

# TCN 4081—Telecommunications Network Security

Department of Electrical & Computer Engineering  
Florida International University  
Fall 2018

<b>Classroom</b>	:	EC 2940
<b>Class Time</b>	:	8:30 pm—12:30 pm
<b>Faculty</b>	:	Dr. Alexander Pons
<b>Office Hours</b>	:	M & W 9:00-11:00 am or by Appointment
<b>Office</b>	:	EC - 3145
<b>Phone</b>	:	305.348.7253
<b>Email</b>	:	apons@fiu.edu
<b>Prerequisite</b>	:	TCN 4211 or Permission from the Instructor
<b>Textbook</b>	:	Mark Ciampa, Security+ Guide to Network Security Fundamentals, Fifth Edition. Course Technology, Cengage Learning, 2015, ISBN 13: 978-1-305-09391-1
<b>Reference Textbook</b>	:	William Stallings, Cryptography and Network Security Principles and Practice, Sixth Edition, Pearson, 2014, ISBN 13:978-0-13-335469-0

## Course Description

This course is intended to provide students with the security aspects that are associated with various types of networks. It provides an introduction to the fundamentals of network security, including compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; and cryptography. The course covers new topics in network security as well, including psychological approaches to social engineering attacks, Web application attacks, penetration testing, data loss prevention, cloud computing security, and application programming development security. Students will also engage in activities that link to the Information Security Community Site. The students will be exposed to Number Theory, Steganography, Encryption Design Principles and Algorithms, Message Authentication and Digital Signature Principle and Designs, and Network System Security Design. This course offers a comprehensive guide for anyone wishing to take the CompTIA Security+ SY0-301 Certification Exam.

## **Course Objectives**

1. Describe many of the vulnerabilities associated with network attacks
2. Identify Malware and Social Engineering Attacks
3. Conduct Vulnerability Assessment and Attack Mitigation
4. Determine the requirements for Wireless network security
5. Describe and use various Cryptographic methods
6. Apply concepts in Number Theory in cypher techniques
7. Use the concept of Steganography to hide information in different mediums

## **Topics Covered**

1. Introduction to Security
2. Security Life-Cycle
3. Cybersecurity Principles (reduce trust area and relationships)
4. Malware and Social Engineering Attacks
5. Application and Network Attacks
6. Vulnerability Assessment and Mitigating Attacks
7. System modeling techniques
8. Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security)
9. Host, Application, and Data Security
10. Network Security
11. Layer 2/Layer 3 security issues and Ipsec
12. Administering a Secure Network
13. Wireless Network Security
14. Access Control Fundamentals
15. Authentication and Account Management
16. Number Theory
17. Basic Cryptography
18. Advanced Cryptography
19. Business Continuity
20. Risk Mitigation

## **Relationship of course to program objectives**

In this course, the student will have to show:

1. An ability to apply knowledge of mathematics, science, and engineering,
2. an ability to design and conduct experiments, as well as to analyze and interpret data,
3. an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability,
4. an ability to identify, formulate, and solve engineering problems (homework),
5. the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context
6. an ability to communicate effectively (through teamwork),

7. an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice,
8. a knowledge of contemporary issues,
9. a knowledge of advanced mathematics.

### Tentative Grading Scale

Grading Scale:		
A	93-100	"Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of ideas, and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions, as outlined in the Student Handbook."
A-	90-92	
B+	87-89	
B	83-86	
B-	80-82	
C+	77-79	
C	73-76	
D	63-66	
F	< 62	

### Grading Scheme

Attendance (Mandatory)	5%
In-Class Assignments (every chapter)	10%
<b>Group Research Paper/Project</b>	25%
Midterm	30%
Final Exam	30%
<b>Total</b>	<b>100%</b>

### Tentative Dates

- **Final Exam** is scheduled on the last Saturday of the semester.
- **Group Presentations** will also be done on the last Saturday of the semester

### **Group Research/Project Paper**

1. The course includes a substantial group project (25%) requiring the review and the implementation of a topic related to Network Security.
2. The group contains 3-4 students working together throughout the semester.
3. Students will give oral presentations and show their demos on the last day of the class.

### University's Code of Academic Integrity

Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of

ideas, and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational Mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions, as outlined in the Student Handbook.

More information can be found at [http://academic.fiu.edu/academic\\_misconduct.html](http://academic.fiu.edu/academic_misconduct.html)

## Department Regulations Concerning Incomplete Grades

To qualify for an Incomplete, a student:

1. Must contact (e.g., phone, email, etc.) the instructor or secretary before or during missed portion of class.
2. Must be passing the course prior to that part of the course that is not completed
3. Must make up the incomplete work through the instructor of the course
4. Must see the Instructor. All missed work must be finished before last two weeks of the following term.

## University policies on sexual harassment, and religious holidays, and information on services for students with disabilities

Please visit the following websites:

<http://academic.fiu.edu/>

<http://drc.fiu.edu>

## Course Policies

- **Attendance:** Attendance in the course is **mandatory** and student is not allowed to miss any class during the semester. There will be a **penalty** for missing classes and it may affect your final grade.
- **Academic Misconduct:** For work submitted, it is expected that each student will submit their own original work. Any evidence of duplication, cheating or plagiarism will result at least a failing grade for the course.
- **Unexcused Absences:** Two unexcused absences are permitted during the term. More than two will result in the loss of points from your final grade. (1 point per absence above two, 3 points per absence above 5).
- **Excused Absences:** Only emergency medical situations or extenuating circumstances are excused with proper documentation. After reviewing documentation you are required to email a description of the excuse and absence dates as a written record to [aons@fiu.edu](mailto:aons@fiu.edu).
- **On Time:** As in the workplace, on time arrival and preparation are required. Two “lates” are equivalent to one absence. (Leaving class early is counted the same as tardy.)
- **Deadlines:** Assignments are due at the beginning of the class period on the date specified. Assignments submitted late (within 1 week) will receive half credit.
- To get assistance try to see me by an appointment.

- Students are encouraged to ask questions and to discuss course topics with the instructor and with each other.
- **Any work submitted should display Panther ID number and should be signed, as the students' own work, and that no unauthorized help was obtained.**
- Cell phones, communicators, MP3 players, head sets are not allowed to be used in the class.
- **DO NOT** send assignments by email.
- Instructor reserves right to change course materials or dates as necessary.

## Exam policy

1. Make sure to complete the assigned homework in order to do well in the exam.
2. All exams are closed book and closed notes.
3. Use of any electronic device with keyboard is prohibited. This also applies to cellphones with messaging system.
4. No discussion is permitted during the exams.
5. Instructor is not compelled to give credit for something he cannot read or follow logically.
6. Cheating is considered as a serious offense. Students who are caught will receive the appropriate consequences.

## Class Schedule

Once a week, 240 minutes each session: Saturdays

Class Schedule:

Week	Date	Weekly Topic
1	10/25/2014	Chapter 1: Introduction to Security Chapter 2: Malware and Social Engineering Attacks
2	11/1/2014	Chapter 3: Application and Network Attacks Chapter 4: Vulnerability Assessment and Mitigating Attacks Chapter 5: Host, Application, and Data Security
3	11/8/2014	Exam 1 Chapter 6: Network Security
4	11/15/2014	Chapter 7: Administering a Secure Network Chapter 8: Wireless Network Security Chapter 9: Access Control Fundamentals
5	11/22/2014	Exam 2 Chapter 10: Authentication and Account Management Chapter 11: Basic Cryptography
6	11/29/2014	Chapter 12: Advanced Cryptography Handout: Types of Ciphers/Deciphers
7	12/6/2014	Chapter 13: Business Continuity Chapter 14: Risk Mitigation
8	12/13/2014	Course Final Exam <b>Group/Paper Presentations</b>