Lecture 1 - Introduction

Networks and System Security

Overview

The aim of this module is to gives students an understanding of the need for computer security and the technologies that support it. It will have practical emphasis which allows students to discover for themselves, with the support of their tutors, the pitfalls of security design and to comprehend the mathematics underlying the protocols by programming small examples

Learning objectives

By the end of the module, you will be able to

LO1

Appraise the need and requirements for computer security within social, commercial and contexts

LO2

Describe the role which cryptography plays within the broader subject of computer security

LO3

Measure the security requirements of particular situations and propose security solutions

LO4

Describe security weaknesses for different security systems.

LO5

Construct security systems and test for weaknesses through breaking them.

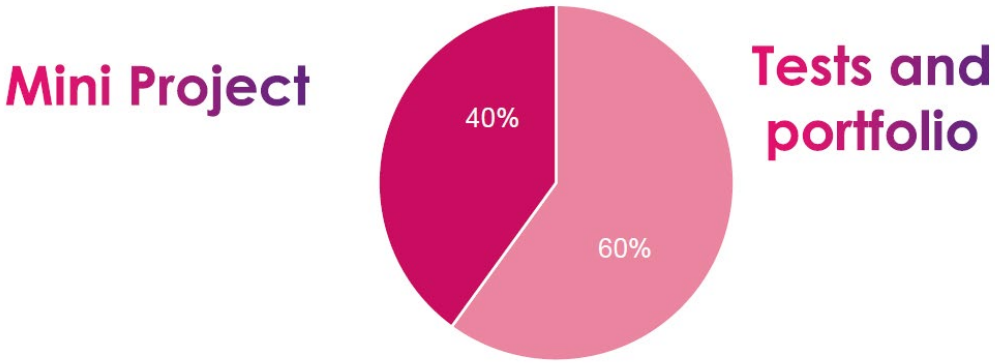
LO6

Identify and address ethical, social, legal and professional issues in Network and Systems Security, including how they manifest in the workplace

Goldsmiths
UNIVERSITY OF LONDON

Lecture 1 - Introduction

Assessment



Pass mark for module is 40%

Formative assessments

- In class quizzes
- Learn.Gold quizzes
- In class polls
- Group discussions
- Research paper discussions
- Case studies
- Laboratory/Tutorial logbooks

Books

- *Network Security Essentials* by W. Stallings (Prentice Hall, 2000), ISB 013 01 6093 8
- *Security in Computing* by C. Pfleeger and S. Pfleeger (Prentice Hall,2006), 4th edition, ISBN 0 13 239077-9

Goldsmiths
UNIVERSITY OF LONDON

Lecture 1 - Introduction

Computer Science Concepts

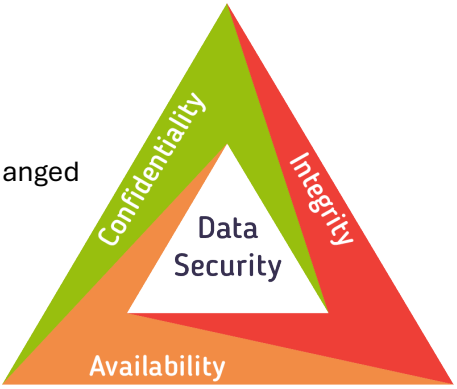
Before the widespread use of computers security relied on physical guardrails such as guards and administrative measures.

After automation was introduced, this improved file protection and distributed systems and networking.

Computer security: the discipline of managing malicious intent and behaviour involving information and
communication technology.
The generic name for the collection of tools designed to protect data and to prevent hackers.

Internet security (lower case “i”
refers to any interconnected collection
of network): Encompasses strategies to discourage, stop, identify, and address security breaches related to information transmission.

- Confidentiality – giving the data to the right person
- Availability – having the right access
- Integrity- receiving the data in the right format and it not being changed



Data integrity - Assures that information and programs are changed only in a specified and authorised manner

System integrity- Assures that a system performs its intended function in an unimpaired

manner, free from deliberate or inadvertent unauthorised manipulation of the system

Additional Security Concepts

Authenticity

Goldsmiths
UNIVERSITY OF LONDON

Lecture 1 - Introduction

Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

Accountability

The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity

Security Challenges

Security is difficult:

- Attacks evolve dynamically
- Security mechanisms involve complex protocols
- Usability often conflicts with security
- Organisations rarely invest until after breaches
- Constant monitoring is required
- Often treated as an afterthought

Key Terms

- **Security Attack:** An action compromising information security.
- **Security Mechanism:** Something designed to detect, prevent, or recover from an attack.
- **Security Service:** Provides protection to data transfers and system operations, relying on mechanisms