Queen Mary
University of London

BIRMINGHAM CITY
University

Information Security: Goals and Enabling Technologies

Ali E. Abdallah

Professor of Information Security

Birmingham City University

Email: Ali.Abdallah@bcu.ac.uk

With thanks to Professors Anne Flanagan and Ian Walden

Lectures are part of the project:

ConSoLiDatE
Multi-disciplinary Cooperation for Cyber Security, Legal and Digital forensics Education

Funded by

The Higher Education Academy

December 2014-March 2016

BIRMINGHAM CITY University

Queen Mary University of London

ConSoLiDatE Objectives

- Development of educational resources conveying essential:
  - Cyber security knowledge
  - Legal principles
  - Practical digital forensic investigations
- Provision of supportive resources for flexible student learning
- Consolidation of links between theory and practice through practical scenarios.

The Higher Education Academy

BIRMINGHAM CITY University

Queen Mary University of London

Introductory remarks

- Why Cyber Security and Law?
- Collaboration between the two communities is much needed.
  - We live in a digital world; Technology constantly changing;
  - Criminal law evolves through many centuries but cyber law is very young;
  - New national/EU/US laws emerge, we need to understand their implications.
- We often use the same vocabulary but mean different things!
  - Concepts of proof, authorisation, etc ..

Why Cyber Security and Law?

- Legal appreciation is important for cyber security specialists– serious implications arise from:
  - Testing; ethical hacking;
  - Personal data; privacy
  - Server locations for processing personal information
- Cyber knowledge exceedingly important for lawyers:
  - Most new crimes involve cyber evidence (more than 90%)
  - Formulating service level agreements rely on understanding cyber risks
  - Protecting client information

Outline

- Motivation
  - Examples of Assets, threats and impacts
- What is information Security about?
  - Protection, Detection and Reaction
- Goals of Information Security
  - Confidentiality, Integrity, Availability
- Enabling concepts, mechanisms and technologies
- Case study
- Summary

Needs for Information Security

- Information security is as necessary as physical security; just as a business locks the doors to its offices it must also take steps to protect its information assets.
- Information security is a business enabler that provides a protected context in which commerce can occur while still protecting intellectual property and customer data.
- The value of information security cannot always be established in hard cost; if a countermeasure is purely preventative then ROI may be measured by performing a cost/benefit analysis

Security Attacks are Frequent Headline News!

Flight Simulator Site Destroyed!

One of the oldest web sites, with millions of users, was destroyed!

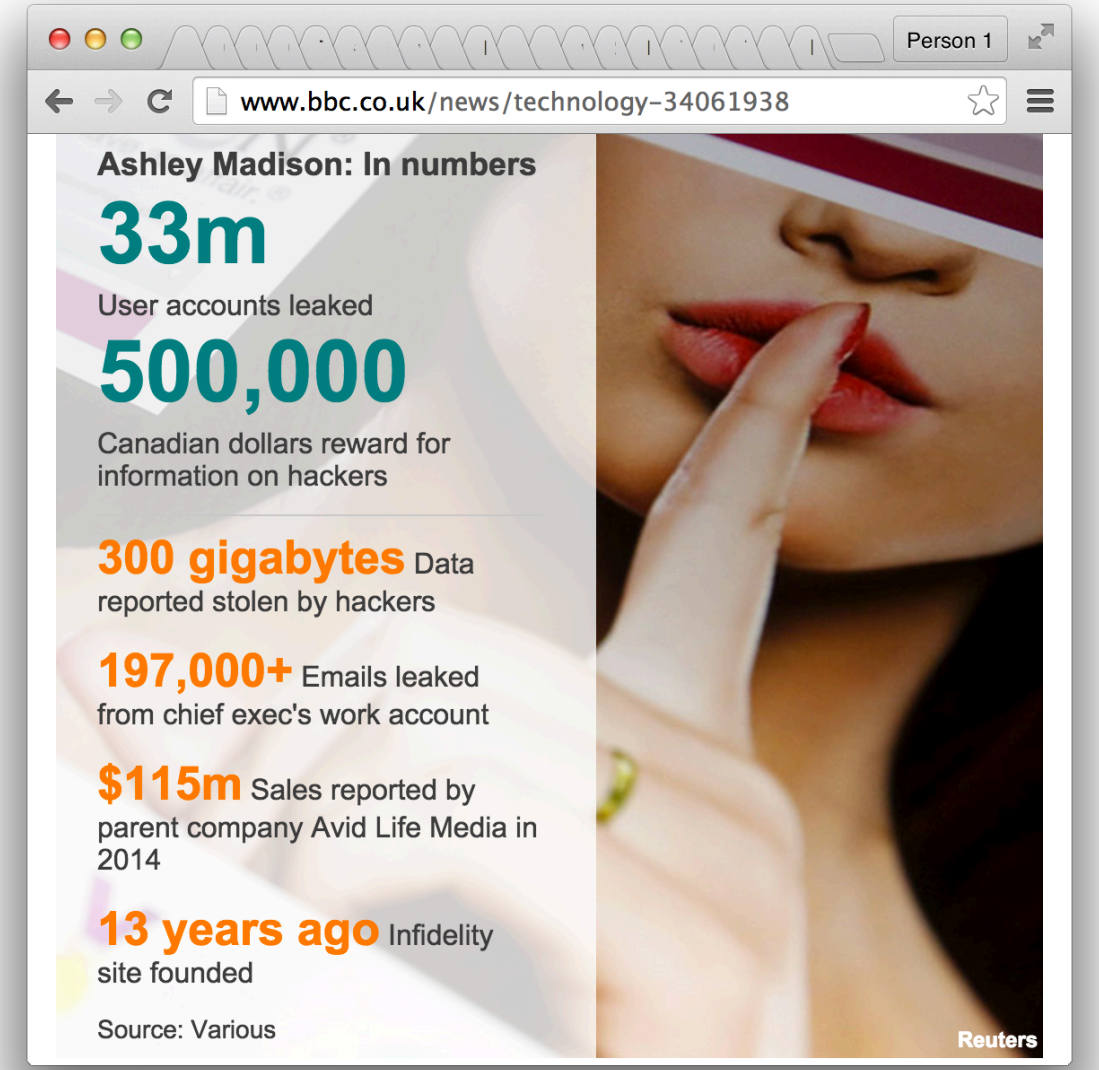
No contingency plan!

http://news.bbc.co.uk/1/hi/technology/8049780.stm

Ashley Madison

With millions of users, security was breached August 2015!

Weak password protection and poor security of core functionalities



http://news.bbc.co.uk/1/hi/technology/8049780.stm

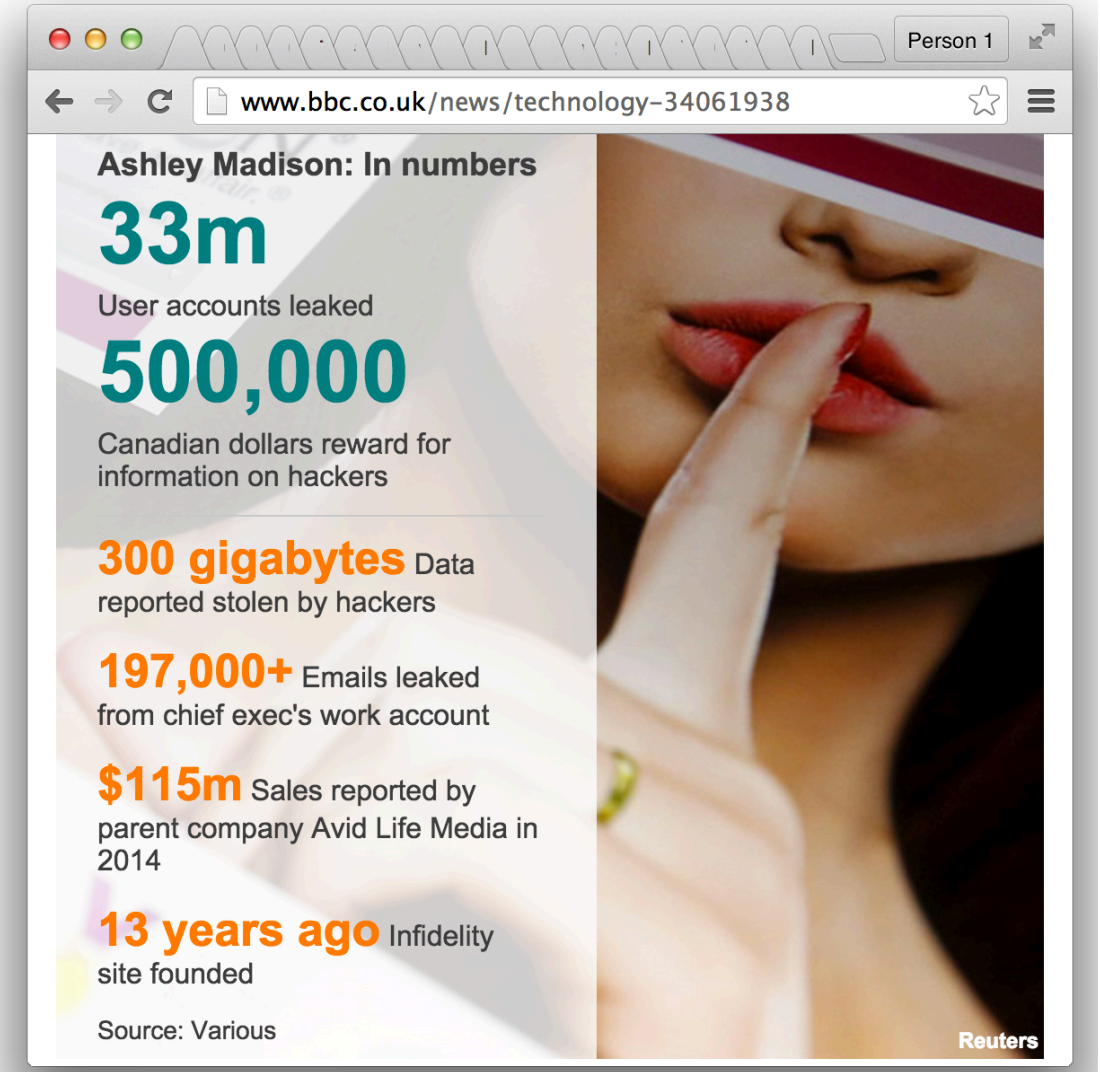
Impact of Recent Ashley Madison Hack

Founder and Chief executive stepped down.

Reported suicides of two individuals associated with website!

Reputation in ruin!

http://www.bbc.co.uk/search?q=Ashley%20Madison



Attacks on a country's infrastructure

In May 2007, Estonia was hit by "Moscow Cyber War".

The hacking principle is very simple- you just send a shed load of requests simultanously!

http://news.bbc.co.uk/1/hi/world/europe/6665145.stm

Cost of Estonia's attack

Considered a "declaration of war".

Services in the whole country came to a halt for thee weeks

http://news.bbc.co.uk/1/hi/world/europe/6665145.stm

Attacks on a personal email

September 2007: Hackers infiltrate Sarah Palin's personal Yahoo email.

Attackers exploited the password resetting system of Yahoo email service.!

http://news.bbc.co.uk/1/mobile/world/americas/7622726.stm

Person 1

news.bbc.co.uk/1/mobile/world/americas/762272...

BBC NEWS

BBC Home > BBC News > Americas

Menu

Hackers infiltrate Palin's e-mail

18 Sep 08 10:55

Hackers have broken in to the e-mail of the US Republican vice-presidential candidate, Alaska Governor Sarah Palin.

The hackers, who targeted a personal Yahoo account, posted several messages and family photos from her inbox.

The campaign of running mate John McCain condemned their action as "a shocking invasion of the governor's privacy and a violation of the law".

The hacking comes amid questions about whether Mrs Palin used personal e-mail to conduct state business.

According to law, all e-mails relating to the official business of government must be archived and not destroyed. However, personal e-mails can be deleted.

Mrs Palin is currently under investigation in Alaska for alleged abuse of power while governor.

'Destroy them'

A group called Anonymous has claimed responsibility for the hacking of Mrs Palin's Yahoo e-mail.

It posted five screenshots, two digital photos of Mrs Palin's family and an address book to the whistle-blowing Wikileaks website. The information was taken from Ms Palin's gov.palin@yahoo.com e-mail account.

Results of the Attack

Personal and official email messages and photos were posted online.

Mrs Palin was investigated for alleged abuse of power. She claimed to have lost vice-presidential race because of this breachl

Hacker was sentenced for one year.

http://news.bbc.co.uk/1/mobile/world/americas/7622726.stm

Attacks on a country's infrastructure

November 2010, Stuxnet worm hit Iran's nuclear installations.

Very sophisticated and carefully targeted attack.

http://news.bbc.co.uk/1/hi/technology/8049780.stm

Secondhand computers

Details of one millions bank customers found!

So far ..

- We have illustrated a number of cyber attacks involving a variety of:
  - targets,
  - sources,
  - intensity,
  - Sophistications, capabilities
  - effects, severity or impacts.
  - motivations
- Attackers only need to find a single weakness!

Security Challenges

- Computer security is not as simple as it might first appear to the novice
- Attackers only need to find a single weakness, the developer needs to find all weaknesses
- Users and system managers tend to not see the benefits of security until a failure occurs.
- Security is often an afterthought to be incorporated into a system after the design is complete.
- Thought of as an impediment to efficient and user-friendly operation.

Information Security Strategy

What are the security objectives?

- Prevention: take measures that prevent your assets from being damaged
- Detection: take measures so that you can detect when, how, and by whom an asset has been damaged
- Reaction: take measures so that you can recover your assets or to recover from a damage to your assets

Private Property Example

- Prevention: locks at doors, window bars, walls round the property
- Detection: burglar alarms, closed circuit TV, discovery of missing stolen items.
- Reaction: call the police, replace stolen items, make an insurance claim

E-Commerce Example

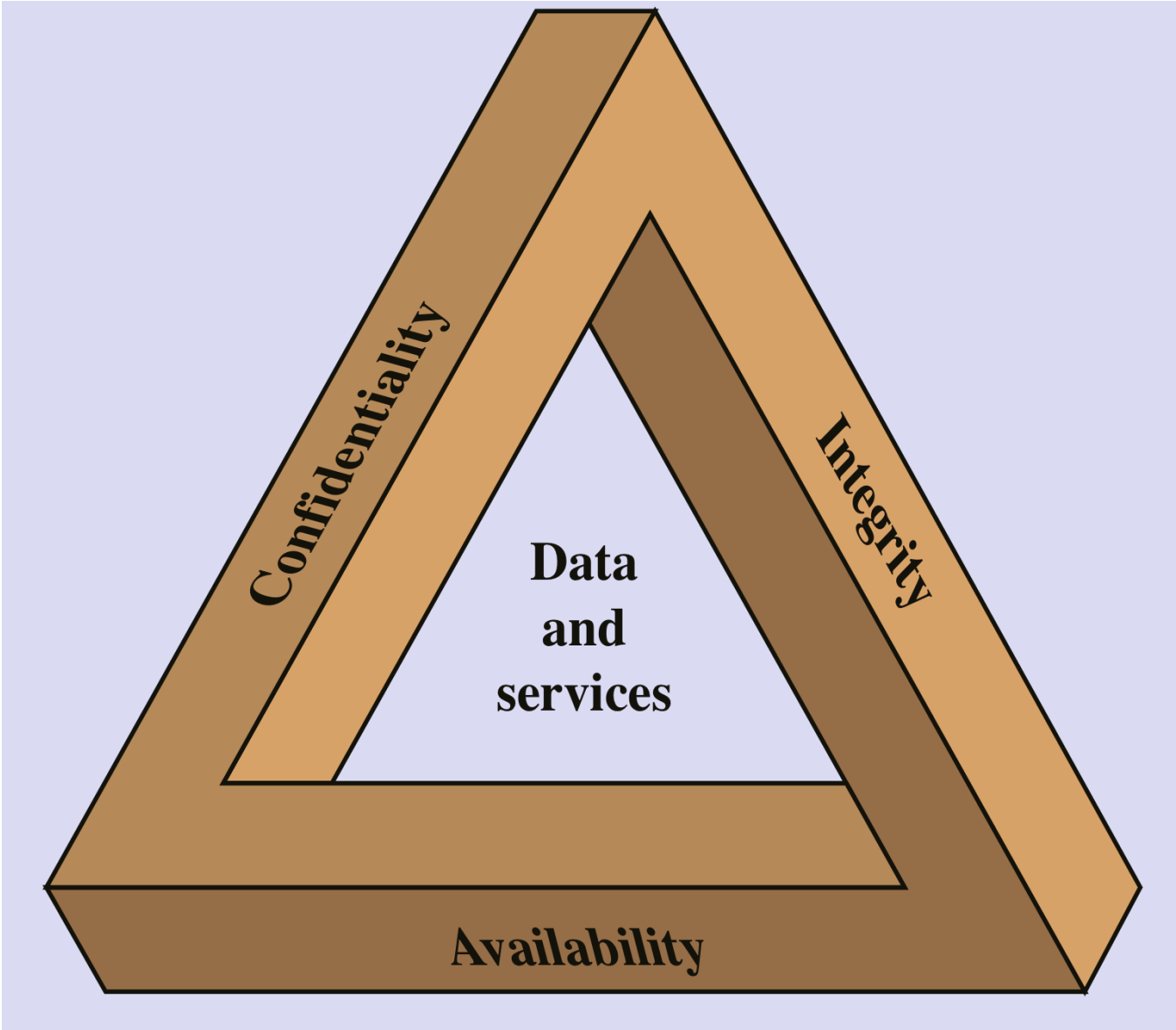
- Prevention: encrypt your orders, rely on the merchant to perform checks on the user, don't use the Internet (?) …
- Detection: an unauthorized transaction appears on your credit card statement
- Reaction: complain, ask for a new card number, consult your lawyer, etc.

Examples of Cyber Security Threats

- Malicious software: Viruses; Worms; Trojans;
- Identity theft
  - Password crackers
  - Phishing
  - Spoofing / masquerading
  - Social engineering
- Unauthorized Access
  - Eavesdropping and tapping
  - targeted data mining
  - Back door/trap door
- Denial of service (DoS, DDoS)
  - Logic bombs
  - Crypto-locker

Information Security Goals

The CIA Triad



Goals of Security: CIA Defined

- **Confidentiality** - the protection of information from unauthorized or accidental disclosure
- **Integrity** – assures information is as entered and intended; that the information has not been incorrectly modified, corrupted or destroyed.
- **Availability-** assures that assets are available when needed to support the organizational enterprise on a timely and reliable basis.

Computer Security?

- Confidentiality: prevent unauthorised disclosure of information
- Integrity: prevent unauthorised modification of information
- Availability: prevent unauthorised withholding of information or resources
- Other aspects: accountability, authenticity

Confidentiality

- Historically, security and secrecy were closely related. Sometimes, security and confidentiality are used as synonyms
- Prevent unauthorised disclosure of information (prevent unauthorised reading)
- Privacy: protection of personal data
- Secrecy: protection of data belonging to an organisation

Integrity

- ITSEC: prevent unauthorised modification of information (prevent unauthorised writing)
- Clark & Wilson: No user of the system, even if authorized, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted.
- Orange Book: Data Integrity - The state that exists when computerized data is the same as that in the source document and has not been exposed to accidental or malicious alteration or destruction. (Integrity synonymous for external consistency.)

Integrity ctd.

- Integrity in communications: detection (and correction) of intentional and accidental modifications of transmitted data
- In the most general sense: make sure that everything is as it is supposed to be; the data in a computer system should correctly reflect some reality outside the computer system.

  Integrity is a prerequisite for many other security services. Operating systems security has a lot to do with integrity.

Availability

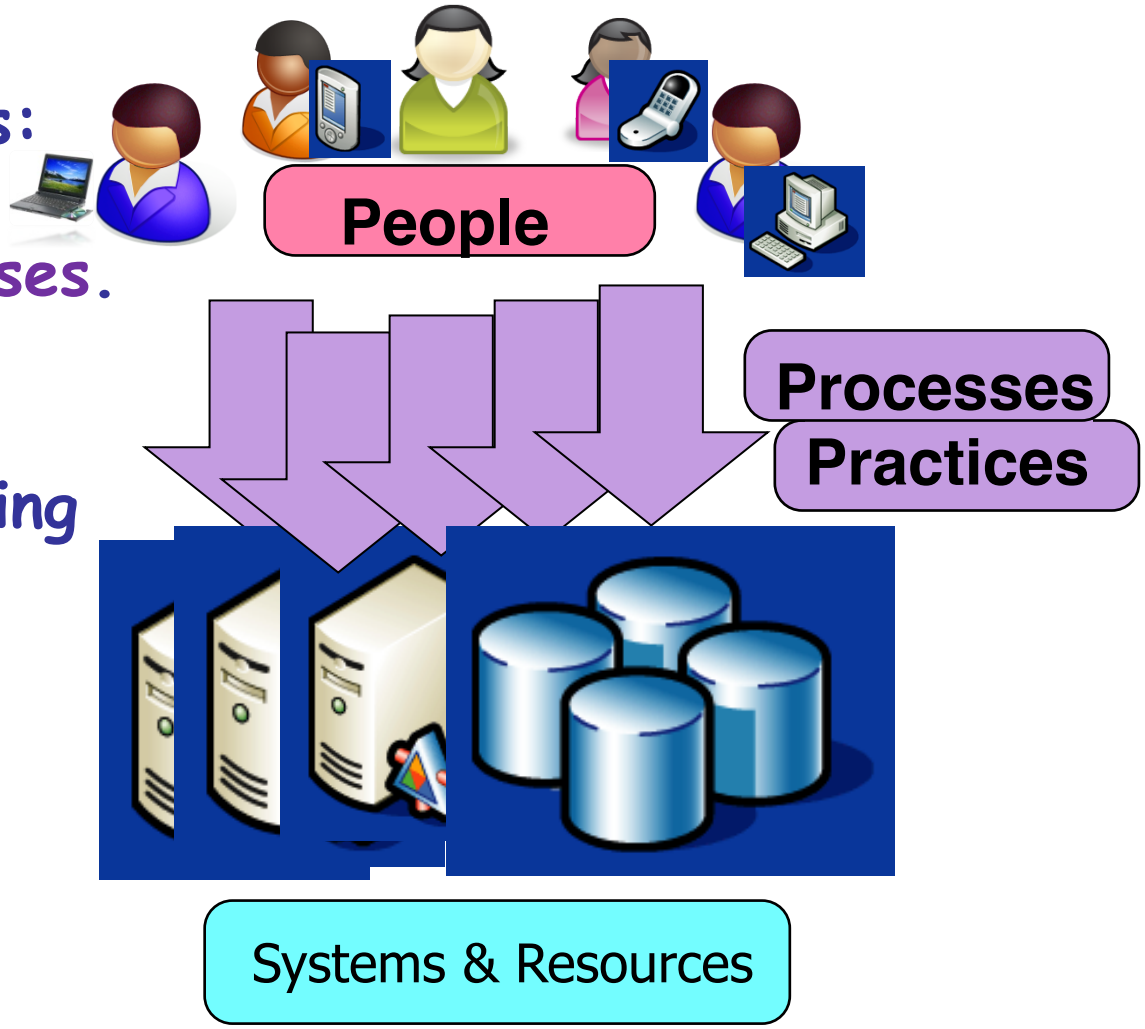
CTCPEC: the property that a product's services are accessible when needed and without undue delay

- IS 7498-2: the property of being accessible and usable upon demand by an authorised entity
- Denial of Service (DoS): The prevention of authorised access of resources or the delaying of time-critical operations

Information Assurance

- Wider scope includes: people, resources, technology and processes.

- Focus on understanding and applying good practices to achieve a holistic view of protection.



Questions???

Enabling Technical Concepts and Mechanisms