# INFT 5115 Security Principles

## Tenets of Cybersecurity

## CIA Triad



University of South Australia

# Tenets of Cybersecurity

- In this seminar we will discuss some of the tenets, or principles, of cybersecurity.
- This discussion is not intended to be comprehensive, but rather to launch our discussion of security principles.
- Additional tenets will be discussed as part of the topics remaining in the course.

# CIA Triad Definition

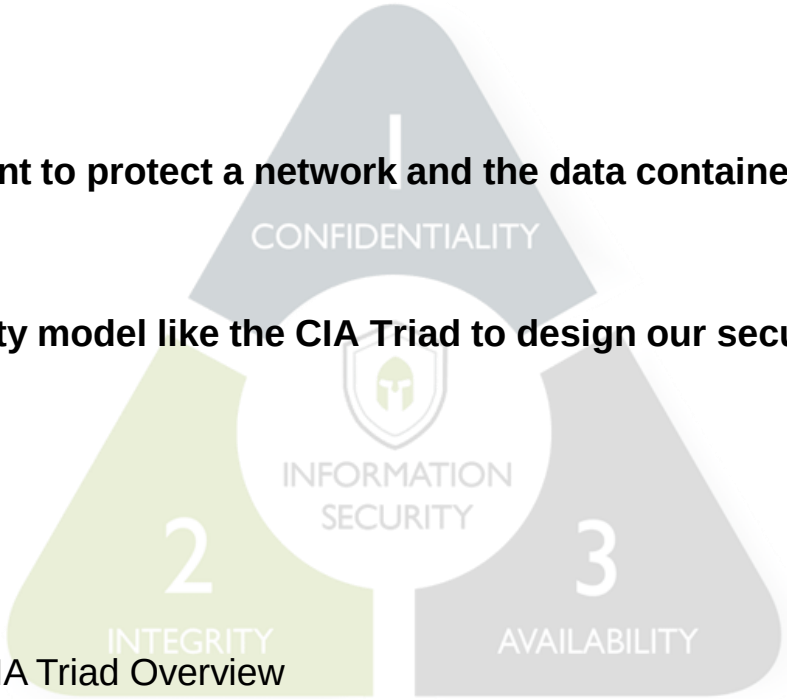
**Confidentiality, integrity and availability**, also known as the CIA triad, is a model designed to guide policies for information security within an organization.

**The Goal?**

**When we want to protect a network and the data contained within it.**

**The How?**

**Use a security model like the CIA Triad to design our security plan.**




See Activity 1 - CIA Triad Overview

# The CIA Triad

## Confidentiality

The theory….

"The property that information is not disclosed to unauthorized individuals, processes, or devices"[1].



[1]FIPS 140-2 cited in Kissel, R., 2013. Glossary of Key Information Security Terms. NIST Interagency Reports, NISTIR 7298.

# The CIA Triad

## Confidentiality

Providing this assurance can be described using three major steps.

**Step 1**

Information must have controls that are capable of preventing some users from accessing the information.

These controls must be sufficiently granular depending on the rationale for the access control.

The requirement for granularity is based partially on technical requirements and partially on benefits to the business.

Examples of how to achieve Confidentiality:

Data at rest and in transit uses data encryption
Access Control Lists
Non technical – Physical Security

Risks to Confidentiality:

Privilege Escalation
Employee Negligence
BYOD

**Discussion – If your system is broken into but the data cannot be read is this a breach of confidentiality?**

# The CIA Triad

## Step 2

It must be possible to limit access to information to authorised users.

Authorisation is defined as “access privileges granted to a user, program, or process or the act of granting those privileges” [1].

## Step 3

An authentication system must be in place to validate the identity of those requesting access to data.

Authentication is defined as “the process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data”.

Authentication generally prefaces authorisation decisions (i.e. the system must identify the user before it can determine which authorisations the user holds).

Examples:

Biometrics
2FA / MFA
Something you know (A username/Password)
Something you have (Smartcard)
Something you are (Fingerprint)

Risks:

Social Engineering
Phishing
Shoulder Surfing
Theft

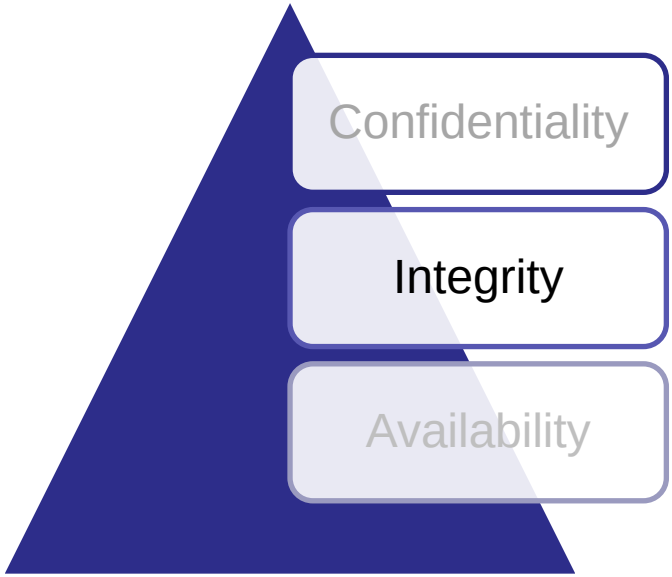


1FIPS 140-2 cited in Kissel, R., 2013. Glossary of Key Information Security Terms. NIST Interagency Reports, NISTIR 7298.

# The CIA Triad

## Integrity

Integrity commonly refers to maintaining the accuracy of data stored in a computer system.




***"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity"***

# The CIA Triad

Data is commonly made available for viewing by users, however they should not have the ability to change the data - For example, your course grades in myUniSA.

Questions to ask could be:

How correct is the information sent and/or received?
Has the data been modified during:

- Transit
- Retrieval
- At rest

**If data has been modified without permission do you have Non-repudiation**
"A*ssurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information*".

It describes processes for assuring the source of messages, and therefore preventing parties from later denying that they sent the message.

Example – Hacker imitates a lecturer to request a grade change for a student?

# Hashing Examples

**What can be used to guarantee correctness of data?**

MD5 - An MD5 hash function encodes a string of information and encodes it into a 128-bit fingerprint. MD5 is often used as a checksum to verify data integrity. However, due to its age, MD5 is also known to suffer from extensive hash collision vulnerabilities, but it's still one of the most widely used algorithms in the world.

Cisco routers clear text password

```
enable password ciscol23
```

The same password hashed using the MD5 hash

```
enable secret 5 $1$mERr$5.a6P4JqbNiMX0lusIfka/
```

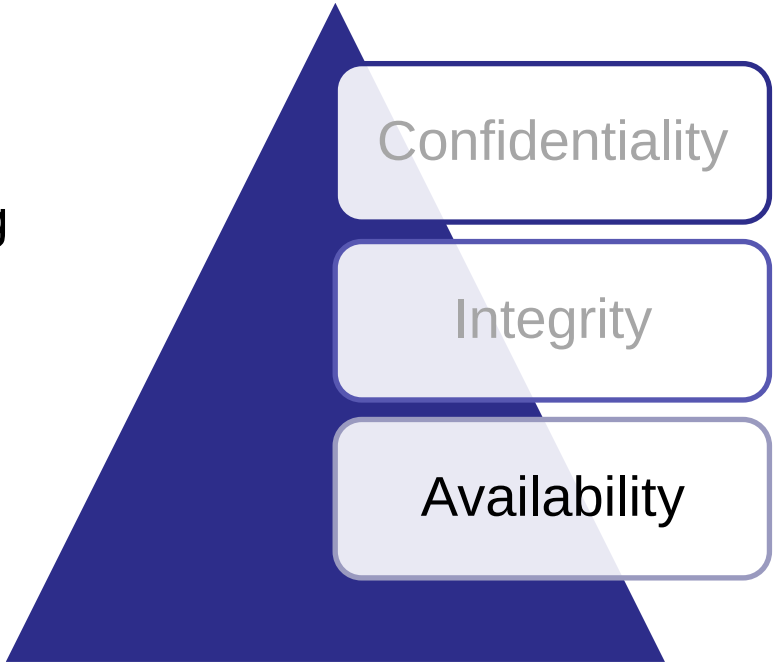
SHA-2 – SHA-2, developed by the National Security Agency (NSA), is a cryptographic hash function. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits.

CRC32 – A cyclic redundancy check (CRC) is an error-detecting code often used for detection of accidental changes to data. Encoding the same data string using CRC32 will always result in the same hash output, thus CRC32 is sometimes used as a hash algorithm for file integrity checks. These days, CRC32 is rarely used outside of Zip files and FTP servers.

# The CIA Triad

## Availability

"The property of being accessible and useable upon demand by an authorized entity."



# The CIA Triad

## Availability

Definition – Ensures that data is always accessible when and where it is needed.

There is limited utility in having a confidential and integral system if it is not available to authorised users.

This is the reason that ‘pulling the plug’ during a cyberattack is rarely an option.

Denial of Service (DoS) attacks, and its variants,  are one of the most common attacks that affect availability.

Examples of how to provide Availability:

Increase redundancy – how?
Backup strategies
Disaster recovery plan

Risks to availability

Hardware Failure
Denial of Service (DoS) attacks.
DDoS

# Group Discussion

Potential Impacts to the CIA Triad

Think of an example business and categorise each of the three elements of the CIA Triad in the following risk factors and impact on the organisation:

- Low
- Moderate
- High