Faculty of Engineering & Information Technology

Introduction to Cybersecurity

Introduction

Asst. Prof. Dr. Ahmed A.O. Tayeh

Contact Details

- If nothing urgent, please contact me via emails
  - atayeh@israa.edu.ps
  - expect a reply in 24 hours
- Office Hours
  - Sunday 8 – 11 AM
  - Sunday 1 – 3 PM
  - Monday 8 – 10 AM
- Do not hesitate to discuss things during lecture breaks
- If questions are related to course topics, raise them during the lectures so others can learn

Study Material

- Slides are the main study material
- Lecture discussions and notes should be considered
- Reference Book "*Computer Security: Principles and Practice*" *3rd edition by William Stallings & Lawrie Brown*
  - course topics are not covered with the same order as the book
  - anything that is not covered during the lectures, are not part of the exam
- Study material uploaded before each lecture at the study portal and the course repository GitHub account
  - https://github.com/atayeh-israa-university/Intro-to-Cybersecurity-2023

Grading

- Midterm exam 30%
- Presence & assignments 20%
- Final exam 50% (*10-20% of the exam might be about your assignments!*)

Fundamental Concepts

- Security: protecting assets
  - buildings, universities, supermarkets
  - computers, data, identity, etc.

- Computer Security: concerns assets of computer systems; the information and services they provide

- Computer Security is quite vast in scope, touching many areas
  - network security
  - database security
  - …

Fundamental Concepts…

- Cybersecurity: “the ability to protect or defend Cyberspace from cyber-attacks” *(National Institutes of Standards Technology – NIST)*
- Cyberspace refers to the virtual word, especially the internet, which is the way computer systems connect
- Anything done via the use of internet occurs within the confines of the cyberspace

https://redsquid.co.uk/blog/how-to-promote-cyber-security-awareness-what-is-it-why-its-important/

Fundamental Concepts…

- Cyber-attack: an attack for disrupting, disabling, destroying or maliciously controlling a computer environment/infrastructure; or destroying the integrity of the data or stealing controlled information

https://www.vistainfosec.com/blog/cyber-attack-vectors-and-how-to-avoid-them/

Fundamental Concepts…

- Security
  - protect our valuable resources (i.e., data & information) in the same manner we secure our houses against thieves

- Safety
  - behave in ways that protect us against threats and risks that come with technology

Importance of Cybersecurity

- Our personal & private data are stored in computer systems
  - data on your computing devices
    - private images & videos
  - financial data
  - educational data
  - your identity
  - information online
  - employment data
  - medical data

- We need to protect our data and privacy!

Importance of Cybersecurity…

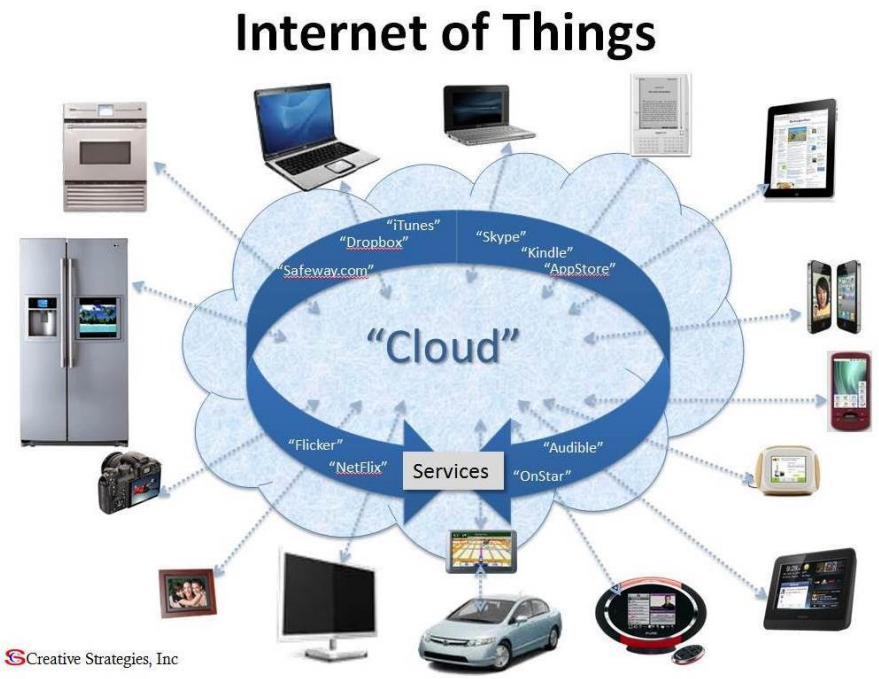
- Our personal & private data are in many systems that go beyond our control
  - doctors' computers
  - hospital's systems
  - bank systems
  - university systems

- Everyone behaviour and cyber hygiene affects others

- Cybersecurity is a shared responsibility!

Importance of Cybersecurity…

- Increase of the risks of attacks and threats
  - Cloud services
    - software hosted externally and available through the internet
  - Ransomware
    - malicious software blocks access to a computer until a sum of money is paid
  - Spear phishing
    - email appears to be from an individual or business that you know
  - The Internet of Things (IoT)
    - large network of physical objects such as sensors



https://ismguide.com/the-internet-of-things/

Importance of Cybersecurity…

- In case of an attack, you lose
  - reputation
  - personal information
  - private data
  - money
  - business discontinuity
  - wars!

- Cybersecurity is a shared responsibility!

Importance of Cybersecurity…

- Information is very valuable
  - helps in decision making
  - increased profits for companies
  - reduce time required to make important business decisions

- Organisations must protect their information & data

Victims of Cyber-Attacks

- Me & You!
- Governments
- Financial Institutions
- Energy Companies
  - Last week's attack against Gaza main electricity company
- Educational Institutions
- Businesses
- Social-Media Platforms

Attackers

- Hackers
- Cyber criminals
- Cyber spies
- Nation-States
- Malicious Insiders
- Hacktivists – hackers with political motives
- Script Kiddies

Attackers' tools

- Malicious Software (Malware) distribution
  - Infected documents
  - Emails
  - Viruses
  - …
- Network attacks
  - Denial of service
    - attackers seek to make a network resources unavailable by disrupting services
  - Man-in-the middle attack
    - alter the communications between two parties
  - Brute force attack
    - attacker submitting many passwords with hope of guessing correctly
  - …

Defenders

- Security Vendors
  - Firewalls
    - monitors and filters incoming and outgoing network traffic based on security policies
  - Anti-malware
    - used to prevent, detect and remove malware
  - …
- ICT Teams
- Governments
  - Laws
  - Policies
  - Prosecutions
- Everyone should be a defender

Organisational Data

- Traditional data
  - personal information
    - application materials, payroll, offer letters, employee agreements, etc.
  - intellectual properties
    - patents, trademarks and new product plans
  - financial data
    - income statements, balance sheets, cash flow statements, etc.

- Internet of Things and Big Data
  - more devices to protect
  - more data in each connected object
  - exponential growth of data

Organisational Data…

- Confidentiality of data is needed to the survival of organisations
  - restrict access to the information to authorised users (privacy)
- Integrity of data is needed to the survival of organisations
  - accuracy, consistency and trustworthiness of the data
  - data must be unaltered during transit and not changed by unauthorised entities
  - version control can be used to prevent accidental changes by authorised users!
- Availability of data is needed to the survival of organisations
  - ensure the availability of the network, services and data to the authorised users
  - plans should be in place to recover quickly from any disaster

Organisational Data…

- CIA Triad is a guideline for information security for any organisation to
  - protect data
  - keep data accurate
  - data accessible to authorised users

https://www.wallarm.com/what/cia-triad-definition

Thank You!