DO NOT TYPE IN THIS BOX

Bulletin #: _____

Academic Year: _____

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 Sciences

2. | CNT | 4 | 403 | | 3 |
   |---|---|---|---|---|
   | **Alpha Prefix** | **1st Digit** | **Last 3 Digits** | **"C"-lec-lab "L"-Lab** | **Cr. Hrs.** |

3. **Present Course Title** Computing and Network Security

PART II. FILL OUT CHANGE INFORMATION ONLY

Change Effective 8 / 24 / 20 19

4a. **New Course Title** _____

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

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):** (COP-3804 or COP-3337 or COP-2270) and CGS-3767

8. **New Corequisite(s):** CGS-4285

9. **Explain Reclassification Request:**

   SCIS is adding a new BS-in-Cybersecurity program that requires COP-2270. Hence this proposal is to include COP-2270 in the prerequisite list and CGS-4285 as a coreq to reduce prereq chain length...

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 Nagarajan Prabakar _____ / _____ / 20 19
(Type name) **(Signature)**

prabakar@cis.fiu.edu 305-348-2033
(Email address) **(Phone number)**

Chairperson (Dept./Div.) S.S. Iyengar _____ / _____ / 20 19
(Type name) **(Signature)**

Chairperson (Curr. Comm.) Wei-Chiang Lin _____ / _____ / 20 19
(Type name) **(Signature)**

College/School Dean John Volakis _____ / _____ / 20 19
(Type name) **(Signature)**

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

CNT-4403 Computing and Network Security

Course Change Justification

SCIS is adding a new BS-in-Cybersecurity program that requires C programming knowledge. For this reason, the revised COP-2270 (Secure Programming in C for Engineers) will be a required course for this program.

Since CNT-4403 is also a required course for this program, and C programming will prepare students well for CNT-4403, we propose to change the prerequisite for CNT-4403 by including COP-2270 in the prerequisite list. Furthermore, with CGS-4285 (Applied Computer Networking) as a corequisite, the prerequisite chain length will be reduced that will improve the graduation rate.

School of Computing and Information Sciences

Course Title: Computing and Network Security **Date:** 9/29/19

Course Number: CNT 4403

Number of Credits: 3

Subject Area: Security	**Subject Area Coordinator:** Nagarajan Prabakar **email:** prabakar@cs.fiu.edu
Catalog Description: Fundamental concepts and principles of computing and network security, symmetric and asymmetric cryptography, hash functions, authentication, firewalls and intrusion detection, and operational issues.	
Textbook: "Principles of Computer Security: Security+ and Beyond" by Wm. Arthur Conklin, et al. McGraw Hill Higher Education (ISBN: 0072255099)	
References: "Introduction to Computer Security" by Matt Bishop Addison Wesley (ISBN: 0321247442)	
Prerequisites Courses: (COP 3804 or COP 3337 or COP 2270) and CGS 3767	
Corequisites Courses: CGS 4285	

Type: Required

Prerequisites Topics:

- Java programming
- Fundamental concepts of operating systems
- Shell scripting
- Basic network concepts, including TCP/IP

Course Outcomes:

1. Be familiar with basic concepts in information security
2. Master the concepts related to applied cryptography, including symmetric cryptography and asymmetric cryptography
3. Be familiar with public key infrastructure
4. Master the theory and common types of access control
5. Master the key factors involved in authentication
6. Be familiar with runtime communication techniques such as intrusion detection systems
7. Be familiar with policy and operational issues in security
8. Be exposed to vulnerabilities, attacks, auditing, and forensics

School of Computing and Information Sciences
CNT 4403
Computing and Network Security

Outline

Topic	Number of Lecture Hours	Outcome
• Basic security concepts o Security services: confidentiality, integrity, availability, etc o Design principles o System/security life-cycle o Security implementation mechanisms o Information assurance analysis model	3	1
• Cryptography o Symmetric cryptosystems o Asymmetric cryptosystems o Hash functions o Digital signatures	8	2
• Access control o Access control matrix model o Discretionary access control (DAC) o Mandatory access control (MAC) o Role-based access control (RBAC)	4	4
• Authentication o Password o Challenge-response o Biometric o Two-factor authentication	4	5
• Trusted intermediaries o Public key infrastructure (PKI) o Certification authorities	3	3
• Runtime communication security o Firewall o Auditing o Intrusion detection	4	6
• Operational issues o Disaster recovery o Legal issues	3	7
• Policy o Creation and maintenance of policies o Prevention o Avoidance	3	7
• Attacks o Social engineering o Denial of service o Protocol attacks	3	8

○ Active and passive attacks ○ Malware		
• Miscellaneous topics ○ Forensics ○ Web security and vulnerabilities	4	8

School of Computing and Information Sciences
CNT 4403
Computing and Network Security

Course Outcomes Emphasized in Laboratory Projects / Assignments

	Outcome	Number of Weeks
1	Cryptography and PKI Outcomes: 2, 3	3
2	Authentication Outcomes: 1, 5	2
3	Access control Outcomes: 4, 7	2
4	Runtime communication security Outcomes: 6	3
5	Attacks and vulnerability analysis Outcomes: 8	1

Oral and Written Communication: No significant coverage

Number of written reports:

Approximate number of pages for each report:

Number of required oral presentations:

Approximate time for each presentation:

Social and Ethical Implications of Computing Topics

No significant coverage

Topic	Class time	Student performance measures

School of Computing and Information Sciences
CNT 4403
Computing and Network Security

Theoretical Contents

Topic	Class time
Cryptography	0.6
Access control model	0.1

Problem Analysis Experiences

1.

Solution Design Experiences

1. Design of access control policy for a given system