While you are waiting for the session to start, can you familiarise yourself with the OWASP website. Its link https://owasp.org/
What is OWASP is about etc?
Find any events that you can attend virtually

Introduction to Module

By

Dr. Imran Ullah Khan

Informatics, University of Sussex

Structure of the Module

Lectures:

Tuesday: 16:00-17:00, Zoom

Friday: 09-10am, Zoom

Labs:

Monday: 3-5pm, Zoom and Google sheet   By Aamir

Tuesday: 9-11am, Zoom and Google sheet by Zickey

Wednesday: 11-1pm, Zoom and Google sheet by Zickey

Friday: 3-5pm, Zoom and Google sheet   By Aamir

Any knowledge gained in this module, must NOT be applied to unauthorised targets.

Lectures and Labs

- Stay on mute
- Don't need to turn on the camera

- In Lab session

Lab assistant will be available in Zoom and Google sheet.

Any question you can ask either on Zoom or Google sheet.
Google sheet provide the option to be anonymous.

Assessment:

- 50% coursework

  Will be released in week 9

  You will have three weeks to complete it, end of

  week 11 Assignment Project Exam Help

  https://powcoder.com

- 50% final exam, Computer based Exam   (Jan 2020)

  Add WeChat powcoder

Both of these components will be discussed in detail in Week 7 when we will have covered a large part of the module.

Learning aims of the module

- Systematically discuss key dimensions of computer security (e.g. secrecy, authentication, integrity, anonymity), and their relationship to the main threats and attack techniques relevant to computer security.

- Systematically describe the main building blocks of cryptography (e.g. public and private key encryption, cryptographic hashing), and their relationship with the key dimensions of computer security from LO1.

- Deploy up-to-date tools and techniques for finding vulnerabilities in computer systems. Draft security policies and implement policy enforcement processes and mechanisms.

- Design secure computer systems by using established computer security principles.

This module is NOT about

- Ethical hacking

- Web penetration

- Network security

However, it does cover these things to some extent.

Once you have the basic knowledge and concepts are clear to you, you can build on the knowledge gained in this module.

Computer security is a huge topic, we can't cover everything.

Rough Schedule

1	2	3	4	5	6	7	8	9	10	11
Theory, Concepts, Types of Malwares etc		Cryptography		Software security including web security				Incident response	Security laws	Review

Module Covers

- Principles and basic concepts of security
- Cryptography including hashing
- Vulnerabilities of applications: XSS, SQLi, Buffer overflows etc
- Incident response: policies and frameworks
- Laws related to cyber crimes: GDPR, Fraud acts etc

  May cover digital forensic

  Security is a wide topic, can not cover everything

▼ Week1 - Introduction to the Module, Principles of Cyber Security, Attacks Types.

Lecture 1a & 1b

📄 1b - Read - Requirements, Principles and AttackTrees

🚀 Quiz01 - CIA, AttacksTypes
14 pts

Lab 1

📎 Lab-1 Concepts CIA.docx

📎 Lab-1 Concepts CIA - Solutions.docx

🔗 Reading List

Lab set up to cover software security

AWS	VirtualBox

✓ AWS – Amazon Web Services
✓ AWS educate account   vs   other account options
✓ Kali Linux
✓ Target
   a) Vulnerable web applications – DVWA
   b) Windows OS – running vulnerable application
 	
Advantages:
1) AWS is booming
2) AWS provides support though it is limited and only related to EC2 instances, still very useful
 	
Disadvantages:
1) Slowspeed – It is slow
2) Not lots of support in online forums/chats
3) Practice or testing without proper clear guidelines is hard
	✓ Virtual box
	✓ Kali linux
	✓ Targets
	   a) Web applications – DVWA
	   b) Windows OS – running vulnerable application
	
	Advantages:
	1) Fast
	2) Lots of online support, videos on YouTube, Will suit independent learner
	
	Disadvantages:
	1) I will not cover it directly in my lab notes as there are lots of support available. I will provide some useful references.

Job prospect of security experts

- Information security experts, cyber security, pen testing expert and security advisers etc.

- Market worth: UK market largest in Europe, $5.5 billion.

- General Data Protection Regulation (GDPR) will drive future spending on cyber security as companies seek to comply with the regulation.

Courses you might be interested

Free Open University course:

Introduction to Cyber Security

https://www.futurelearn.com/courses/introduction-to-cyber-security

- 8 Weeks and 3 hours per week
- Next intake check its date online
- £62 for unlimited access to resources and certificate of achievement
- APMG exam

Cyber security challenge

- https://www.cybersecuritychallenge.org.uk/

Companies bounty programs/Challenges

- https://www.microsoft.com/en-us/msrc/bounty
- https://developer.apple.com/security-bounty/
- Hundreds of bounty programs; Check for other SMEs

The NIST Internal/Interagency Report NISTIR 7298 (*Glossary of Key Information Security Terms* , May 2013) defines the term *computer security* as follows:

" Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated."
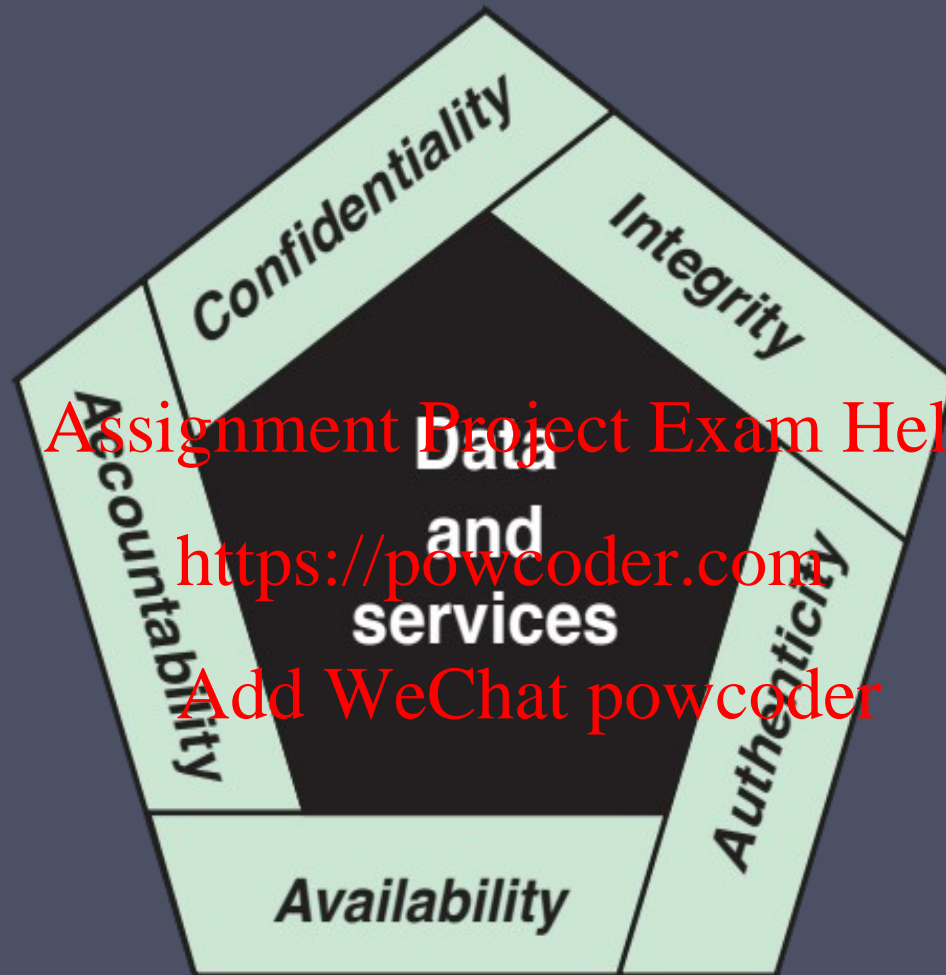
Figure 1.1 Essential Network and Computer Security Requirements

Key Security Concepts

Confidentiality

Integrity

Availability

- **Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information**

- **Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity**

- **Ensuring timely and reliable access to and use of information**