CYBERSECURITY (CYB)

CYB 611 Introduction to Cybersecurity (3 credits)
This course is to introduce the fundamental concepts in cybersecurity. The courser will first introduce the vulnerabilities of computer systems and networks and then lead students to understand the fundamental principles in security using cases and examples. Various risk management strategies for organizations will then be introduced. In addition, the course will introduce methods to identify the potential threats from inside and outside of an organization and to deploy security technologies to mitigate the threats. Privacy, ethical and legal issues related to cybersecurity will be discussed. Students will gain hand-on experience by investigating security problems through laboratory exercises.
Course Rotation: NYC & PLV: Fall

CYB 613 Operating Systems Theory and Administration (3 credits)
Operating systems (OS) provide the platform on which running software acquires and uses computing resources. OS are responsible for working with the underlying hardware to provide the baseline security capabilities of a system. Understanding the underlying theory of operating system design is critical to cybersecurity as operating systems control the operation of a computer and the allocation of associated resources. This course is to provide students with an understanding of the roles of an operating system, its basic functions, and the services it provides. Through lab exercises, this class will also identify the key issues and functions in administrating a Linux operating system.
Course Rotation: NYC & PLV: Fall

CYB 621 Information Security Mangemnt (3 credits)
This course introduces students to methods and practices to develop policies and plans for managing personnel, systems and processes related to information security in an organization. This course will first introduce methods to identify information assets, prioritize threats to information assets, and define an information security strategy and architecture. The course will then introduce methods and practices to develop system specific plans against various threats. Most importantly, students will learn about legal and public relations implications of security and privacy issues. Last but not the least, the course will present a disaster recovery plan for recovery of information assets after cybersecurity incidents.
Course Rotation: NYC & PLV: Spring

CYB 623 Network Security and Defense (3 credits)
This course will introduce the students to an overall view of network security and the latest defense techniques and strategies known in the enterprise. Starting with understanding network elements and architecture to how to identify and understand the different vector of attacks on a network.
This includes sampling forensics and understanding the new concept of threat intelligence. Students will understand risk assessment and risk management for different components of the network and the impact of the different kinds of threats and attacks. In addition, the course will elaborate on the essentials of how to design, architect a secure enterprise network and how to define security policies, and how-to police it using intrusion detection/ prevention systems. The course is mainly a hands-on all along from examining network security, learning how to attack a network, and learn how to defend it. Policy design and enforcement lab as well as IDS/IPS set up and configuration.
Course Rotation: NYC & PLV: Spring

CYB 625 Ethical Hacking and Penetration Testing (3 credits)
This course will introduce students to cybersecurity operations which includes understanding of the cyberspace in the enterprise. Ethical hacking and penetration testing are at the center of cybersecurity operations. What are the common vulnerabilities and threats to web applications whether front the front-end (browser side) or the back-end (Server-side). All aspects of penetration testing and how to use it in order examine the security of online operation. The importance of data security and the different attacks on databases. Also, the course will illustrate the use of Identity and access management to enforce security and governance. This is a hands-on class, as it will use secure VPN to teach the students about the different topics in a lab environment. In addition, students will the arsenal of offensive security tools comes with Kali Linux to apply and examine the topics taught in class.
Course Rotation: NYC & PLV: Fall

CYB 631 Automating Information Security with Python and Shell Scripting (3 credits)
This course is designed to acquaint students interested in learning about system administration using tools such as Python and PowerShell. No prior experience in either is required, and a good deal of time will be spent introducing students with topics of general interest and their coding equivalents using these tools. Students will be introduced to topics such as Python and PowerShell automation, NSA Top 10 Mitigations, CIS Critical Security Controls, MITRE ATT&CK mitigations, application of the NSA/DISA Secure Host Baseline, deployment and managing PKI and smart cards.
Course Rotation: NYC & PLV: Fall

CYB 633 Malware Analysis and Reverse Engineering (3 credits)
This course provides fundamental knowledge of secure software development methodologies and applied security topics related to compiled programs. In-depth coverage of source code auditing, fuzzing, introduction to reverse engineering, and exploitation will be emphasized.
Course Rotation: NYC & PLV: Fall

CYB 651 Cyber Intelligence Analysis & Modeling (3 credits)
This course introduces students to identify the sources of cyber intelligence, including open source information, system logs/files, dark web forum, etc. In addition, the course will guide students to analyze these information to gain insights in solving cybersecurity problems using methods and techniques from textual analysis, data mining and machine learning.
Course Rotation: NYC & PLV: Spring

CYB 691 Cybersecurity Capstone Project (3 credits)
This capstone course focuses on research projects in cybersecurity. The goal of the capstone course is to provide an opportunity for students to incorporate cybersecurity knowledge and skills learned from previous courses and apply them to a real-world project. The project can come from a student's internship experience, as an extension of a previous research project, or a project with an external client, such as a faculty or an industry expert. Students are expected to work in a team setting to plan, analyze and design a solution to the problem being explored in the project.
Course Rotation: NYC & PLV; Spring