



Aston University

BIRMINGHAM UK

CS2IS

Information Security

Unit 01B: Introduction

Dr Philip Weber

p.weber1@aston.ac.uk

MB214N

Dr Zhuangzhuang Dai

z.dai1@aston.ac.uk

MB214H

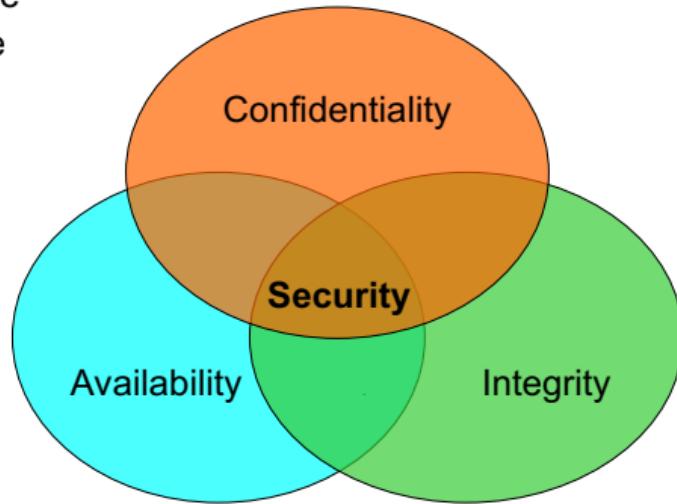


Outline

- ▶ Module aims, structure, assessment and feedback
- ▶ Information Security definition and goals
- ▶ Key concepts and terminology

What is Information Security?

- ▶ The protection of information systems in order to preserve the *confidentiality, availability* and *integrity* of their *assets*:
 - ▶ hardware
 - ▶ software
 - ▶ data



Key security goals: confidentiality

- ▶ Only authorised people or systems must be able to access protected assets (e.g., data or software)
- ▶ But: it is not always easy to define who is authorised to perform what operation on which data...

London clinic leaks HIV status of patients

⌚ 2 September 2015 | London



Dr Alan McOwan: "Not everybody on the list is HIV positive"

A London sexual health centre mistakenly leaked the details of nearly 800 patients who have attended HIV clinics, bosses have admitted.

The 56 Dean Street clinic in Soho sent out the names and email addresses of 780 people when a newsletter was issued to clinic patients.

Patients were supposed to be blind-copied into the email but instead details were sent as a group email.

Key security goals: availability

- ▶ Assets such as data and services must be accessible to authorised parties at the appropriate times
- ▶ There are numerous characteristics associated with availability; a data item or service is deemed available if
 - ▶ it is present in a useable form
 - ▶ it is making clear progress
 - ▶ it completes in an acceptable period of time
 - ▶ requests are handled timely and fairly
 - ▶ it can be used easily and in the way it was intended to be used
 - ▶ etc.

Greater Manchester Police website hit by denial-of-service attack

© 3 September 2015 | Manchester



A 12-year-old boy was sexually assaulted.
At about 1.40pm on Friday 28 August 2015 the 12-year-old victim was in the public toilets in the Arcades on Warrington Street when he was approached by a man.



Witness appeal following PCSO hit
Police are appealing for witnesses if Support Officer (PCSO) was knocked Stockport.



There is no pride in domestic abuse
GMP is working with national charity awareness about domestic abuse in and transgender (LGBT) community



Witness appeal after report of human trafficking
Police are appealing for information trafficking in Bolton.



Image issued of suspect following or
At 5am on Tuesday 11 August, a man large metal pole next to the main bus before going down Ashburner Street

Latest news

[View all latest news](#)

/ Your community

GMP

The GMP website was available again on Thursday

Greater Manchester Police's (GMP) website was attacked on Wednesday, the force said.

The site was unavailable for more than two hours from 20:00 BST in a "malicious attempt to disrupt services", GMP said.

Deputy Chief Constable Ian Hopkins said they were treating it as a "denial-of-service attack" and apologised for any inconvenience caused.

A person has claimed responsibility on Twitter for causing the website crash, a GMP spokeswoman said.



The Bronze Soldier of Tallinn

- Estonian independence in 1991
- c. 40% ethnic Russian
- “most wired” country in Europe
- Member of NATO
- April 2007: Estonian government moves Bronze Soldier from central Tallinn to a military cemetery

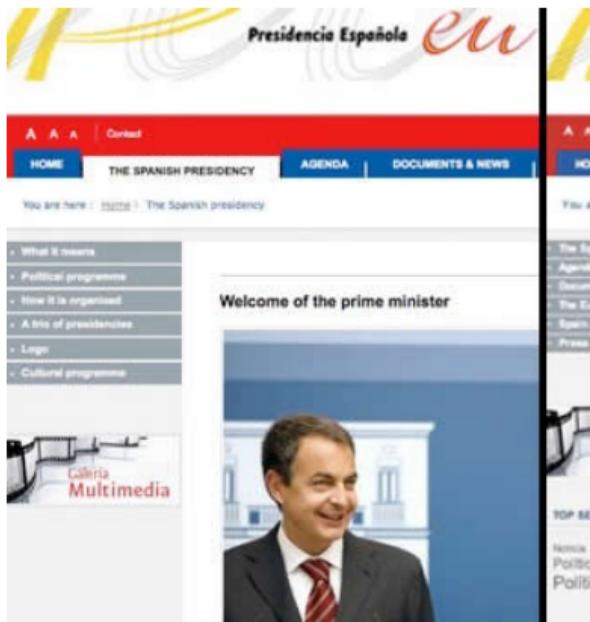


- Following the Bronze Soldier’s relocation, government, banking, media and other websites came under sustained DDoS attacks for several weeks.
- Coincided with rioting in Tallinn and protests outside Estonia’s Moscow embassy.
- The “most wired” country was effectively shut down.



Key security goals: integrity

- ▶ Combination of several desirable properties – assets must be
 - ▶ precise
 - ▶ accurate
 - ▶ unmodified (except in acceptable ways, by acceptable entities)
 - ▶ consistent
 - ▶ meaningful
 - ▶ useable



The screenshot shows the homepage of the Spanish Presidency website. At the top, there is a banner with the text "Presidencia Española" and "eu". Below the banner, a red navigation bar contains links for "HOME", "THE SPANISH PRESIDENCY", "AGENDA", and "DOCUMENTS & NEWS". A contact link is also present. The main content area displays a photograph of José Luis Rodríguez Zapatero, the Prime Minister of Spain at the time. To the left of the photo is a sidebar with a list of links related to the presidency, including "What it means", "Political programme", "How it is organised", "A list of presidencies", "Logo", and "Cultural programme". A "Galería Multimedia" link is also visible.



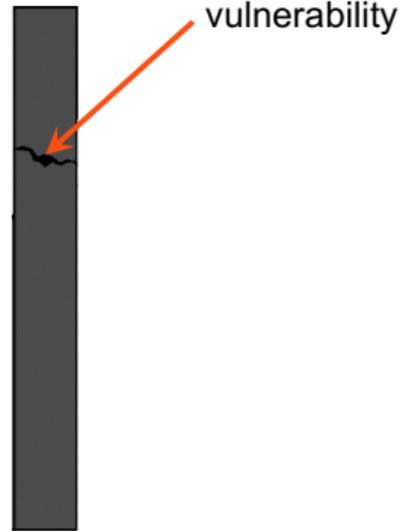
The screenshot shows a search results page from the Spanish Presidency website. The search query was "Resultados de búsqueda". The results list includes "No se han encontrado Resultados !!", "Error", and a stack trace: "org.apache.lucene.search.OneSearchException: Búsqueda de 'query'". On the right side of the page, there is a large image of Mr. Bean, the famous British character. The sidebar on the left includes links for "The Spanish presidency", "Agenda", "Documents & News", "The European Union", "Spain in focus", and "Press". A "Galería Multimedia" link is also present. The footer features a "TOP SEARCHES" section with links to "Noticia UE", "Brussels UE", "Políticas", "Presidencia Cultura", "Política", and "cultur".

Outline

- ▶ Module aims, structure, assessment and feedback
- ▶ Information Security definition and goals
- ▶ Key concepts and terminology

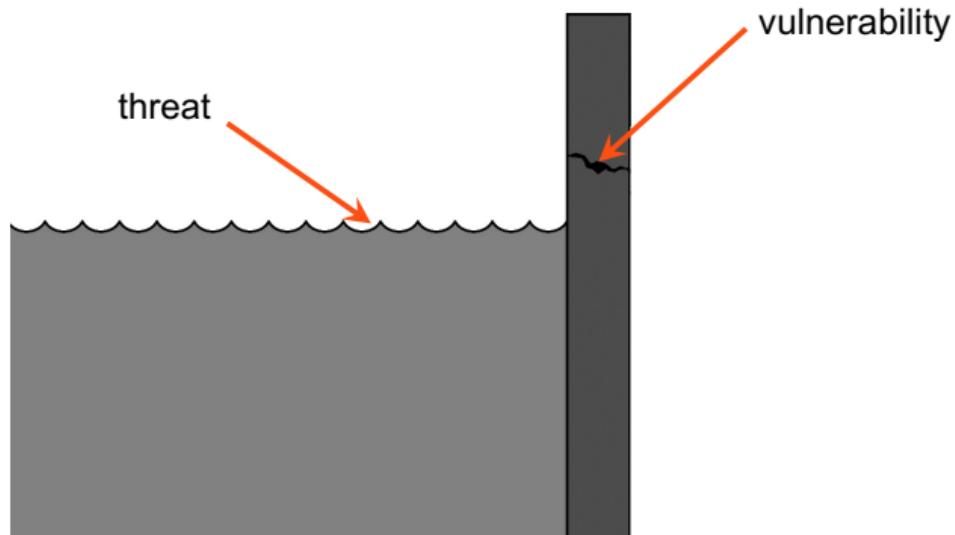
Vulnerabilities, threats and controls

A *vulnerability* is a weakness in the information system (e.g., in its design, implementation or procedures) that can be exploited to cause loss or harm.



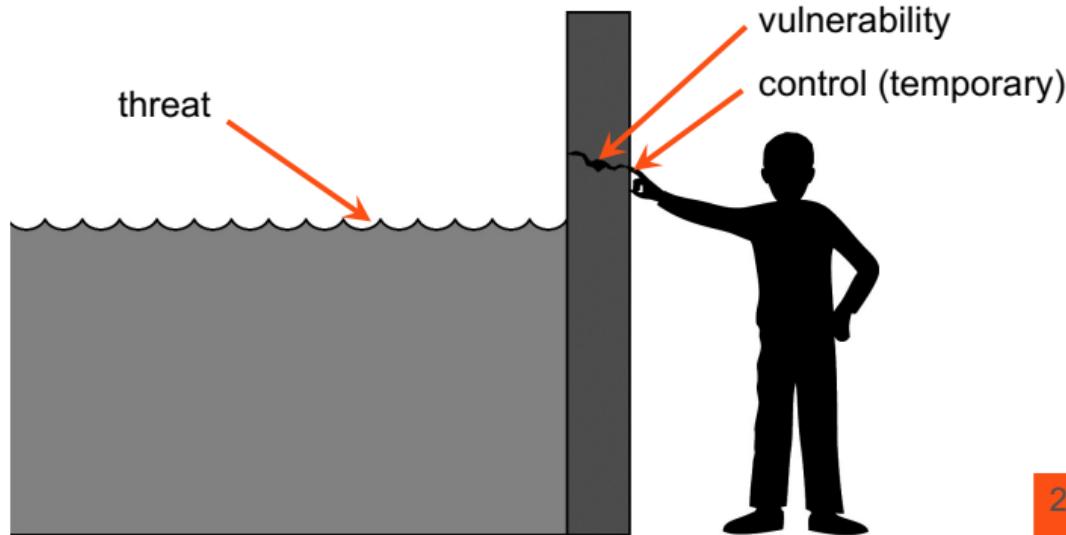
Vulnerabilities, threats and controls

A *threat* is a set of circumstances that has the potential to cause loss or harm, often through exploiting a vulnerability.



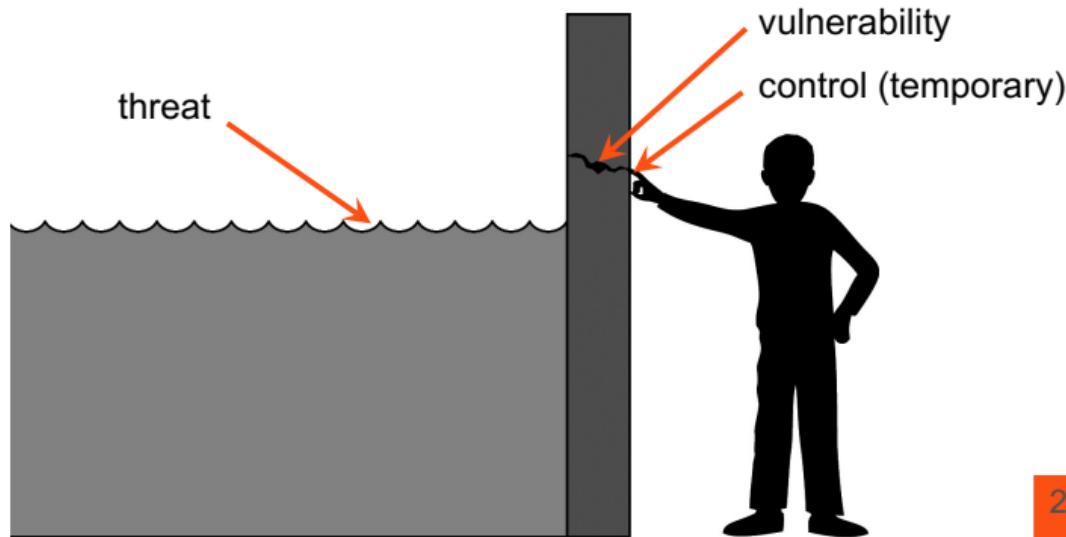
Vulnerabilities, threats and controls

A *control* is a protective measure (e.g., an action, device, procedure or technique) that removes or reduces a vulnerability.



Vulnerabilities, threats and controls

A *threat* is blocked by *control* of a *vulnerability*.



Vulnerabilities, threats and controls: example

A memory stick with the details of more than 700 patients at Cambridge University Hospital was left in a vehicle. A car wash attendant was able to access the unencrypted material.



Vulnerability	Threat(s)	Control
Patient records are stored in an unencrypted memory stick	Loss of sensitive data	Encrypt the data file

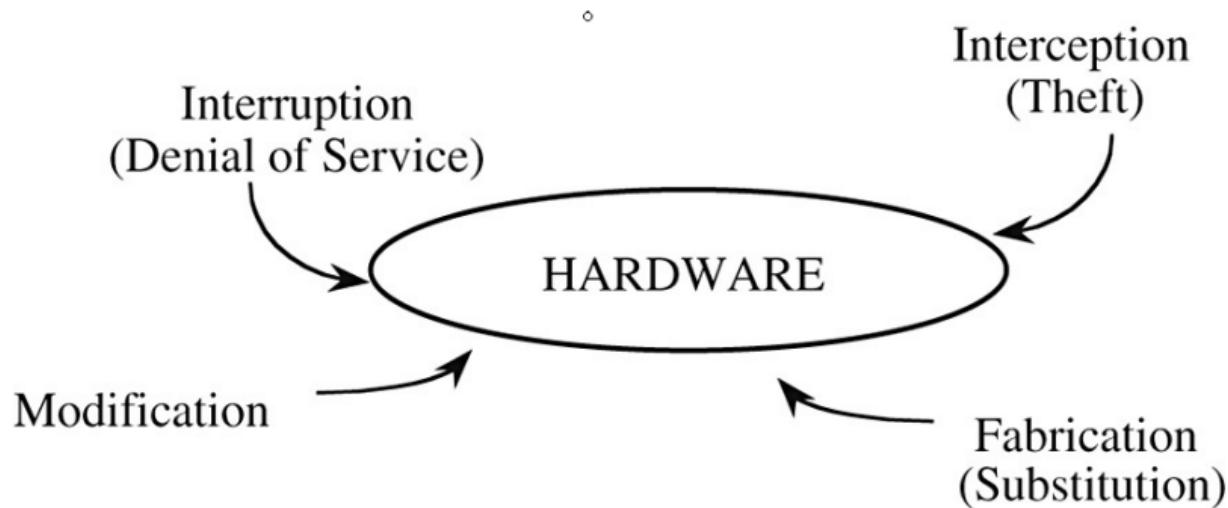
Classes of vulnerabilities

- ▶ *Interception* – unauthorised party has gained access to an asset
 - ▶ e.g., wiretapping to obtain data in a network or copying data
- ▶ *Interruption* – an asset becomes lost, unavailable or unusable
 - ▶ e.g., malicious destruction or deletion
- ▶ *Modification* – unauthorised party tampers with an asset
 - ▶ e.g., changing database entries or altering of software
- ▶ *Fabrication* – unauthorised party creates a counterfeit asset
 - ▶ e.g., inserting database entries or network transactions

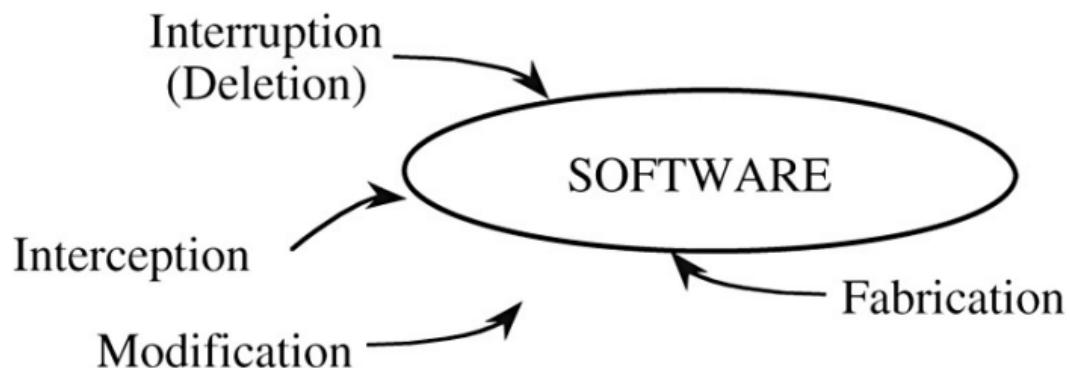
Classes of vulnerabilities

- ▶ *Interception* – may allow an unauthorised party to gain access to an asset
 - ▶ e.g., wiretapping to obtain data in a network or copying data
- ▶ *Interruption* – may allow an asset to become lost, unavailable or unusable
 - ▶ e.g., malicious destruction or deletion
- ▶ *Modification* – may allow an unauthorised party to tamper with an asset
 - ▶ e.g., changing database entries or altering software
- ▶ *Fabrication* – may allow an unauthorised party to create a counterfeit asset
 - ▶ e.g., inserting database entries or network transactions

Hardware vulnerabilities

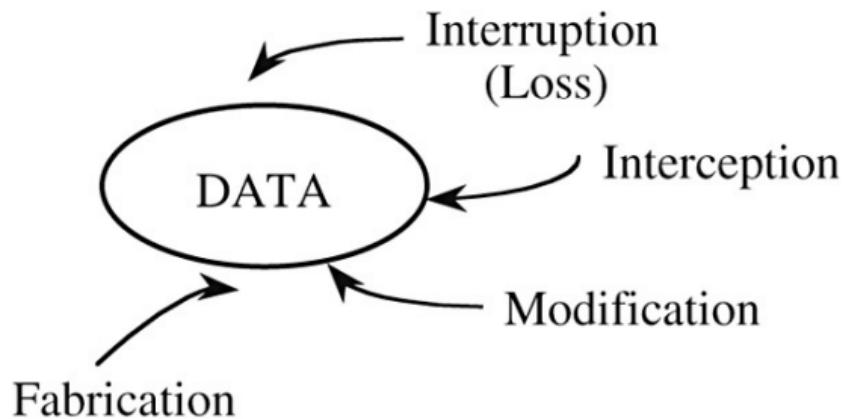


Software vulnerabilities





Data vulnerabilities



Controls

- ▶ *Encryption*: scramble data so that interpretation is meaningless for an intruder without knowledge of how the scrambling was done
- ▶ *Software controls*: programs must enforce security restrictions, e.g., check user passwords and access rights
- ▶ *Hardware controls*: locks, intrusion detection systems, hardware implementations of encryption
- ▶ *Policies and procedures*: regular password changes, rules for accessing sensitive data

Principle of control effectiveness

- ▶ Controls must be used – and used properly – to be effective.
- ▶ Controls must be efficient (enough), easy to use, and appropriate.

Characteristics of Information Security

- ▶ Assets are small, portable and can be very valuable
 - ▶ unreleased Pixar film worth millions of dollars fits on a DVD
- ▶ No physical contact is required
 - ▶ attacker can easily be located on a different continent
- ▶ Security breaches often hard to detect
 - ▶ compromised computer systems may continue to be used

The ‘Three Golden “Rules” ’ of Computer Security

- ▶ do not own a computer;
- ▶ do not power it on;
- ▶ and do not use it.

(Robert Morris, American cryptographer)

Not really... Which key Information Security goal is not achieved?

Summary of key points in this unit

- ▶ Information Security is a field of Computer Science concerned with the protection of computer-system *assets*: data, software, hardware
- ▶ The key goals of security are to ensure asset confidentiality, availability and integrity
- ▶ Security engineering
 - ▶ identifies system vulnerabilities
 - ▶ implements controls that block threats by removing/reducing vulnerabilities