Networks and Systems Security
Week 01
Foundations of Computer Security

Aims of the Seminar

Welcome to the Foundations of Computer Security. This workshop is designed for you to learn about the fundamental concepts of computer security. The aim is to build on the lecture material of giving you a practical understanding of security needs and technologies.

By the end of this workshop, you will be able to:

- Discuss computer security concepts in practical contexts
- Apply the **Confidentiality, Integrity, and Availability (CIA) Triad** to analyse security scenarios
- Differentiate between **passive and active security attacks**
- Identify fundamental security design principles and key terminology

Workshop Outline:

1. Confidentiality, Integrity, and Availability
2. Assessment First Step

Feel free to discuss your work with peers, or with any member of the teaching staff.

Reminder

We encourage you to discuss the content of the workshop with the delivery team and any findings you gather from the session.

Workshops are not isolated, if you have questions from previous weeks, or lecture content, please come and talk to us.

Exercises herein represent an example of what to do; feel free to expand upon this.

Helpful Resources

NCSC Annual Review 2021
https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202021.pdf

Cybersecurity Framework

https://www.nist.gov/cyberframework

The Internet Society

https://www.internetsociety.org/

1. Confidentiality, Integrity, and Availability

In small groups, analyse the following scenarios. For each one, identify the primary principle of the CIA Triad being violated: Confidentiality, Integrity, or Availability.

Be prepared to justify your answer.

- **Confidentiality**: Preserving authorized restrictions on information access and disclosure.
- **Integrity**: Guarding against improper information modification or destruction.
- **Availability**: Ensuring timely and reliable access to and use of information.

Case Studies

A. The 2017 Equifax Data Breach

- What happened: A massive data breach at one of the largest credit bureaus in the United States. Attackers gained unauthorized access to the personal and financial data of nearly 150 million people.

B. The Stuxnet Worm

- What happened: A highly sophisticated computer worm designed not just to steal information, but to cause physical damage. It specifically targeted the control systems of Iranian nuclear centrifuges, causing them to subtly malfunction and destroy themselves.

C. The 2016 Dyn DNS DDoS Attack

- What happened: A massive "Denial of Service" attack that targeted a major internet infrastructure company called Dyn. The attack flooded Dyn's servers with traffic, making a large number of major websites and online services—such as Twitter, Spotify, and Reddit—unavailable for hours across Europe and North America.
- Keywords for research: "Dyn DDoS attack 2016," "Mirai botnet," "denial of service attack."

D. The 2021 Colonial Pipeline Ransomware Attack

- What happened: A ransomware attack forced the shutdown of the largest fuel pipeline in the United States, which supplies nearly half of the East Coast's fuel. The shutdown lasted for several days, leading to widespread fuel shortages and panic buying. The company paid a multi-million dollar ransom to the attackers to receive a decryption tool and restore operations.

- Keywords for research: "Colonial Pipeline ransomware," "DarkSide ransomware," "critical infrastructure attack."

E. The 2023 MOVEit Supply Chain Attack

- What happened: A Russian-affiliated cybercriminal group exploited a previously unknown ("zero-day") vulnerability in a popular file transfer software called MOVEit. This allowed them to steal massive amounts of sensitive data from thousands of organizations worldwide that used the software, including government agencies, financial institutions, and major corporations like the BBC and British Airways.
- Keywords for research: "MOVEit data theft," "Cl0p ransomware gang," "zero-day vulnerability."

F. The 2020 SolarWinds Supply Chain Attack

- What happened: State-sponsored hackers compromised the software build process of a major IT management company, SolarWinds. They secretly inserted malicious code into a legitimate software update for the company's "Orion" platform. This trojanized update was then unknowingly distributed to over 18,000 SolarWinds customers, allowing the attackers to gain long-term, stealthy access to the networks of numerous government agencies and private companies.
- Keywords for research: "SolarWinds hack explained," "Sunburst backdoor," "software supply chain attack."

Discussion Questions

1. Primary Impact: Which single principle of the CIA Triad was most significantly compromised in your chosen incident? Was it a loss of Confidentiality, Integrity, or Availability?
2. Justification: Explain *why* you chose that principle as the primary one. What specific outcomes of the attack support your conclusion?
3. Secondary Impacts: Were any of the other two CIA principles also affected, even to a lesser degree? If so, how?

Be Prepared: Nominate a spokesperson to share a 2-minute summary of your group's analysis with the class.

2. Assessment Introduction

Conduct focused research on your target career path and assess your readiness for the job market.

Activity Steps

Step 1: Search for Job Openings

- Visit job posting websites (e.g., LinkedIn, Indeed, Glassdoor, company career pages)
- Search for a specific job title that interests you
- Select and save **at least 3 different job openings** from different companies
- Ensure the positions are suitable for recent graduates or entry-level professionals

Step 2: Review Job Descriptions

For each of the 3 job openings:

- Read the complete job description carefully
- Note the responsibilities and duties listed
- Identify the required skills, qualifications, and experience
- Pay attention to any preferred qualifications or "nice to have" skills

Step 3: Research the Companies

For each company advertising the openings:

- Visit the company website and research their mission, values, and culture
- Look at employee reviews on sites like Glassdoor (if available)
- Check their social media presence and recent news
- Consider factors such as: company size, industry reputation, location, growth potential

Then answer: Is this company a good fit for you? Why or why not? Consider:

- Does their mission align with your values?
- Would you enjoy the work environment?

- Does the company offer growth opportunities?
- Is the location/remote work policy suitable for you?

Step 4: Skills Gap Analysis

Create a table with the following columns:

- **Required Skill/Qualification**
- **I Have This Skill** (Yes/No/Developing)
- **Evidence/Example**
- **How to Develop** (if you don't have it)

List all the skills mentioned across your 3 job postings and honestly assess:

- Which skills do you currently possess?
- Which skills are you still developing?
- Which skills do you lack entirely?
- What steps can you take to acquire missing skills?

Deliverable

By the end of today's workshop, submit a brief document containing:

1. Links to your 3 selected job postings
2. Company research summary for each (2-3 sentences per company on whether it's a good fit)
3. Your completed skills gap analysis table
4. A short action plan (bullet points) identifying the top 3 skills you need to develop

The end 😊