Module 2. Security Threats and Countermeasures

Module Learning Objectives

Based on the understanding of the fundamentals of security established in module 1, students will learn in more details about cyber attacks as well as the mechanisms and implementation of effective countermeasures in this module.

Module Student Learning Outcomes

Upon completion of this module, students will be able to:

- Describe different types of attack vectors in detail.
- Enumerate different types of cyber crimes.
- Explain major types of countermeasures.
- Describe approaches to safeguard key components of a typical IT infrastructure.
- Demonstrate understanding of the basics of cryptography.
- Accurately explain the key elements in public key infrastructure.

Module design:

Submodule 1: Security Threats
• Attack Vector & Attack Surface *Common attacks (attacks by target and by method)*
• Common Types of Attack Vectors
• Types of cyber crimes *Intrusions, Ransomware, Espionage, Intellectual Property, Fraud and Financial, Cyber Stalking and Predators, Cyber Bullying, Sexual Exploitation, Identity Theft, Cyber Assisted Crimes, Cyber Terrorism*
Submodule 2: Introduction to Cryptography
• Common cryptographic uses *Security Functions (data protection, data integrity, authentication, non-repudiation)* *Block Vs Stream Data* *Digital Signatures (Authentication)*
• Cryptography basics *Hash Functions (MD4, MD5, SHA-1, SHA-2, SHA-3)—Integrity checking, for protecting authentication data, collision resistance* *Symmetric Cryptography (DES, Twofish)*
• Lab: Cryptography basics
• Applications of cryptography and PKI *Public Key Cryptography (Diffie-Hellman, RSA, ECC, ElGamal, DSA)—Public Key Infrastructure, Certificates, Key management (creation, exchange/distribution)* *Cryptography in practice--Common Cryptographic Protocols, DES -> AES (evolution from DES to AES), Cryptographic Modes (and their strengths and weaknesses), Cryptographic standards (FIPS 140 series)* *Cryptographic Failures--Types of Attacks (brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.) Implementation failures*