CT437

Computer Security & Forensic Computing

Name: Andrew Hayes
Student ID: 21321503
E-mail: a.hayes18@universityofgalway.ie

2025–01–15

Contents

1 Introduction

1.1 Lecturer Contact Information

- Name: Dr. Michael Schukat.
- E-mail: michael.schukat@universityofgalway.ie.
- Office: CSB-3002.

1.2 Marking

- 2 hours of labs per week from Week 03.
- 30% Continuous Assessment consisting of 2 assignments, in-class quizzes, & lab worksheets.
- In-class quizzes will be open-book Canvas MCQs consisting of 5 randomised questions out of a pool of 20+ questions. One question is presented at a time, there is no back-tracking allowed. 5minutes duration.
- 70% exam.

1.3 Cybersecurity versus Computer Security

Cybersecurity is the practice of protecting systems, networks, & programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Computer security is a historically older term coined at a time when the focus was on individual stand-alone computers rather than entire systems.

Computer forensics is a branch of digital forensic science pertaining to evidence found in computers & digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analysing, and presenting facts & opinions about the digital information.

1.4 Definitions, Terminology, & Case Studies

Computer security, cybersecurity, or information technology security (IT security) is the protection of computer systems & networks from the theft or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. The protection can be on a personal, organisational, or government level. Protection from cybercrime of data (from theft or manipulation) and services (from disruption or misuse).

1.4.1 States of Data

- **Data at rest** refers to data stored in memory or on a permanent storage device such as a hard drive, solid-state drive, or USB drive.
- **Data in process** refers to data that is being used to perform an operation such as updating a database record.
- **Data in transit** refers to data travelling between information systems, e.g., data transfer over a network via TCP/IP.

1.4.2 How to Provide Protection?

- **Awareness, training, & education** are the measures put in place by an organisation to ensure that users are knowledgeable about potential security threats and the actions they can take to protect information systems.
- **Technology** refers to the software & hardware-based solutions designed to protection information systems such as firewalls, which continuously monitor your network in search of possible malicious incidents.

- **Policy & procedure** refers to the administration controls that provide a foundation for how an organisation implements information assurance, such as incident response plans & best practice guidelines.

Defense in Depth (DiD) is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect assets. If one mechanism fails, another one steps up immediately to thwart an attack.