Task – 3

Lockpicking: Problem Statement

Created By

Rahul Gouda - 2069

1. Advanced Mechanical Lock Design and Security

Problem Statement

Mechanical locking systems continue to be deployed across residential, commercial, and industrial environments. However, advancements in precision tools, material analysis, and manufacturing consistency have made many traditional lock designs susceptible to manipulation. The problem is to examine how evolving mechanical technologies influence the effectiveness of lockpicking methods and to identify design weaknesses that allow unauthorized access, emphasizing the need for innovation in physical lock engineering.

2. Transition from Physical Locks to Electronic Locks

Problem Statement

The replacement of purely mechanical locks with electronic and keypad-based locking systems has transformed physical security mechanisms. While these systems reduce dependency on traditional keys, they introduce vulnerabilities related to electronic components, logic flaws, and configuration errors. The problem is to analyse how this technological transition impacts unauthorized access methods and how security controls can be strengthened to prevent system bypass.

3. Smart Locks and Embedded Systems Security

Problem Statement

Smart locks rely on embedded systems, sensors, and software-controlled mechanisms to manage physical access. Vulnerabilities in embedded firmware, memory handling, or hardware interfaces can allow attackers to bypass lock functionality without legitimate authorization. The problem is to assess embedded system weaknesses in smart locks and determine how secure design principles can reduce the risk of unauthorized manipulation.

4. Wireless Communication Technologies in Lock Systems

Problem Statement

Modern locking systems increasingly use wireless technologies such as Bluetooth, Wi-Fi, and RFID for access control. These communication channels can be exploited through interception, replay attacks, or unauthorized pairing if not properly secured. The problem is to evaluate the impact of wireless communication technologies on lock security and to identify measures that prevent unauthorized access through wireless exploitation.

3. Biometric Lock Systems and Security Limitations

Problem Statement

Biometric locking systems use physiological and behavioural traits to control access. Despite their convenience, these systems face challenges such as biometric spoofing, data leakage, and false authentication. The problem is to identify vulnerabilities in biometric lock technologies and assess how cybersecurity measures can improve the reliability and privacy of biometric access control systems.

5. Smart Lock Integration with Cloud Services

Problem Statement

Many smart lock systems rely on cloud platforms for access management and monitoring. Insecure APIs, weak access policies, or service outages can affect lock availability and security. The problem is to evaluate risks introduced by cloud integration in smart lock systems and their impact on physical access control.

6. Digital Credentials and Authentication Mechanisms

Problem Statement

Digital locks replace physical keys with credentials such as PINs, mobile applications, or biometric identifiers. Weak authentication logic, improper credential storage, or insufficient revocation mechanisms can allow attackers to gain unauthorized access. The problem is to identify weaknesses in digital authentication mechanisms used in lock systems and evaluate how robust cybersecurity controls can improve access reliability.

7. Firmware Updates and Secure Lock Operation

Problem Statement

Smart locks rely on firmware updates to introduce new features and security patches. Insecure update mechanisms may allow attackers to install malicious firmware, permanently compromising lock behaviour. The problem is to assess firmware management processes in modern locking systems and determine how secure update mechanisms can prevent unauthorized modification.

8. Integration of Artificial Intelligence in Lock Systems

Problem Statement

Artificial intelligence is increasingly used in lock systems for access pattern analysis and anomaly detection. At the same time, attackers may use AI to identify lock weaknesses and automate bypass techniques. The problem is to examine the dual role of AI in lock security and evaluate how defensive cybersecurity applications can counter AI-assisted lock exploitation.

9. Cybersecurity Monitoring and Intrusion Detection in Locks

Problem Statement

Traditional mechanical locks provide no visibility into tampering or unauthorized access attempts. Smart locks can generate logs and alerts, but poor implementation limits their effectiveness. The problem is to evaluate how cybersecurity monitoring and intrusion detection mechanisms enhance lock security and support forensic analysis after access violations.

10. Cybersecurity Standards and Regulatory Challenges in Lock Systems

Problem Statement

The absence of universally enforced cybersecurity standards for electronic and smart locks results in inconsistent security levels across products. Consumers often lack the ability to assess the security quality of locking systems. The problem is to analyse how standardization and regulatory frameworks can improve cybersecurity practices within the lock industry.

11. Mobile Application Security for Lock Control

Problem Statement

Mobile applications are commonly used to manage and control smart locks. Security flaws such as insecure storage, weak session handling, or improper authentication can expose locks to unauthorized control. The problem is to assess security risks associated with mobile-based lock management applications.