University of Portsmouth
BSc (Hons) Computer Science
Third Year

IT And Internetworking Security (ITINS)

M33141

January 2026 - June 2026

20 Credits

Thomas Boxall
thomas.boxall1@myport.ac.uk

Contents

Page 1

Lecture - Introduction

2026-01-26 14:00 Shikun

NB: This was split between 26th January and 2nd February lectures.

1.1 Introduction to Module

This module could alternatively be known as "Cyber Security for Enterprise and Infrastructure" however course leadership didn't like the sound of it, so ITINS it is.

The module will be delivered through a mix of lectures and practical tutorials. The tutorials will use Cisco Packet Tracer to simulate networks, rather than use real hardware. There may be an option later in the module to visit the networking labs and see the real hardware. Worth noting that simulations are easier and quicker than completing the same activities on the real hardware.

There are a number of useful books for this module. The Cisco CCNA Security Guide (210-260) will be the main book for this module, and even the older versions are still relevant (and cheaper to acquire).

Assessments for the module will be worth 50% and will involve submitting 3 labs (2 to be selected from a list of 5) and a short report. The exam will be a mix of MCQ and longer form questions. The questions in the final exam will be from the CCNA. The final exam will be held during the May/June exam period and has previously fell towards the end of the time slot.

1.2 Introduction to Security

Computer Security is the idea of protection afforded to an information system in order to preserve the integrity, availability and confidentiality of information system resources. This covers hardware, software, firmware, information / data, and telecommunications.

Definitions

Threat A potential for violation of security

Vulnerability A way by which loss can happen

Attack An assault on system security, a deliberate attempt to evade security services

1.2.1 Impact of a Cyber Incident

A cyber incident is said to have a *low* impact if there is a limited adverse effect on organisational operations, assets or individuals. The loss may cause degradation in mission capabilities to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced. There may also be minor damage to organisational assets, minor financial loss or minor harm to individuals.

The impact is classified as *moderate* if there is a serious adverse effect on the operations of the organization, assets or individuals. There may be a significant degradation in the mission capabilities, duration and extent that the organisation is able to perform its primary functions but the effectiveness

of the functions is significantly reduced. It may result in significant damage to organisational assets, result in significant financial loss or result in significant harm to individuals that does not involve loss of life, or serious or life threatening injuries.

A *high* impact incident is classified as one which has a significant or catastrophic adverse effect on organisational operations, assets or individuals. The loss might cause a severe degradation in or loss of mission capability to an extent and duration that the organisation is not able to perform one or more of its primary functions. It may result in major damage to organisational assets, result in major financial loss or result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

1.2.2 Security Requirements

Different situations will prioritise different aspects of cyber security and therefore protecting assets differently. While all of the below examples all require strong security surrounding them, there is a security trait (confidentiality, integrity, availability, etc) which is considered to be the most important trait.

Student Grades are considered *confidential* as they should not be shared

Paitient Information is considered for it's *integrity* to be the strongest

Authentication Services are considered to require *availability* as the strongest trait as so many other systems rely on them

Admission Tickets should be *authentic* to prevent people spoofing them

Stock Sell Order should have *non-repudiation* as it's strongest trait to ensure the order is maintained.

1.2.3 Challenges with Security

Naturally, given users are involved in the equation, there are challenges with security:

- Security isn't simple, it is easy to get it wrong
- All potential attacks must be considered
- Procedures used can seem counter-intuitive
- Often involves algorithms and secret information
- Engineers must decide where to deploy mechanisms
- There is a battle of wits between attacker / administrators
- Not perceived until it fails
- Requires regular monitoring
- Security is often considered as an after-thought
- Regarded as an impediment to using the system

1.2.4 Cloud and Virtual Networking Security

Within a Data Center, there is a need for elevated security. This may include, for example, on-prem security officers, fences and gages, continuous video surveillance, security breach alarms, electronic motion detectors, security traps, and biometric access and exit sensors.

Definitions

Hyperjacking Attackers hijack a VM controlling software to attack other devices

Instant On Activation Old VM is activated with out of date security policies

Antivirus Storm When all VMs attempt do download antivirus data file at the same time

1.3 Introduction to Hackers

Modern hackers will go by many titles including:

- Script Kiddies
- Vulnerability Brokers
- Hacktivists
- Cyber Criminals
- State-Sponsored Hackers

However, generally they will fall into one of three categories.

White Hat Hackers are those who hack ethically. They use their skills in an ethical way to identify and responsibly report vulnerabilities in a legal way.

Grey Hat Hackers are those who commit crimes, and do arguably unethical things - but not for personal gain or to cause damage. They sit in the grey area between White and Black hat hackers.

Black Hat Hackers are unethical criminals. They violate computers and network security for personal gain or for malicious reasons.

1.3.1 Tooling

The tooling used by hackers has also evolved. Back in the 1980s, the tools were more rudimentary, requiring more specialist knowledge to operate them. While more recently, the tools have become more sophisticated therefore requiring less technical knowledge to operate them.

Attack tools can be categorised into the following:

- Eavesdropping
- Data modification
- IP based spoofing
- Password-based
- Denial-of-Service
- Man-in-the-Middle
- Compromised Key
- Sniffer

1.4 Policy

Policy says what is not allowed. It might sometimes also say what is allowed with relation to computer system.

The secure mechanism to enforce policy, where the set of reachable states are entirely contained within the set of secure states with a buffer, is regarded as often unobtainable yet the cyber security professional's preference.

The precise mechanism to enforce policy, where the set of reachable states is entirely contained within the set of secure states with no buffer, is precise in that there is no additional security; this is what managers like to aim for.

However in reality, the board mechanism to enforce policy is where some of the set of reachable is within secure but the other half is dangling out of secure. This is the reality for many organisations.

Freely Given, Highly Questionable

These notes are a byproduct of my learning process - mistakes, bad jokes and snark included. If you take an error of mine as gospel and ruin your perfect 1st, that is a *you* problem boo. I am a student, not a prophet, use a textbook if you want certainty.

Yes, they have been typeset in LaTeX; I'd rather typeset in stone with a blunt chisel than use Word Online for another minute. If the formatting looks obsessive, it's because it was either this or a breakdown. You can find the source on my GitHub.

Thomas Boxall is a Computer Science Student studying at the University of Portsmouth, UK. In all honesty, he should probably be revising or doing some work towards his dissertation, not fondling the template of his notes again. You can find Thomas online at thomasboxall.net