Course Code	Course Title
COMP 3632	**Principles of Cybersecurity**

Course Description

This course is an introduction to the principles of cybersecurity. Cybersecurity, also called computer security or IT security, refers to the study of techniques to protect computing systems from attacks that threaten data confidentiality, system integrity and availability. By modeling, analyzing, and evaluating the security of computer systems, students will learn to find weaknesses in software, hardware, networks, data storage systems, mobile applications, and the Internet, and identify current security practices and defenses to protect these systems.

List of Topics

Topic
Introduction; Security Mindset
Classic Crypto
Symmetric Key Crypto 1
Symmetric Key Crypto 2
Public Key Crypto 1
Public Key Crypto 2 & Hash Function
Reverse Engineering
Holiday; No Class
Malware
Software Exploitation : Buffer Overflow | ROP Attack Example.
Software Exploitation : Others
Software Protection : Obfuscation
Software Security Analysis : Dynamic Vulnerability Detection
Software Security Analysis: Static Vulnerability Detection
mid-term exam TBA

Topic
Industry Perspective on Computing Security (Guest Lecture: Prof. Ricci IEONG)
Side Channel
Authentication: Password & Biometrics
Network Security
Authorization
Protocol
System Security
Blockchain
Web Security (Guest Lecture: Prof. Wei Meng)
Smart Contract | Internet of Things (Short)
Machine Learning Security
Final

Textbooks (Optional)

Information Security: Principles and Practice

Introduction to Computer Security

Reference books

N/A

Grading Scheme

In-class quizzes	5%
Hacking practice	5%
Assignments (~4)	40%
Midterm exam	20%
Final exam	30%

Total	100%

Course Intended Learning Outcomes

1. State and describe the underpinning principles of cybersecurity and relate them to past and ongoing events
2. Apply cybersecurity principles to recognize vulnerabilities in computer systems, including protocols, hardware, and software.
3. identify and implement effective defenses for computer systems against potential cybersecurity attacks.
4. Study and understand cybersecurity protections and attacks on networks, databases, financial systems and operating systems.
5. Understand how to design and apply business continuity plans, incidence response plans, and cybersecurity risk analysis to enforce cybersecurity best practices in business.

Assessment Rubrics

N/A