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.

# Page 2

# Lecture - Threats, Risk Assessments & Trust

2026-02-10 14:00 Shikun

## 2.1 Policies

Within Cyber Security, policies are used to unambiguously partition system states. They correctly capture security requirements for a given system, user or the organisation as a whole. This definition can be simplified to *a statement of what is and what is not allowed.*

All security policy and mechanisms for their enforcement sit on top of assumptions. The assumptions support the mechanisms for enforcement to work correctly. Some of these assumptions may be documented in the policy, however some may not be.

There may also be 'grey areas' in the policies, or where they are not as precise as needed. For example - if an imaginary bank's policy states that bank officers are authorised to transfer money amongst account; and a bank officer moves £100,000 into their account - has the bank's security policy been violated? The answer can be seen both ways for this - yes in that they shouldn't be able to touch their own account, but also no - as this hasn't been documented in the policy. This makes the 'yes' answer assumption based and someone else may see this differently.

Alternatively, if it is deemed that a website has to be available, however the security policy doesn't mention availability - the definition of security isn't appropriate.

## 2.2 Trust vs. Assurance

Definitions

**Trust** the assumption that a system or service is secure

**Assurance** the degree of confidence that a system or service meets its security requirements

Trust is considerably more subjective than assurance. Trust is founded in beliefs, expectations, perceptions and subjective opinions often of those who shout the loudest. While assurance is based in evidence, standards, metrics and criteria - it's a quantitative way of saying "yes, this is a secure system."

Assurance is a measure of how well the system meets its requirements. It doesn't say what the system is to do, rather it only covers how well the system does it. Assurance proves confidence; helps to identify and address any gaps or weaknesses; provides evidence and assurance to stakeholders, customers, regulators and auditors; and enables continuous improvement of the service.

In traditional industries - drugs are considered trustworthy based on a few factors:

- Certification
- Manufacturing standards

- Preventative sealing in packages

In cyber industries, data and services are considered trustworthy based on:

- Testing
- Auditing
- Monitoring
- Evaluating both effectiveness and performance

## 2.3 Analysis

Businesses are presented the question "Is it cheaper to prevent x from happening, or recover if x happens?"

This isn't an easy question to answer - especially when x could be a major cyber incident stopping all business activities for n time; loss of earnings and loss of padding in the CEO's back pocket... However, what if x doesn't happen and never comes close to happening - that's just a waste of money on preventative measures surely.

Cost-Benefit analysis is the solution to this - it is a data driven process used to evaluate the strengths and weakness of the options.

Part of CBA is Risk Analysis, which asks if the thing should even be protected in the first place, and how much should we protect this thing.

Risk analysis can be seen in a simple of example of what is the loss if a mobile phone gets stolen. Obviously there is the loss of service, and the loss of the physical asset - but what about the other dangers? What about the bank cards connected to Google Pay (or Apple pay for *those* weirdos)? When phrasing it like that - cyber cover for a mobile phone while still extortionately expensive, doesn't feel like such a bad deal...

## 2.4 Humans Are Insecure

The systems we use are only as secure as the humans driving them. It would be great to have an IT system which users can't get within 10' of - so secure, but also just a bit useless as no one can do anything with it. A "secure" system can be breached by improper operation (for example when accounts with no passwords are created).

Within organisations, there is a need for there to be a match between those who have the power and those who have the responsibility for cyber security. For example, those who are responsible for security have the power to enforce security, otherwise there is confusion. However, when system administrators are responsible for implementing security officers can make the rules, there is power given without responsibility.

Data (from somewhere) shows that 80-90% of all security problems initiate from "insiders." This is the situation where an account (either with the account holders' knowledge or not) that already exists in the system is used in an unauthorised way. The remaining 10-20% of attacks come from outside the organisation, most commonly seen in the form of DDoS attacks.

It's not just internal roles (Management, IT staff, Custodians, Ops Staff, Compliance officers, etc) who are risks in the system here - external (vendors, suppliers, contractors, temporary employees, etc) also provide risk. Often higher than that of internal staff as less internal vetting may have been conducted when taking on a new contractor. In this equation - HR are often the linchpin, as they are responsible for the hiring, termination and employee training.

Definitions

**Masquerader** A person who is not authorised to use a computer, but gaines access appearing to be someone with authorisation

**Misfeasor** A person who has limited authorisation to use a computer, but misuses that authorisation

**Clandestine User** A person who seizes supervisory control of a computer and proceeds to evade auditing and access controls

**Hacker** Generic term for someone who does unauthorised things with other people's computers

## 2.5 Risk

Risk is *the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset).*

A vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (man made or act of nature) that has the potential to cause harm. The likelihood that a threat will use a vulnerability to cause harm creates a risk.

The impact of a risk happening is the loss of availability, integrity, and confidentiality; as well as possible other business losses such as lost income, loss of life and loss of real property.

It is not possible to identify all risks nor to eliminate all risks. However we can use a risk assessment to do some of this for us.

### 2.5.1 Risk Assessment

A risk assessment is a systematic and comprehensive analysis of the probability of a certain event occurring and the potential consequences that might result from that event. It is used to identify and characterise risks.

Risk assessments, while dense paperwork, can help to improve security and may even increase productivity. They can also reduce costs. They work in a four step process:

1. Identify risks
2. Analyse the likelihood of those risks
3. Formulate solutions for reducing risks
4. Continuously monitor risks

There are lots of different types of risk assessment:

- Business impact assessment
- Qualitative risk assessment
- Quantitative risk assessment
- Cost-Benefit analysis
- Probability profile analysis
- Failure modes, effective and criticality analysis

There are a number of formal Cyber Security risk frameworks which can be used to identify and respond to risks in:

- NIST Cyber Security Framework
- ISO 27005
- FAIR (Factor Analysis of Information Risks)

A risk assessment might identify risks such as

- Ransomware
- Data leaks
- Phishing
- Malware
- Insider Threats
- Denial of Service
- Unauthorised access
- Misuse of information by authorised users
- Weaknesses in organisational security controls
- Data leaks and breaches
- Service disruption

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective qualitative analysis based on informed opinion, or where reliable monetary figures and historical information is available - the analysis might use quantitative analysis.

For a given risk, Management can choose to accept the risk based on one of three options (or some combination):

- the relative low value of the asset
- the relative low frequency of occurrence
- the relative low impact on the business

However, management might choose to release the proverbial purse strings and relinquish some cash to mitigate the risk. They'll select and implement the appropriate control measures to reduce the risk. In some cases the risk can be transferred (banished) to another business by buying insurance or out-sourcing the risk inducing activity to another business.

### 2.5.2 Risk Management

A key part of risk management is to identify the assets and estimated values, including the people, buildings, hardware, software, and data supplies. Then a threat assessment is conducted which includes acts of nature, accidents and malicious acts originating from inside or outside the organisation. A vulnerability assessment is also conducted, where for each vulnerability - the probability it will be exploited is calculated through evaluating policies, procedures, standards, training, and physical security.

This data is then used either in a qualitative or quantitative way to calculate the impact each threat would have on each asset. From which the appropriate controls can be identified and implemented. This process has to consider the productivity, const effectiveness and value of the asset.

The Single Loss Expectancy (SLE) is a value which is calculated by multiplying the Asset's Value by the Exposure Factor (as a percentage of the assets value). The SLE can then be multiplied by the Annual Rate of Occurrence (ARO) which is the number of times per year that an incident is likely to occur to find the Annual Loss Expectancy (ALE).

## 2.6 Trusted Systems

A Trusted System is a platform designed to reliably enforce a specific security policy, ensuring it functions as intended without unauthorised modifications. Access is granted through an access right - which is a way in which an object can be accessed by a subject; typically this is granted as 'read', 'write' and 'execute'.

## 2.7 Formal Evaluation

Formal Evaluation is a method to achieve *trust*. It is not a guarantee of security. These methods are formal, which doesn't mean auditors in smart suits and little bow ties - it means the results have been found using the *language of mathematics*, logic and proof. The formal outcome should be able to be verified.

The formal evaluation process looks at the security requirements; if the assurance requirements showing how to establish the security requirements have been met; what the procedures to demonstrate the system meets the requirements look like; and outputs some metrics for the results. The products passing a formal evaluation are trusted, and often some level of formal evaluation will be required for an organisation to do business with another organisation.

Due to the complex requirements, it is often not feasible to formally verify an entire system. However discreet components are often verified.

There are a number of different specifications for formal evaluation, the first and most well known being produced by the US Department of Defence, called the *Trusted Computer System Evaluation Criteria* (TCSEC) but colloquially known (and feared) as the *Orange Book*.

### 2.7.1 TCSEC

The TCSES emphasises confidentiality. It has seven levels: D, C1, C2, B1, B2, B3, A1 where D is failed and A1 is perfect.

- C1 (discretionary protection) ensures appropriate identification and authentication are in place within the system, as well as discretionary access control is implemented.
- C2 (controlled access protection) validates that object reuse and auditing is appropriately configured.
- B1 (labelled security protection) mandates access control on a limited set of objects. It looks for an informal model of the security policy.
- B2 (structured protections) ensure that there is a trusted path for login; the principle of least privilege is followed; that there is a formal model of security policy; covert channel analysis is followed; and that there is configuration management throughout the estate.
- B3 (security domains) look for a full reference validation mechanism at the system architecture level; expects there to be constraints on the code development process; and looks for documentation and testing requirements.
- A1 (verified protection) demands formal methods for analysis and verification as well as trusted distribution.

### 2.7.2 ITSEC

ITSEC is the European answer to TCSEC. It came along a few years after the TCSEC and it's levels are considerably more hand-wavey.

- E1: Security target defined and tested; must have informal architecture description

- E2: Informal description of design; configuration control and code distribution
- E3: Correspondence between code and security target
- E4: Formal model of security policy; structured approach to design; design level vulnerability analysis
- E5: Correspondence between design and code; source code vulnerability analysis
- E6: Formal methods for architecture; formal mapping of design to security policy; mapping of executable to source code

### 2.7.3 Common Criteria

Eventually, US, UK, France, Canada and the Netherlands came together to produce the *Common Criteria for Information Technology Security Evaluation* (CCITSE or CC). Under the CC, each level of trust rating from the TCSEC can be specified as a protection profile (PP). A PP looks very similar to a level of trust rating but has two fundamental differences:

- the TCSEC binds sets of features and assurances together - the CC allows PP to combine features and assurances together in any combination
- the TCSEC specifies a fixed set of ratings (profiles) but the CC allows for consumers to write a customised set of requirements in a standard format

The CC is split into functional requirements (362 page document) which is divided into 11 classes with multiple families per class; and assurance requirements (216 page document) which is divided into 10 classes, with several families per class.

There are over 2200 registered products with the CC, which maintains an online portal of registered products.

## 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