BLOOMING

Inclusion and Diversity in STEAM

Lesson Plan
Securing the Future: Understanding Network Security and Cryptography

---

Objective:

- Students will learn the basics of network security, including common threats, the importance of encryption, and methods for protecting data during transmission. The lesson will introduce key concepts such as cryptography, quantum-resistant security, and real-time attack detection.

Materials:

- Projector for slides on network security concepts
- Handouts on common network attacks (man-in-the-middle, denial of service, phishing, etc.)
- Laptops or computers for a simulated network security exercise
- Network security tools/software (e.g., Wireshark, basic encryption tools)
- Internet access for researching network vulnerabilities and defenses

---

Background Information:

Network security refers to the practices and technologies designed to protect the integrity, confidentiality, and availability of data as it is transmitted over networks. As cyberattacks grow more sophisticated, it's essential to implement robust security measures such as encryption, firewalls, and real-time attack detection. Emerging threats, such as quantum computing, pose new challenges

Co-funded by the European Union

Erasmus+
Enriching lives, opening minds.

to traditional cryptographic methods, making quantum-resistant cryptography an important field of study.

1. Introduction to Network Security (15 minutes):
   - Start with an overview of why network security is crucial in today's digital age. Explain how networks are vulnerable to various types of attacks, including man-in-the-middle (MITM) attacks, denial of service (DoS), and phishing.
   - Introduce basic terms like encryption, firewalls, and network protocols, and discuss the importance of ensuring that data transmitted over networks is secure.
   - Mention the emerging challenge of quantum computing, which threatens traditional cryptographic systems.

2. Common Network Attacks and Defenses (20 minutes):
   - Divide the class into small groups and assign each group a common network attack (e.g., MITM, DoS, phishing, or SQL injection).
   - Ask each group to research and present the following:
     - How the attack works
     - The potential damage it can cause
     - Methods for preventing or mitigating the attack (e.g., using encryption, firewalls, or multi-factor authentication)
   - After each presentation, discuss the importance of security protocols that can detect and prevent these types of attacks.

3. Hands-on Activity: Simulating Network Traffic and Attack Detection (30 minutes):
   - Set up a simulated network using a network security tool like Wireshark.

- Have students observe normal and malicious network traffic to understand how attacks like MITM and DoS can be detected.
- Instruct students to identify potential vulnerabilities in the simulated network and suggest possible defenses, such as stronger encryption or network segmentation.
- Guide students through encrypting data (e.g., using basic encryption software) and demonstrate how encrypted data is protected during transmission.

4. Exploring Quantum-Resistant Cryptography (15 minutes):
   - Introduce the concept of quantum computing and why it poses a threat to current encryption methods (traditional cryptography like RSA and ECC).
   - Discuss quantum-resistant cryptography and how it uses algorithms designed to withstand quantum-level attacks.
   - Explain how researchers like Dr. Anca Jurcut are developing these quantum-resistant algorithms to ensure the future of secure communications.

Visualize and Discuss:

- After the simulation, use a flipchart or whiteboard to create a visual map of different network security layers (firewalls, encryption, intrusion detection systems, etc.). Discuss how these layers work together to create a secure network.
- Ask students to consider how security protocols might evolve as technologies like quantum computing become more widespread, and how real-time attack detection will play a key role in future network security.

Additional Discussion Points:

- Applications of Network Security: Discuss how network security is critical in various sectors like banking, healthcare, government, and even personal use (e.g., securing online transactions, email, and social media).
- The Future of Cryptography: Engage students in a discussion on the potential future of cryptography and how quantum-resistant algorithms will safeguard data in the era of quantum computing.
- Ethical Hacking: Introduce the concept of ethical hacking, where security experts intentionally test networks for vulnerabilities to strengthen defenses.

Assessment:

- Ask students to write a reflection on:
    1. What network attack they found most dangerous and why.
    2. How encryption protects data during transmission.
    3. Why quantum computing presents a challenge to current cryptography methods and how quantum-resistant cryptography helps overcome this challenge.
- Evaluate group presentations and participation in the hands-on activity. Assess their ability to detect attacks and propose defenses.