	Change "C"-lec-lab "L"-Lab
- 5b. Change Credit Hours: From 3.00 To 3.00

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.*
- Introduction to cyber threats with a focus on attack types, and privacy issues that include fair information practices, anonymity vs. privacy, risks, tracking and surveillance, tools, and policies.

7. New Prerequisite(s): M.S. or Ph.D. standing or permission of the instructor
8. New Corequisite(s): None

9. Explain Reclassification Request:
- We restructure the MS Cybersecurity program syllabus, to enable National Centers of Academic Excellence in Cybersecurity certification by the National Security Agency.

10. Did you attach a copy of the course justification and course syllabus that contains the changes you are requesting? NO  YES

11. Does this proposed change impact the assessment process of a program or certificate? If yes, then send notification to assessment@fiu.edu. NO  YES

PROPOSAL REQUESTED BY:

Faculty Contact	<u>Bogdan Carbutar</u>	<u>Bogdan Carbutar</u>	<u>11</u> / <u>6</u> / 20 <u>21</u>
	(Type name)	(Signature)	
	<u>carbutar@cs.fiu.edu</u>	<u>(305) 348-7566</u>	
	(Email address)	(Phone number)	
Chairperson (Dept./Div.)	<u>Jason Liu</u>	<u>Jason Liu</u>	<u>11</u> / <u>15</u> / 20 <u>21</u>
	(Type name)	(Signature)	
Chairperson (Curr. Comm.)	<u>Elias Alwan</u>		<u>    </u> / <u>    </u> / 20 <u>    </u>
	(Type name)	(Signature)	
College/School Dean	<u>John Volakis</u>		<u>    </u> / <u>    </u> / 20 <u>    </u>
	(Type name)	(Signature)	

Submit one original form. Attach one copy of the course justification and a draft of the course syllabus reflecting any changes requested in this Proposal for a Course Change. The syllabus should include the course description, objectives, learning outcomes, major topics, and textbooks. Where applicable, please ensure that the changes you are requesting are included in the syllabus and supporting documentation.

## MEMORANDUM

To: Mary Cossio  
Faculty Senate

From: Faculty Contact and KFSCIS Chair

Subject: **Memo in Lieu of Faculty Contact and School's Director Signatures for Bulletin #3**

Date: November 18, 2021

---

As instructed by the Faculty Senate, this memo will serve as approval of the attached proposals for Bulletin #3 by our Faculty Contact (Bogdan Carbunar) and KFSCIS Director (Jason Liu) in lieu of physical signatures. The proposals in this Bulletin were approved by our Curriculum Committee on (11/17/2021).

## MEMORANDUM

To: Mary Cossio  
Faculty Senate

From: Dean or Assoc. Dean and College Curriculum Committee Chair

Subject: **Memo in Lieu of Curriculum Chair and Dean Signatures for Bulletin #3**

Date: November 18, 2021

---

As instructed by the Faculty Senate, this memo will serve as approval of the attached proposals for Bulletin #3 by our Curriculum Committee Chair (Elias Alwan), and the Dean for College of Engineering and Computing (John L. Volakis), in lieu of physical signatures. The proposals in this Bulletin were approved by our Curriculum Committee on (11/17/2021).

In addition to the above, memos in lieu of signatures have also been included by departments unable to obtain physical signatures for their faculty contact and/or department chair.

## **Security and Privacy: Attacks and Defenses**

### **Course Justification**

Attackers increasingly target a broad spectrum of computing systems, while regular Internet users who access many remote, online services, become increasingly vulnerable to a variety of privacy vulnerabilities. Graduate students will benefit from understanding basic security and privacy attacks and defenses.

The Knight Foundation School of Computing and Information currently offers the Masters of Science in Cybersecurity program, with a suite of computer and network security courses. We need however to restructure the program to allow its later certification by the National Security Agency (NSA), to receive the National Centers of Academic Excellence (CAE) in Cybersecurity designation.

We are proposing the following restructuring of the course syllabus:

- Move previously covered topics of information security planning, policy, security management models to CIS-5370, whose syllabus we are also changing.
- Cover new topics that include NSA-required (1) cyber attacks and threat information sources, (2) attack detection and defenses, (3) privacy risks, (4) fair information practices, (5) privacy protection tools, and (6) security and privacy policies, laws, and regulations.

# Knight Foundation School of Computing and Information Sciences

**Course Title:** Security and Privacy: Attacks and Defenses

**Date:** 11/06/2021

**Course Number:** CIS-5374

**Number of Credits:** 3

<b>Subject Area:</b> Cybersecurity	<b>Subject Area Coordinator:</b> <b>email:</b>
<b>Catalog Description:</b> Introduction to cyber threats with a focus on attack types, along with their countermeasures, and privacy issues that include fair information practices, anonymity vs. privacy, risks, tracking and surveillance, tools, and policies.	
<b>Textbook:</b> None	
<b>References:</b> None	
<b>Prerequisites Courses:</b> None (M.S. or Ph.D. standing or permission of the instructor)	
<b>Corequisites Courses:</b> None	

Type: Required

Prerequisites Topics:

- Pre-college Mathematics

Course Outcomes: At the end of the course, students should be able to:

- O1. List various types of security attacks
- O2. Explain the concepts behind address spoofing, connection sniffing, spoofing and session hijacking
- O3. Describe password guessing and cracking techniques and tools
- O4. Understand and list various types of malware, including viruses, Trojan horses, backdoors, ransomware
- O5. Explain denial of service (DoS) and distributed denial of service (DDoS) attacks, bots, botnets
- O6. Describe web app attacks, 0-day exploits, advanced persistent threats
- O7. Master the concepts behind covert channels
- O8. Master the concepts behind social engineering attacks and insider attacks
- O9. Describe details of cyber attacks, including attack surfaces, vectors and tress, timing, and detection
- O10. List and describe threat information sources, e.g., AlienVault (Open Threat Exchange), Cisco's Talos Intelligence, VirusTotal, the Spamhaus project, DHS CISA Automated Indicator Sharing, FBI's InfraGard, SANS Internet Storm Center, and Google Alerts, Common Vulnerabilities and Exposures (CVE) database

O11 Outline defense concepts that include defense in depth, network hardening, intrusion detection (signature and anomaly based), moving target defense, cyber deception, and exposure minimization

O12. List, explain and describe various types of Personally Identifiable Information (PII) and assess impact of disclosure

O13. Understand the risks to privacy

O14. Explain tracking and surveillance

O15. Explain relationship and differences between anonymity (pseudonymity), security and privacy

O16. Describe Fair Information Practice Principles including transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, accountability and auditing

O17. Master the concepts behind privacy protection tools that include VPNs, mix-nets (scramblers), pseudonymization, secure multi-party computation, and cryptocurrencies

O18. Understand legal issues associated with cyber threats

O19. List and describe privacy policies, laws and regulations

### Outline

Topic	Lecture Hours	Outcome
Introduction <ul style="list-style-type: none"> <li>• Background of security and privacy</li> <li>• Basic concepts</li> </ul>	6	O1, O12, O13, O14, O15
Cyber attacks	12	O2 – O8
Attack detection and defenses	6	O9, O10, O11
Fair Information Practices	3	O16
Privacy Protection Tools	6	O17
Policies, laws and regulations	3	O18, O19

### Grading Policy

- Midterm: 30%
- Final Exam: 30%
- Assignments: 30%
- Participation: 10%