Topics

- Basic concepts: Data and information, Acquisition process
- Data protection and data security, Threats: Viruses, human factor
- Data loss and corruption
- User authentication methods, Passwords, encryption.
- Protection of privacy, destruction of data
- Network security knowledge: protocols, devices, network attacks
- Virtual private networks
- Ethical hacking
- Design and implement secure applications

Schedule

Week #	Lecture	Labor
Week 1	Basic concepts	Labor usage, handouts requirements
Week 2	Security design principles	Functional and architectural design of coding task 1.
Week 3	Security design walkthrough	Functional and architectural design of coding task 2.
Week 4	Introduction to Kali Linux	Basic commands
Week 5	Working with Kali Linux	Coding - safe logon and user management
Week 6	Python security tools	Coding - safe document storage
Week 8	Bank Holiday	Bank Holiday
Week 9	Malicious code	Virus and malwae checking tools
Week 10	Cryptography	Kali password storing functions
Week 11	Security coding walkthrough	Coding task pre-evaluation
Week 12	Test	coding task pre-evaluation
Week 13	Presentations of coding assignments	Presentations of coding assignments
Week 13	Evaluation	Presentations of coding assignments

Textbooks

- Stallings, W., Brown, L. (2015): Computer security: principles and practice 3rd edition, Pearson Education, 978-0-13-377392-7
- Matt Bishop (2019): Computer Security Art and Science, Pearson Education 978-0-321-71233-2
- Alan G. Konheim: Computer Security and Cryptography (Wiley, 2007, ISBN: 978-0-471-94783-7)
- John R. Vacca: Computer and Information Security handbook (Morgan Kaufmann, 2009, 844 pages, ISBN 978-0-12-374354-1)
- Simon Singh: The code book ISBN 0385495323
- James M. Stewart, Mike Chapple, Darril Gibson - CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, 2015, ISBN 1119042712
- Tony Hsiang-Chih Hsu - Practical Security Automation and Testing: Tools and techniques for automated security scanning and testing in DevSecOps, 2019, ISBN 1789802024
- Vijay Kumar Velu,Robert Beggs : Mastering Kali Linux for Advanced Penetration Testing: Secure your network with Kali Linux 2019.1 – the ultimate white hat hackers' toolkit, Packt Publishing Ltd, 2019. jan. 30
- Daniel Regalado, Shon Harris, Allen Harper, Chris Eagle, Jonathan Ness, Branko Spasojevic,

Ryan Limm, and Stephen Sims: Gray Hat Hacking: The Ethical Hacker's Handbook
- Andrew S. Tanenbaum - David J. Wetherall: Computer networks, ISBN:978-0132126953
- Kevin Mitnick: The Art of Invisibility
- Chris Wysopal: Art of Software Security Testing, The Identifying Software Security Flaws, ISBN 0321304861

Task

Objective: The objective of this task is to design, implement, and analyze a secure file storage system. The system should ensure the confidentiality, integrity, and availability of stored files. Additionally, students are required to explore and implement encryption techniques, access controls, and other security measures to protect sensitive data

1. System Design: Define the requirements and functionalities of the secure file storage system. Design the architecture, specifying components such as servers, databases, and client interfaces. Clearly outline the security objectives (confidentiality, integrity, availability). Encryption Implementation:

2. Algorithms: Choose a suitable encryption algorithm(s) for securing stored files. Implement encryption and decryption mechanisms to protect the confidentiality of files. Discuss the key management strategy to securely handle encryption keys.

3. Access Control and Authentication: Implement access controls to restrict file access based on user roles and permissions. Integrate a robust authentication mechanism to verify the identity of users. Consider multi-factor authentication for enhanced security.

4. Audit Trail and Logging: Implement logging mechanisms to record user activities and file access. Create an audit trail for monitoring and analysis of security incidents. Discuss how the audit trail can be used for forensic purposes.

5.Data Integrity and Redundancy: Implement mechanisms to ensure the integrity of stored files. Explore techniques for redundancy and data backup to ensure availability. Discuss the recovery plan in case of data loss or system failure.

6. User Interface and User Experience: Develop a user-friendly interface for uploading, downloading, and managing files securely. Ensure that the user interface promotes security best practices and guides users on secure behavior.

7.Security Analysis: Conduct a thorough security analysis of the implemented system. Perform penetration testing to identify vulnerabilities and propose mitigation strategies. Provide a detailed report on the overall security posture of the system.

8. Documentation and Presentation: Document the entire design and implementation process. Prepare a presentation highlighting key features, security measures, and the rationale behind design choices.

Evaluation Criteria:

Functionality (30%): Successful implementation of encryption, access controls, and authentication.

File upload/download functionality. Proper error handling and user feedback.

Security Measures (30%): Effectiveness of encryption techniques. Robustness of access controls and authentication. Quality of logging and audit trail.

User Interface (15%): User-friendly design. Clarity in guiding users on secure practices.

Security Analysis (15%): Thoroughness of security analysis. Effectiveness of mitigation strategies.

Documentation and Presentation (10%): Clarity and completeness of documentation. Quality of the presentation and ability to articulate key points.

Handouts

1. Software System Security
2. Week 1-2
3. Week 3-4
4. Week 5-6
5. Week 7-8
6. Week 9-10
7. Week 11-12
8. Week 13-14

Test Questions

1. Define computer security
2. Explain Confidentiality, Integrity and Availability
3. What are the challenges in Computer Security
4. Define attack types
5. Define Threats, Attacks, and Assets
6. Explain Security Requirements
7. Explain Fundamental Security Design Principles
8. Explain Computer Security Strategies
9. Define the basic concepts of cryptographic algorithms: Plaintext, Encryption algorithm, Secret key, Ciphertext, Decryption algorithm
10. Explain Message Authentication and Hash Functions
11. Explain Public-Key Encryption
12. Explain Digital Signatures and Key Management
13. How can public-key encryption be used to distribute a secret key?
14. Explain DES algorithm
15. Explain AES algorithm
16. Explain MD5 algorithm
17. Explain Message Authentication Code
18. What are Malicious software ? What Harm do they cause ? What are the prevention actions you recommend?
19. Explain network penetration testing
20. Define Fundamental Security Design Principles