MASTER OF SCIENCE IN CYBER SECURITY

Specialization **Security of Information and Communication Systems**

The Master of Science in Cyber security program is designed to meet the high demand for Cyber security professionals in both the public and private sectors. The program focuses on network and software security, risk management, protection mechanisms, business continuity planning, disaster recovery, and governance of information systems.

The graduates from the program can apply these skills to protect resources in the cyber domain and work as senior cybersecurity professionals in various sectors of industry that have significant online resources.

NURE's Master of Science in Cyber Security will enable you to:

- Develop, evaluate, and communicate information and physical security policies, standards, and guidelines.
- Design, implement, and deploy cybersecurity solutions for protecting an organization's information resources. Identify the appropriate cryptographic algorithms and protocols to be deployed in the context of an organization's security policy.
- Assess the security vulnerabilities of an organization's networks against cyber adversaries. Design and implement secure software. Design and implement appropriate incident response and handling procedures in case of a security breach.
- Adapt to a dynamic multidisciplinary technological environment through teamwork, ethical concerns, and effective communication.

CORE MODULES:

The following modules are indicative of what you will study on this specialization.

Secure Communications

Security principles for communication networks. Common attacks to communication networks. Countermeasures. Ethernet networks. Attacks and defences. Authentication, Authorization and Accounting (AAA). Security in other applications: remote execution, file transfer, network file systems. Wireless Security and the IEEE 802.11 Standards.

Network Security

Risk management and the vulnerability lifecycle of software and networked services are discussed. Threats like denial of service, spam, worms, and viruses are studied in-depth. State of the art technologies like secure shell, network and transport layer security, intrusion detection and prevention systems, cross-site scripting, secure implementation techniques and more for securing the Internet and web applications are presented.

Data/Database Security

This module introduces the concept of database security to include: Database Architecture, Password Policies, Auditing, Privileges, and Roles Administration. Emphasis is placed on areas unique to data and database security.

Security Architecture and Design

This module provides an introduction to the fundamental components of security architecture. Topics include computer organization; hardware, software and firmware components; open and distributed systems; and protection mechanisms.

Cybersecurity Governance & Management

Introduction to cybersecurity. Attacks, threats and security incidents. Risk management, countermeasures & security assessment. New trends in cybersecurity: Internet of things, Cloud computing, and Big Data. Standards and Best Practices: ISO 27001.

IT, Cybercrime & Response

Monitoring and intrusion detection systems. Pentesting and system exploitation. Profiles and roles: access and control authentication. Software engineering and project management. Malware analysis. Forensic investigation.

Research Methods

This module is shared with other MSc courses run by the Department. Its main focus is on introducing you to research, and developing the skills you need to read and evaluate original research literature.

Resources, opportunities

The quality of our teaching and learning environment is obvious not only within courses, but also in resources for high-quality education provided by our University. The educational process takes place in the computer classes, laboratories, which are equipped with up-to-date technics. Students work with telecommunication and computer equipment of such companies as: Intel, Cisco.

JOBS & CAREERS

The roles and job titles in the security sector often involve somewhat overlapping responsibilities, and can be broad or specialized depending on the size and special needs of the organization. As the cybersecurity domain expands and develops further, new roles and titles are likely to emerge, and the roles attributed to the current titles will likely crystallize or evolve.

Jobs in the field of information security: Security Specialist; Security Analyst; Security Engineer; Security Consultant; Security Auditor; Security Manager; IT Project Manager; Security Architect; Security Director; Cryptographer; Cryptanalyst, Forensics Analyst, Source Code Auditor, Penetration Tester, Vulnerability Assessor, Forensics Expert.

IT jobs that can lead to cyber security careers include: Computer Software Engineer, Database Administrator, Network Administrator, Network Engineer, System Administrator, Web Administrator.