Task – 3

Lockpick: Problem Statement

Created By

Sanjay Sharma - 2065

1. Physical Lockpicking (Mechanical Security Systems)

Problem Statement

Mechanical locking systems are widely used to secure physical assets; however, many traditional locks rely on predictable internal mechanisms such as pin-tumbler designs. Due to manufacturing tolerances, material wear, and design limitations, these locks can often be manipulated without the original key. The problem is to identify and analyze the vulnerabilities present in mechanical locks that allow unauthorized access through lockpicking techniques, highlighting the need for improved physical security designs.

2. Cybersecurity and Digital Access Control

Problem Statement

Digital systems depend heavily on authentication and authorization mechanisms to restrict access to sensitive resources. Lockpicking in cybersecurity refers to bypassing these mechanisms without valid credentials by exploiting weaknesses such as weak password policies, flawed authentication logic, improper session management, or system misconfigurations. The problem focuses on identifying such vulnerabilities and assessing their impact on system confidentiality, integrity, and availability.

3. Software Application Security

Problem Statement

Modern software applications implement logical locks to control user access to features and data. These controls may fail due to insecure coding practices, insufficient input validation, or incorrect access control logic. The lockpicking problem in software security involves analyzing application workflows to detect methods through which attackers can bypass restrictions and gain unauthorized privileges, leading to data leakage or functional abuse.

4. Network Security and Infrastructure Protection

Problem Statement

Networks employ security mechanisms such as firewalls, authentication gateways, and access control lists to prevent unauthorized communication. Lockpicking at the network level occurs when attackers exploit misconfigured rules, weak authentication, or outdated protocols to bypass network defenses. The problem is to evaluate network security configurations and identify entry points that allow unauthorized access to protected network segments.

5. Operating System and Privilege Management

Problem Statement

Operating systems enforce access control through user roles and privilege separation. Lockpicking in this context refers to exploiting vulnerabilities that allow a user to bypass permission boundaries and obtain elevated privileges. The problem involves analyzing privilege enforcement mechanisms to identify weaknesses that could result in unauthorized administrative access.

6. Cryptographic Locking Mechanisms

Problem Statement

Cryptographic systems act as digital locks to protect sensitive information. The lockpicking problem arises when poor key management, weak encryption parameters, or flawed implementations enable attackers to bypass cryptographic protections without directly breaking the underlying algorithms. This problem emphasizes the importance of secure cryptographic design and proper implementation practices.

7. IoT and Smart Lock Systems

Problem Statement

IoT-based smart locks integrate physical security with digital communication technologies. These systems often suffer from vulnerabilities such as insecure firmware, weak wireless encryption, and insufficient authentication mechanisms. The problem involves assessing the security of smart lock systems to identify weaknesses that could allow remote or physical unauthorized access.

8. Capture The Flag (CTF) and Security Training Environments

Problem Statement

In controlled training environments such as CTF competitions, lockpicking challenges simulate real-world security weaknesses. The problem requires participants to analyze a protected system, identify vulnerabilities, and bypass access controls to retrieve restricted information. This helps in developing practical security assessment and exploitation skills while maintaining ethical boundaries.

9. Security Assessment and Forensic Research

Problem Statement

Lockpicking is a critical activity in security assessment and forensic research, where professionals evaluate the effectiveness of security mechanisms under controlled conditions. The problem is to systematically test locks and access controls to identify vulnerabilities before they can be exploited by malicious actors, thereby strengthening overall security posture.

10. Ethical and Legal Considerations

Problem Statement

While lockpicking techniques are valuable for security testing and research, they pose ethical and legal challenges if misused. The problem lies in ensuring that lockpicking knowledge is applied strictly within authorized and lawful contexts, balancing the need for security awareness with responsible and ethical use.