PACE UNIVERSITY | Seidenberg School of Computer Science and Information Systems

MS IN CYBERSECURITY CURRICULUM

PROGRAM REQUIREMENTS

To complete the program, a student will need to complete 10-13 courses (30-39 credits) depending on the number of bridge courses that the student needs. Whether a student is required to complete bridge courses will depend on their previous academic transcripts. A typical student who does not need bridge courses can complete the program requirements in three semesters if the student takes about 3-4 courses per semester.

In additional to required courses, the program provides two optional concentrations: Cyber Operations and Cybersecurity Leadership. Cyber Operations focuses on the technical aspect of protecting computing systems, reconnaissance, and exploitation in the cyber space. Cybersecurity Leadership prepares students for cybersecurity leadership roles such as Chief Information Security Officers who are well-versed with technology, policy, risk management, and governance. Students who do not focus on either concentration will choose elective courses from a list of curated cybersecurity related topics.

Course Name		Credits
Bridge Courses (0-9 credits)		
CS601C or Equivalencies	Computational Statistics	3
IS612, CS502 or Equivalencies	Introduction to Coding or Fundamental Computer Science I Using Java	3
IS632 or Equivalencies	Business Telecommunications	3
Required Courses (18 credits)		
CYB611	Introduction to Cybersecurity	3
CYB613	Operating Systems: Theory and Administration	3
CYB621	Information Security Management	3
CYB623	Network Security and Defense	3
CYB625	Ethical Hacking and Penetration Testing	3
CYB691	Cybersecurity Capstone Project	3
Cyber Operations Concentration (0-9 credits)		
IT670	Mobile Forensics	3

CS608	Algorithms and Computing Theory	3
CYB633	Malware Analysis and Reverse Engineering	3
Cybersecurity Leadership Concentration (0-9 credits)		
IS642	Information Security Planning and Policy	3
IS643	Information Security Auditing and Risk Management	3
IS644	Business Continuity and Disaster Recovery Planning	3
Elective Courses (3-12 credits)		
CYB631	Automating Information Security with Python and Shell Scripting	3
CYB651	Cyber Intelligence Analysis and Modeling	3
IT662	Web and Application Security	3
IT664	Computer Forensics	3
IS647	Legal Issues in Information Systems	3
IS613	Database Management Systems	3
IS665	Data Warehousing, Data Mining and Visualization	3
IS678	Location Analytics and Web GIS	3
CS610	Introduction to Parallel and Distributed Computing	3
CRJ601	Introduction to Homeland Security	3
CRJ604	U.S. Constitution and Ethical Issues	3
Program Total		**30-39 Credits**

COURSE DESCRIPTIONS

Required Courses

CYS611 Introduction to Cybersecurity

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.

CYB613 Operating Systems: Theory and Administration

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.

CYB621 Information Security Management

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.

CYB623 Network Security and Defense

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.

CYB625 Ethical Hacking and Penetration Testing

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.

CYB691 Cybersecurity Capstone Project

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.

Required Courses for Cyber Operations Concentration

These courses can also be taken as electives without the concentration.

IT670 Mobile Forensics

The field of mobile forensics has expanded exponentially over the past few years as more of our lives are captured on smartphones and other mobile devices. This course will provide students with an overview of cellular networks and the various devices that operate on these networks. Moreover, an in-depth analysis of the file systems and operating systems, including iOS and Android platforms will be explained. Students will have to opportunity to use professional mobile forensic tools utilized to examine mobile telephones, SIM cards, media cards and synced data on paired computers in a forensic manner. The course will introduce students to professional investigative techniques, legal procedures and reporting standards necessary to build a successful case. Other topics in the course will include investigations involving tablet computers, digital cameras, multimedia players and Global Positioning System (GPS) electronics.

CS608 Algorithms and Computing Theory

The purpose of this course is to acquire a thorough grounding in the core principles and foundations of computer science. Students will learn methods for expressing and comparing algorithm complexity (worst- and average-case upper bounds, lower bounds) as well as to verify correctness. Algorithm-design techniques (divide-and-conquer, dynamic programming) as well as data structures (trees, heaps, hash tables) widely used in modern software development will be studied. The knowledge gained will be applied to a variety of practical problems, such as searching, sorting, and graph problems (shortest paths, minimum spanning trees). The question of what problems are hard to compute will be addressed with an introduction to NP-completeness theory, including the

development of the NP-complete classification and the identification of NP-hard problems by reductions.

CYB633 Malware Analysis and Reverse Engineering

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.

Required Courses for Cybersecurity Leadership Concentration

These courses can also be taken as electives without the concentration.

IS642 Security Planning and Policy: NIST Standards

The United States government requires all federal systems to have a customized security plan. In addition, the National Training Standard for Information Systems Security (INFOSEC) Professionals requires programs that meet this standard to produce students capable of developing a security plan. This course provides an introduction to security planning as recommended by NIST guidelines on developing security plans. The student is required to conduct a case study where a security plan is developed for a fictitious or real small size organization. The purpose of this course is to provide an overview of the security requirements on existing computing environment and describe the controls in place or planned for meeting those requirements. The security plan presents all managerial, operational, and technical controls an organization will need in the next three years.

IS643 Security Auditing and Risk Management

This course provides an introduction to security auditing based on the ISO 27000 family of standards. In addition to risk management, the course also presents both nominal security audit based on ISO 27002 and technical security audit based on ISO 27001. Each student is required to conduct a case study where he/she performs security audit for a fictitious or real small-size organization. Security Audit programs contain about a dozen security areas of audit focus, performed by either an external or internal auditor, who aims at validating the compliance of the Information Technology Organization as well as the enterprise at-large to the ISO 27000 Series, as well as Sarbanes-Oxley, HIPAA, and PCI-DSS.

IS644 Business Continuity and Disaster Recovery Planning

Recent events in this world have increased the need for organizations to develop strategies for mitigating, preparing for, responding to, and recovering from small and large scale emergencies. In the context of a highly integrated global economy, nearly every business is likely to feel the effects of emergencies around the world, and in the face of intense competition, it is crucial that all businesses have a plan for continuing operations before, during, and after emergencies of all types. This course presents an introduction to business continuity and disaster recovery planning. It includes a comprehensive advanced business continuity planning and management workshop which is designed to teach practical methods to develop, test, and maintain a business continuity plan. In addition to ISO 22301 and the BS 25999 business continuity standards, this course is based on industry best practices and guidelines for business continuity, disaster recovery, and emergency management.

Elective Courses

CYB631 Automating Information Security with Python and Shell Scripting

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.

CYB651 Cyber Intelligence Analysis and Modeling

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.

IT650 Computer Forensics

This course provides a general overview of the theory and application of information warfare and forensic computing. The background information on information warfare highlights the inherent problems in today's computing environment and indicated the necessity of forensics to complement computer security. The course focuses on information warfare arsenal and tactics, defensive strategies, and causalities; network surveillance tools for information warfare; fundamentals of computer forensics; computer forensics services and technologies; search and seizure; data recovery and identification and digital evidence collection, duplication, and preservation; computer

image verification and authentication; reconstruction of past events; legal issues; and advanced topics in forensics.

IS647 Legal Issues in Information Technology

The course will introduce the student to the legal and regulatory environment of computer technology, especially issues concerning the Internet. The course will introduce and familiarize students with the law subjects concerning business activities particularly as they relate to computer technology. In addition, the course will state the international and ethical dimensions where appropriate. Last but not least, the course will discuss how the students can assist business entities to avoid and minimize exposure to litigation.

IS613 Database Management Systems

This course is an introduction to database management systems and deals with the logical and physical organization of databases. Areas to be included are database management systems (DBMS), database query languages (SQL), relational model and database modeling (ERD), normalization, database administration and advanced database topics, etc. MS Visio will be used for ERD data modeling. Microsoft Access, and/or Oracle, SQL Server will be used for building database and practice SQL.

IS665 Data Warehousing, Data Mining and Visualization

This course provides a foundation for learning the basic concepts of data mining, data warehousing and visualization. The course focuses on distinctly “real -world” orientation that emphasizes application of data analysis over algorithm design and development in most topic areas. The course pre-requisites are understanding database concepts and familiarity with information or business decision systems.

IS678 Location Analytics and Web GIS

Geographic information systems are have become a necessary tool in decision making, visualization, and spatial analytics across a variety of disciplines and application domains. This course explores emerging cloud based GIS technology, location analytics, and web-based GIS solutions. Through hands on projects, students will used web-based data, build web GIS applications, use cloud-based services for location analytics, mobile applications and field collection applications.

CS610 Introduction to Parallel and Distributed Computing

Parallel computing theory: Parallel Random-Access Machines (PRAMs), Amdahl’s law for theoretical speedup limits, Petri Nets; parallel vs. distributed computing: speedup, fault-tolerance, resource-sharing; parallel architectures; data flow, instruction-level pipelining, embedded multicore systems, shared-memory, multiprocessors, distributed-memory

multicomputers, interconnection networks, distributed systems: client-server systems, cluster computing, computing grids, cloud computing; parallel and distributed programming with industry standard MPI (Message Passing Interface); and parallel algorithms.

CRJ 601 Introduction to Homeland Security

Introduction to Homeland Security is foundational to the remainder of the curriculum in the Master of Arts in Management for Public Safety and Homeland Security Professionals. This course is designed for people who have been identified as current and future leaders in homeland security. The course provides a basic overview of the ideas that can help leaders think and act more strategically. It also introduces many of the subjects that will be covered in other courses in the master's program. The course provides students with an overview of the purposes of homeland security and how resources can be managed to engage the risks and opportunities of the homeland security field. Successful completion of this course is required for continuation in the master's program.

CRJ 604 U.S. Constitution and Ethical Issues

This course is designed to provide students with a hands-on chance to grapple with many complicated constitutional and ethical issues that practitioners will encounter in developing strategies to secure the nation in all situations, such as in routine activities for responding to terrorist attacks, natural disasters, etc. The course is structured to give students an opportunity to interact in groups, discuss constitutional case studies, and debate legal/moral/ethical dilemmas that will constantly arise. Special attention will be given to due process concerns.