The University of Guyana
Faculty of Natural Sciences

LECTURE 1

Computer and Information Security Fundamentals

(CSE 2203)

SEMESTER II (2018-2019)

Sandra Khan BSc MSc CISSP PG Dip Education (Higher Ed)

sandra.khan@uog.edu.gy

Before we begin..

- Please switch cell phones to silent

- Admin Issues
- Will be using Moodle to manage course
- Office Hours: (E29) Wednesdays 13:00 – 15:00 hrs

- ***Email:sandra.khan@uog.edu.gy***

Course Outline

Week 1 – Security Basics

Week 2 – Introduction to Cryptography

Week 3 - Authentication, Encryption (DES/RSA), Hashing

Week 4 - Integrity – Digital Certificates, Message Digests

Week 5 – Network and Internet Security

Week 6 - Internet Commerce, SSL, IPSec, Firewalls

Week 7 – VPN / IDS

Week 8 & 9 – Wireless Security

Week 10 – System Security

Week 11 – Access Control

Week 12 – Application Security

Week 13 – Cyber Crime

Learning Objectives

By the end of this lesson students will be able to:

- Define Information Security
- Define Computer Security
- Describe the major security goals (CIA Triad)
- Utilise the fundamental terminology and concepts of the discipline
- Explain the nature of the Computer and Information Security challenge and the scope and context of the discipline
- Evaluate a computer security incident scenario using industry standard terms.

What is Information Security? Cyber Security? Computer Security? Network Security?

Computer Security

“Computer security is the protection of the items you value, called the assets of a computer or computer system. There are many types of assets, involving hardware, software, data, people, processes, or combinations of these.”

“To determine what to protect, we must first identify what has value and to whom.”

(Pfleeger & Pfleeger, 2015)

QUESTIONS

Which of the answers best describes the discipline of information/cyber security?

a) An interdisciplinary course comprising elements of law, policy, human factors, ethics, and risk management
b) All of the answers combined.
c) A discipline that focuses on the creation, operation, analysis, and testing of secure computer systems.
d) A computing-based discipline involving technology, people, information, and processes

QUESTIONS

Which of the following best describes "information"?

a) A computing-based discipline involving technology, people, information, and processes
b) Data, such as census, medical or readings from sensors etc
c) A sequence of symbols that convey some meaning in a given context
d) A discipline developed by Claude Shannon in the 1940’s
Documents such as books, the content on the World Wide Web (WWW) etc

Why do we need Computer/Information Security?

https://www.dreamstime.com/stock-photo-information-security-word-cloud-white-background-image60618093

Why do we need Computer/Information Security?

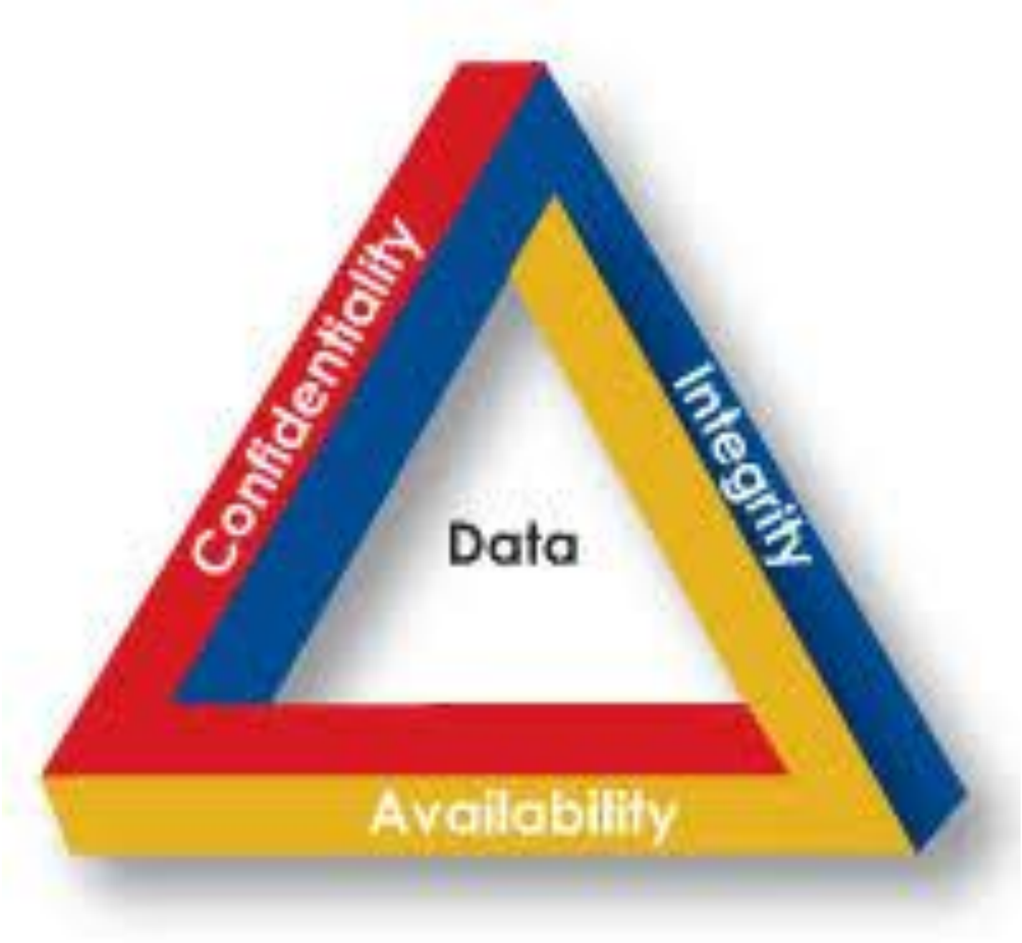
ID
PW
XX Bank
BANK
ID
PW

CONFIDENTIAL

To pay or not to pay...
Pay ransom and I'll free your PC!

https://www.ipa.go.jp/security/english/vuln/10threats2014_en.html

Security Goals – CIA TRIAD

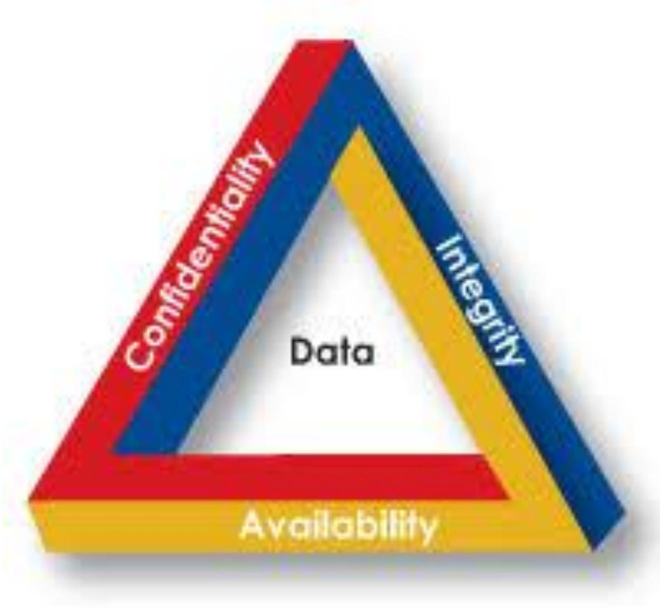


The purpose of Information Security is to protect your information's

- **Confidentiality**
- **Integrity**
- **Availability**

https://www.appliedtrust.com/resources/security/every-company-needs-to-have-a-security-program

Fundamental Principles



Confidentiality - the ability of a system to ensure that an asset is viewed only by authorized parties

Integrity - the ability of a system to ensure that an asset is modified only by authorized parties

Availability - the ability of a system to ensure that an asset can be used by any authorized parties

https://www.appliedtrust.com/resources/security/every-company-needs-to-have-a-security-program

Additional Security Goals

Privacy – A person's desire to limit the disclosure of personal Information.

Non-repudiation – is the assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data. (Protection from Non -deniability)

https://www.appliedtrust.com/resources/security/every-company-needs-to-have-a-security-program

CIA QUESTIONS

A third party (e.g. a spy) is not able to read a message when:

a) The message is using a cryptographic protocol to implement confidentiality
b) The message has high availability
c) The message is sent with integrity
d) The message is sent using a nonrepudiation technique

Komisarczuk, P., Martin, K. & Alis, J. (2019), Information Security: Context and Introduction [Coursera course]

Vulnerability – Threat – Control Framework

The goal of Computer / Information Security is to protect valuable information assets.

In the literature, there is a commonly used framework that describes how assets may be harmed and how to counter or **mitigate** that harm.

This framework is called the:

Vulnerability – Threat – Control Framework or Paradigm

Vulnerability – Threat

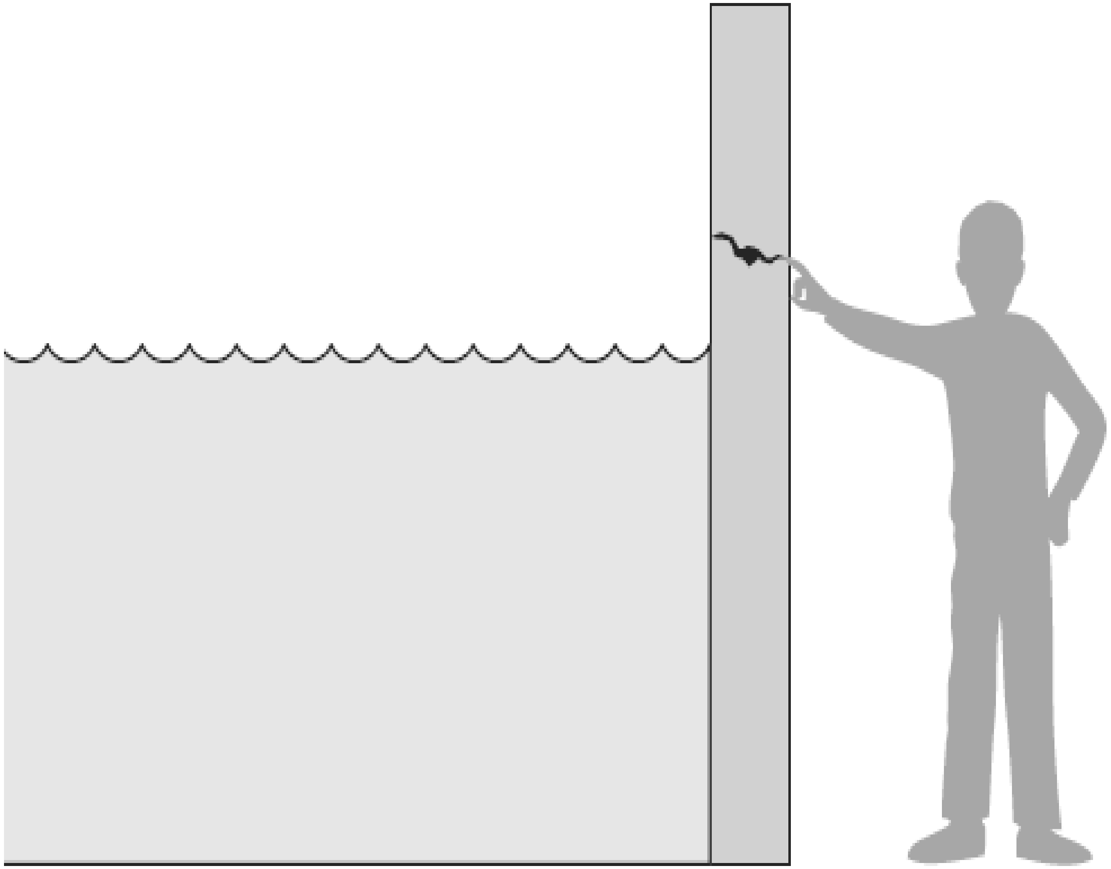


FIGURE 1-4 Threat and Vulnerability

A threat is a set of circumstances that can be exploited to cause harm.

Software threats are often referred to in the Literature as exploits.

Pfleeger et al (2015)

Vulnerability – Threat

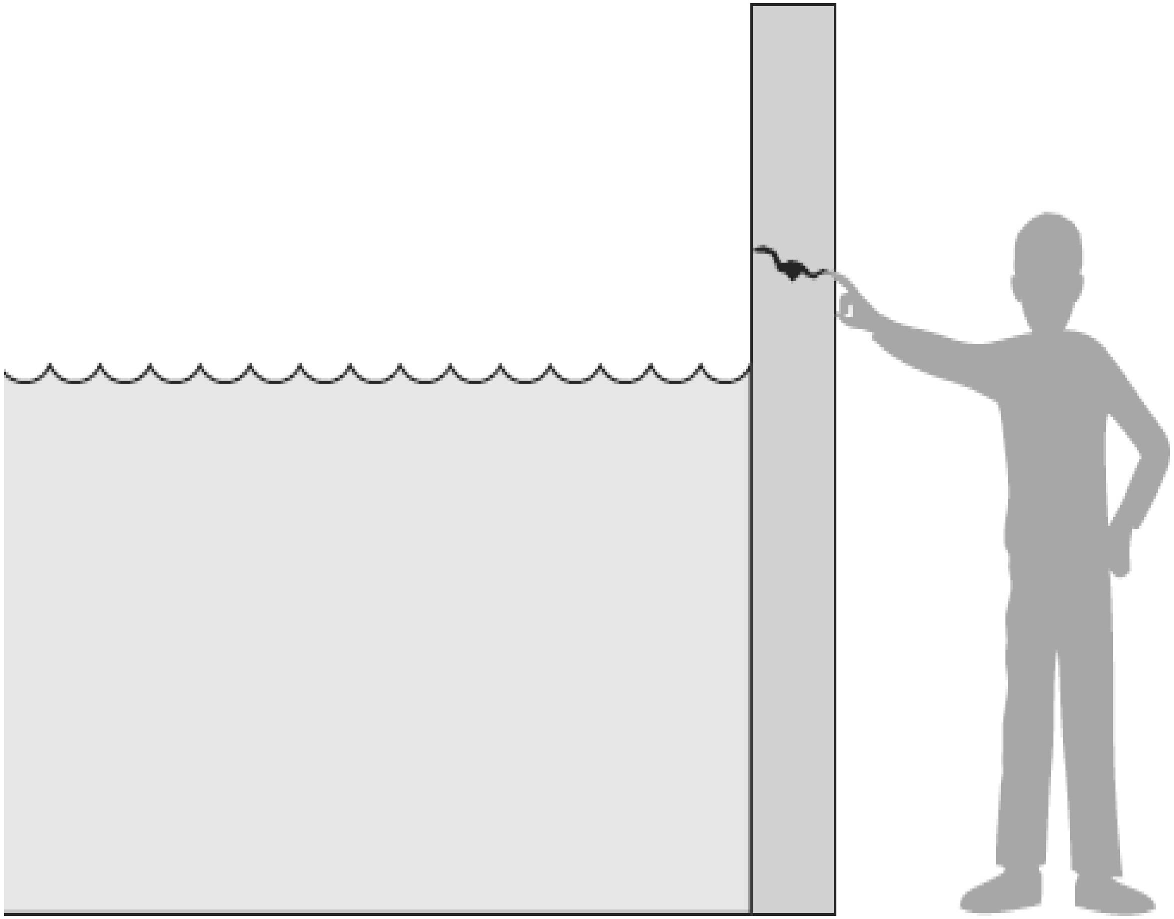


FIGURE 1-4 Threat and Vulnerability

Once there is a vulnerability or weakness, there is opportunity for an attacker to exploit and a corresponding RISK of a system failure / breach.

INCIDENTS can be malicious or unintentional or due to acts of nature.

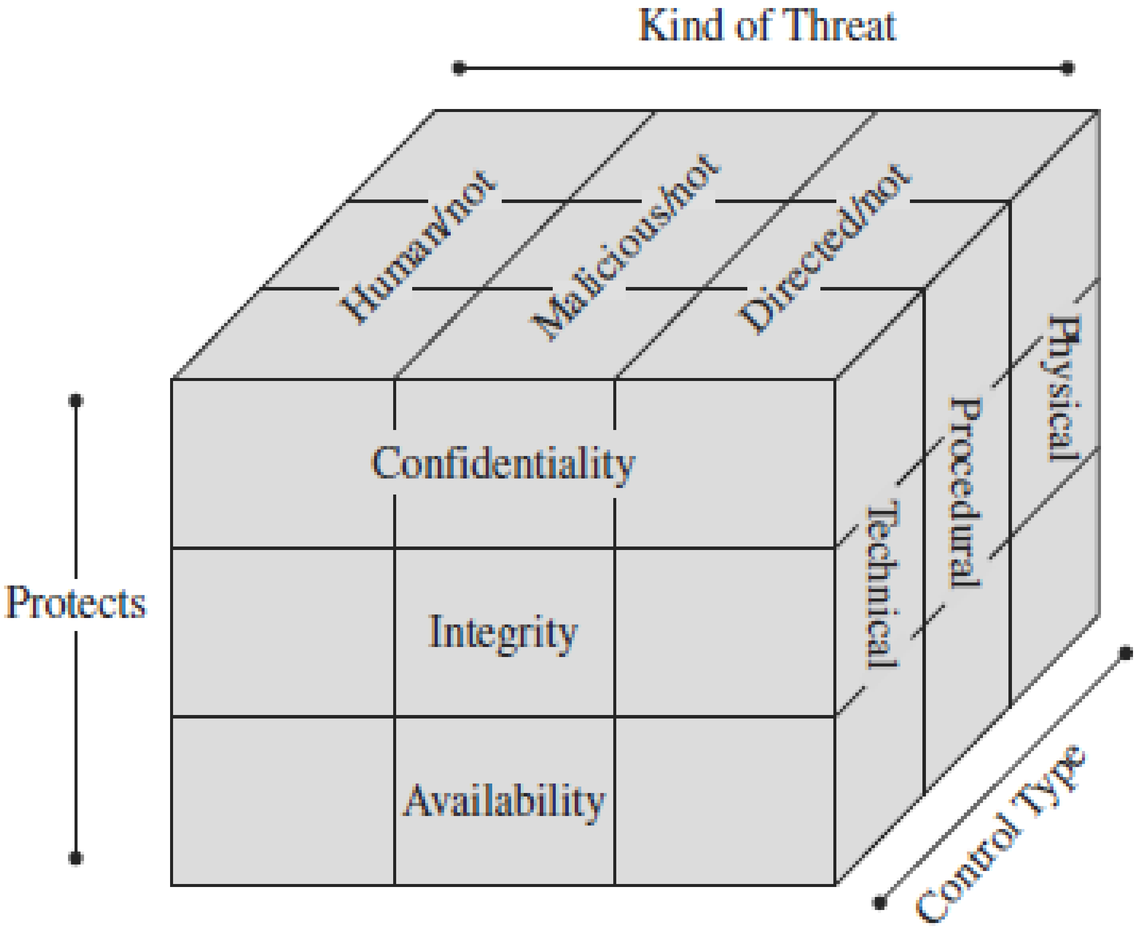
Pfleeger et al (2015)

Controls / Countermeasures

In order to prevent vulnerabilities from becoming incidents or being cxploited, we use controls or countermeasures as protection.

A control or countermeasure is an action, device, procedure or technique that removes or reduces a vulnerability.

Controls / Countermeasures



A ***control*** prevents ***threats*** from exploiting ***vulnerabilities***.

Vulnerability – Threat - Control

The Vulnerability – Threat – Control paradigm provides a framework to develop effective security policies to prevent attacks and reduce the risk to the enterprise / organisation.

So, a **threat** is blocked by **control** of a **vulnerability**.

Elements required for a successful attack

A malicious attacker must have three elements in place in order to facilitate his / her success:

- Method
- Opportunity
- Motive

This is often easily remembered using the acronym M-O-M

Deny any of the M-O-M, and an attack cannot succeed.

FURTHER INFORMATION

Course notes and references are available via Moodle.

Required Readings:

Pfleeger, C. P., & Pfleeger, S. L. (2015).
Security in computing: Chapter 1

Readings

Required Reading(s)

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing*. Prentice Hall Professional Technical Reference.

Stallings, W. (2006). *Cryptography and Network Security, 4/E*. Pearson Education India.

Recommended Reading(s)

Stallings, W. (2007). *Network security essentials: applications and standards*. Pearson Education India.

https://www.sans.org/security-resources/glossary-of-terms/

REFERENCES

Komisarczuk, P., Martin, K. & Alis, J. (2019), Information Security: Context and Introduction, Royal Holloway, University of London [Coursera course].

Martin,K.(2009). Intro to Cryptography [PowerPoint Presentation]. Retrieved from Royal Holloway ISG

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing.* Prentice Hall Professional Technical Reference.

End of Lecture 1