

SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF CYBER SECURITY

QUESTION BANK



VII SEMESTER

CY3761-SECURITY IN MOBILE EXPLOITATION

Regulation – 2023

Academic Year 2026 – 27 (Odd Semester)

Prepared by

Ms. K. R. Nandhashree, Assistant Professor (O.G)/CYS



SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203.



DEPARTMENT OF CYBER SECURITY

QUESTION BANK

SUBJECT CODE & NAME: CY3761-SECURITY IN MOBILE EXPLOITATION

SEM / YEAR: VII Sem/ IV Year

UNIT I – INTRODUCTION TO MOBILE SECURITY

Overview of mobile security landscape--Importance of mobile security -Mobile operating systems and their vulnerabilities-Common attack vectors on mobile devices --Legal and ethical considerations in mobile security-- Impact of mobile exploits on personal and enterprise security--Introduction to mobile malware and its types.

PART A

Q. No	Questions	BT Level	Competence
1	Define Mobile Security.	BTL-1	Remembering
2	What is meant by the mobile security landscape?	BTL-1	Remembering
3	State the importance of mobile security in the current digital era.	BTL-2	Understanding
4	List the major mobile operating systems used today.	BTL-1	Remembering
5	What is meant by a vulnerability in a mobile operating system?	BTL-1	Remembering
6	List any four common attack vectors on mobile devices.	BTL-1	Remembering
7	Differentiate between a threat and a vulnerability in mobile security.	BTL-2	Understanding
8	What is mobile malware?	BTL-1	Remembering
9	List the different types of mobile malware.	BTL-1	Remembering
10	What is meant by a Trojan in mobile devices?	BTL-1	Remembering
11	What is spyware in the context of mobile security?	BTL-1	Remembering
12	What are the legal considerations involved in mobile security?	BTL-2	Understanding
13	What are the ethical considerations in mobile security testing?	BTL-2	Understanding
14	Mention any four impacts of mobile exploits on personal security.	BTL-2	Understanding
15	List the consequences of mobile exploits in enterprise environments.	BTL-2	Understanding
16	Define mobile exploit.	BTL-1	Remembering
17	Why are smartphones considered attractive targets for cyber attackers?	BTL-2	Understanding
18	State the objectives of mobile security.	BTL-2	Understanding
19	List any four security challenges faced by mobile devices.	BTL-1	Remembering

20	Why is awareness of mobile security important for users and organizations?	BTL-2	Understanding
----	--	-------	---------------

PART - B

1	Explain the mobile security landscape and discuss the importance of mobile security in protecting personal and enterprise information.	BTL-3	Applying
2	Analyze the architecture of major mobile operating systems and discuss the common vulnerabilities associated with each.	BTL-4	Analyzing
3	Discuss the various attack vectors on mobile devices and explain how attackers exploit these vectors to compromise device security.	BTL-3	Applying
4	Examine the legal and ethical considerations involved in mobile security assessment and explain their significance in professional practice.	BTL-4	Analyzing
5	Evaluate the impact of mobile exploits on personal users and enterprise organizations with suitable examples.	BTL-5	Evaluating
6	Explain the different types of mobile malware and discuss their characteristics, propagation techniques, and impact on mobile devices.	BTL-3	Applying
7	Analyze the lifecycle of a mobile malware attack and propose suitable preventive measures to mitigate such attacks.	BTL-4	Analyzing
8	Discuss the major security threats affecting mobile devices and evaluate appropriate countermeasures for protecting mobile environments.	BTL-5	Evaluating
9	Explain the evolution of mobile security and discuss the emerging challenges in securing modern mobile computing environments.	BTL-3	Applying
10	Compare different categories of mobile threats and analyze their impact on the confidentiality, integrity, and availability of information.	BTL-4	Analyzing
11	Assess the role of mobile security in enterprise environments and recommend best practices for securing organizational mobile devices.	BTL-5	Evaluating
12	Explain the causes of vulnerabilities in mobile operating systems and discuss effective techniques for minimizing security risks.	BTL-3	Applying
13	Analyze the importance of legal compliance and ethical responsibility while performing mobile security testing and vulnerability assessment.	BTL-4	Analyzing
14	Evaluate various strategies for protecting mobile devices against malware attacks and unauthorized access.	BTL-5	Evaluating
15	Explain how mobile exploits affect individuals and organizations, and discuss suitable mitigation strategies to reduce security risks.	BTL-3	Applying
16	Analyze the relationship between mobile operating system vulnerabilities and mobile attack vectors with suitable illustrations.	BTL-4	Analyzing
17	Evaluate the importance of implementing a comprehensive mobile security framework for modern organizations and justify your recommendations.	BTL-5	Evaluating

UNIT II – MOBILE APPLICATION SECURITY

Fundamentals of secure mobile app development OWASP Mobile Top 10 vulnerabilities--Techniques for secure coding in mobile apps--Reverse engineering of mobile applications--Securing data storage mobile apps--Authentication and authorization mechanisms in mobile apps--Best practices for secure API usage in mobile apps.

PART – A

1	Define secure mobile application development.	BTL-1	Remembering
2	What is OWASP Mobile Top 10?	BTL-1	Remembering
3	State the purpose of the OWASP Mobile Top 10 vulnerabilities.	BTL-2	Understanding

4	List any four OWASP Mobile Top 10 vulnerabilities.	BTL-1	Remembering
5	What is secure coding in mobile applications?	BTL-1	Remembering
6	List any four secure coding practices for mobile applications.	BTL-1	Remembering
7	Define reverse engineering of mobile applications.	BTL-1	Remembering
8	Why is reverse engineering performed on mobile applications?	BTL-2	Understanding
9	What is secure data storage in mobile applications?	BTL-1	Remembering
10	List the methods used to secure data storage in mobile applications.	BTL-1	Remembering
11	Define authentication in mobile applications.	BTL-1	Remembering
12	Differentiate between authentication and authorization.	BTL-2	Understanding
13	What is authorization in mobile applications?	BTL-1	Remembering
14	What is meant by secure API usage in mobile applications?	BTL-2	Understanding
15	List any four best practices for secure API usage in mobile applications.	BTL-1	Remembering
16	Why is secure coding important in mobile application development?	BTL-2	Understanding
17	State the importance of securing sensitive data in mobile applications.	BTL-2	Understanding
18	Mention the risks associated with insecure APIs in mobile applications.	BTL-2	Understanding
19	What are the objectives of mobile application security?	BTL-2	Understanding
20	List the key components of secure mobile application development.	BTL-1	Remembering
PART – B			
1	Explain the fundamentals of secure mobile application development and discuss their significance in developing secure mobile applications.	BTL-3	Applying
2	Analyze the OWASP Mobile Top 10 vulnerabilities and explain how they affect the security of mobile applications.	BTL-4	Analyzing
3	Discuss various secure coding techniques used in mobile application development and explain how they prevent security vulnerabilities.	BTL-3	Applying
4	Analyze the process of reverse engineering mobile applications and discuss its security implications.	BTL-4	Analyzing
5	Evaluate different techniques used for securing data storage in mobile applications and recommend suitable approaches for protecting sensitive information.	BTL-5	Evaluating
6	Explain the authentication and authorization mechanisms used in mobile applications with suitable examples.	BTL-3	Applying
7	Analyze various authentication mechanisms for mobile applications and compare their effectiveness in enhancing application security.	BTL-4	Analyzing
8	Evaluate the best practices for secure API usage in mobile applications and justify their importance in preventing security breaches.	BTL-5	Evaluating
9	Explain the role of secure coding practices in mitigating security vulnerabilities in mobile applications.	BTL-3	Applying
10	Analyze the security risks associated with insecure data storage and propose suitable mitigation techniques for mobile applications.	BTL-4	Analyzing
11	Evaluate the impact of reverse engineering on mobile application security and recommend effective protection techniques.	BTL-5	Evaluating

12	Explain the importance of authentication and authorization in mobile application security and discuss their implementation challenges.	BTL-3	Applying
13	Analyze the security challenges associated with API integration in mobile applications and recommend best practices for secure API implementation.	BTL-4	Analyzing
14	Evaluate different secure coding standards and best practices adopted for developing robust mobile applications.	BTL-5	Evaluating
15	Explain how the OWASP Mobile Top 10 can be used as a guideline for designing secure mobile applications.	BTL-3	Applying
16	Analyze the relationship between secure coding, secure data storage, authentication, and API security in developing secure mobile applications.	BTL-4	Analyzing
17	Evaluate a comprehensive mobile application security strategy by incorporating secure development practices, data protection mechanisms, authentication techniques, and secure API usage.	BTL-5	Evaluating
UNIT III – ANDROID SECURITY			
Android security architecture overview -Android permissions model and best practices- Exploitation techniques targeting Android devices--Rooting Android devices: risks and implications--specific security vulnerabilities-- Android malwareanalysis and detection-- Securing Android devices in enterprise environments.			
PART - A			
1	Define Android security architecture.	BTL-1	Remembering
2	List the key components of Android security architecture.	BTL-1	Remembering
3	What is the Android permissions model?	BTL-1	Remembering
4	State the importance of the Android permissions model.	BTL-2	Understanding
5	List any four best practices for Android permissions management.	BTL-1	Remembering
6	Define Android exploitation.	BTL-1	Remembering
7	List the common exploitation techniques targeting Android devices.	BTL-1	Remembering
8	What is rooting in Android devices?	BTL-1	Remembering
9	Mention the risks associated with rooting Android devices.	BTL-2	Understanding
10	What are Android security vulnerabilities?	BTL-1	Remembering
11	List any four common Android security vulnerabilities.	BTL-1	Remembering
12	Define Android malware analysis.	BTL-1	Remembering
13	What is Android malware detection?	BTL-1	Remembering
14	State the objectives of Android malware analysis.	BTL-2	Understanding
15	What is meant by securing Android devices in enterprise environments?	BTL-2	Understanding
16	List the security measures used to protect Android devices in enterprises.	BTL-1	Remembering
17	Why is Android considered a major target for cyber attackers?	BTL-2	Understanding
18	Differentiate between rooting and exploitation in Android devices.	BTL-2	Understanding
19	State the importance of malware detection in Android devices.	BTL-2	Understanding
20	List the objectives of Android security.	BTL-2	Understanding

PART - B			
1	Explain the Android security architecture and discuss how its components contribute to securing Android devices.	BTL-3	Applying
2	Analyze the Android permissions model and explain the best practices for effective permission management in Android applications.	BTL-4	Analyzing
3	Explain the various exploitation techniques targeting Android devices and discuss suitable countermeasures to mitigate these attacks.	BTL-3	Applying
4	Analyze the security implications of rooting Android devices and discuss the associated risks and benefits.	BTL-4	Analyzing
5	Evaluate the impact of Android security vulnerabilities on users and organizations and recommend appropriate mitigation strategies.	BTL-5	Evaluating
6	Explain the process of Android malware analysis and discuss the techniques used for malware detection.	BTL-3	Applying
7	Analyze different Android malware detection techniques and compare their effectiveness in identifying malicious applications.	BTL-4	Analyzing
8	Evaluate the security risks associated with Android malware and recommend suitable defense mechanisms for securing Android devices.	BTL-5	Evaluating
9	Explain the best practices for securing Android devices in enterprise environments.	BTL-3	Applying
10	Analyze common Android security vulnerabilities and discuss how attackers exploit them to compromise device security.	BTL-4	Analyzing
11	Evaluate different approaches for protecting Android devices against exploitation, malware, and unauthorized access.	BTL-5	Evaluating
12	Explain the relationship between Android security architecture and the permissions model in ensuring application security.	BTL-3	Applying
13	Analyze the importance of malware analysis in identifying and mitigating Android security threats.	BTL-4	Analyzing
14	Evaluate enterprise security policies and best practices for managing and securing Android devices in organizational environments.	BTL-5	Evaluating
15	Explain the risks associated with Android rooting and discuss effective strategies to minimize security threats arising from rooted devices.	BTL-3	Applying
16	Analyze the relationship between Android vulnerabilities, exploitation techniques, and malware attacks with suitable examples.	BTL-4	Analyzing
17	Evaluate a comprehensive Android security framework by integrating security architecture, permissions management, malware detection, and enterprise security practices.	BTL-5	Evaluating
UNIT IV – IOS SECURITY			
iOS security architecture overview--iOS app sandboxing and code signing— Jailbreaking iOS devices: risks and security implications--Techniques for securing iOS applications-- iOS malware analysis and detection--iOS security updates and patch management-- Securing iOS devices in enterprise environments.			

PART – A			
1	Define iOS security architecture.	BTL-1	Remembering
2	List the key components of the iOS security architecture.	BTL-1	Remembering
3	What is app sandboxing in iOS?	BTL-1	Remembering
4	State the purpose of app sandboxing in iOS.	BTL-2	Understanding
5	What is code signing in iOS?	BTL-1	Remembering
6	Why is code signing important in iOS applications?	BTL-2	Understanding
7	Define jailbreaking in iOS devices.	BTL-1	Remembering
8	Mention the risks associated with jailbreaking iOS devices.	BTL-2	Understanding
9	List any four techniques for securing iOS applications.	BTL-1	Remembering
10	What is iOS malware analysis?	BTL-1	Remembering
11	Define iOS malware detection.	BTL-1	Remembering
12	State the objectives of iOS malware analysis.	BTL-2	Understanding
13	What are iOS security updates?	BTL-1	Remembering
14	Why is patch management important in iOS security?	BTL-2	Understanding
15	What is meant by securing iOS devices in enterprise environments?	BTL-2	Understanding
16	List the security measures adopted for iOS devices in enterprise environments.	BTL-1	Remembering
17	Differentiate between app sandboxing and code signing in iOS.	BTL-2	Understanding
18	State the importance of malware detection in iOS devices.	BTL-2	Understanding
19	What are the objectives of iOS security?	BTL-2	Understanding
20	Why are security updates essential for iOS devices?	BTL-2	Understanding
PART - B			
1	Explain the iOS security architecture and discuss how its components contribute to securing iOS devices.	BTL-3	Applying
2	Analyze the role of app sandboxing and code signing in enhancing the security of iOS applications.	BTL-4	Analyzing
3	Explain the process of jailbreaking iOS devices and discuss its risks and security implications.	BTL-3	Applying
4	Analyze the security challenges associated with jailbroken iOS devices and recommend suitable mitigation measures.	BTL-4	Analyzing
5	Evaluate various techniques for securing iOS applications and justify their effectiveness in protecting sensitive information.	BTL-5	Evaluating
6	Explain the process of iOS malware analysis and discuss the techniques used for malware detection.	BTL-3	Applying
7	Analyze different malware detection techniques for iOS devices and compare their effectiveness in identifying malicious applications.	BTL-4	Analyzing

8	Evaluate the security risks posed by iOS malware and recommend appropriate defense mechanisms to mitigate these threats.	BTL-5	Evaluating
9	Explain the importance of security updates and patch management in maintaining the security of iOS devices.	BTL-3	Applying
10	Analyze the role of security updates in preventing vulnerabilities and protecting iOS devices from emerging threats.	BTL-4	Analyzing
11	Evaluate enterprise security practices for securing iOS devices and recommend suitable strategies for organizational deployment.	BTL-5	Evaluating
12	Explain the relationship between iOS security architecture, app sandboxing, and code signing in ensuring application security.	BTL-3	Applying
13	Analyze the impact of jailbreaking on iOS device security and discuss appropriate preventive measures.	BTL-4	Analyzing
14	Evaluate different approaches for securing iOS applications against malware, unauthorized access, and data leakage.	BTL-5	Evaluating
15	Explain the techniques used to secure iOS applications and discuss their significance in mobile application security.	BTL-3	Applying
16	Analyze the relationship between malware analysis, security updates, and patch management in strengthening iOS security.	BTL-4	Analyzing
17	Evaluate a comprehensive iOS security strategy by integrating security architecture, application security, malware protection, patch management, and enterprise security practices.	BTL-5	Evaluating

UNIT V – ADVANCED TOPICS IN MOBILE EXPLOITATION

Mobile device management (MDM) and its role in security--BYOD (Bring Your Own Device) policies and security considerations--Securing mobile payment systems and digital wallets--IoT (Internet of Things) devices and mobile security.

PART – A

1	Define Mobile Device Management (MDM).	BTL-1	Remembering
2	State the purpose of Mobile Device Management (MDM).	BTL-2	Understanding
3	List the key features of Mobile Device Management (MDM).	BTL-1	Remembering
4	What is meant by Bring Your Own Device (BYOD)?	BTL-1	Remembering
5	State the objectives of a BYOD policy.	BTL-2	Understanding
6	List any four security considerations in BYOD environments.	BTL-1	Remembering
7	What is a mobile payment system?	BTL-1	Remembering
8	Define a digital wallet.	BTL-1	Remembering
9	State the importance of securing mobile payment systems.	BTL-2	Understanding
10	List the security features of digital wallets.	BTL-1	Remembering
11	What is the Internet of Things (IoT)?	BTL-1	Remembering
12	Define IoT devices in the context of mobile security.	BTL-1	Remembering
13	State the security challenges associated with IoT devices.	BTL-2	Understanding
14	Why is IoT security important in mobile environments?	BTL-2	Understanding
15	Mention the benefits of implementing Mobile Device Management in enterprises.	BTL-2	Understanding

16	List the common threats to mobile payment systems.	BTL-1	Remembering
17	Differentiate between Mobile Device Management (MDM) and BYOD.	BTL-2	Understanding
18	State the importance of security policies in BYOD environments.	BTL-2	Understanding
19	List the best practices for securing IoT devices connected to mobile networks.	BTL-1	Remembering
20	Why is mobile exploitation prevention important in modern organizations?	BTL-2	Understanding
PART - B			
1	Explain the concept of Mobile Device Management (MDM) and discuss its role in enhancing mobile device security within enterprise environments.	BTL-3	Applying
2	Analyze the architecture, components, and security features of Mobile Device Management (MDM) solutions.	BTL-4	Analyzing
3	Explain the concept of Bring Your Own Device (BYOD) and discuss the security considerations involved in implementing BYOD policies in organizations.	BTL-3	Applying
4	Analyze the security risks associated with BYOD environments and recommend suitable security policies to mitigate these risks.	BTL-4	Analyzing
5	Evaluate the effectiveness of Mobile Device Management (MDM) in addressing security challenges arising from BYOD implementations.	BTL-5	Evaluating
6	Explain the architecture of mobile payment systems and discuss the security mechanisms used to protect financial transactions.	BTL-3	Applying
7	Analyze the security threats affecting mobile payment systems and digital wallets, and discuss suitable mitigation strategies.	BTL-4	Analyzing
8	Evaluate various security mechanisms employed in digital wallets and justify their effectiveness in protecting users' financial information.	BTL-5	Evaluating
9	Explain the role of IoT devices in mobile ecosystems and discuss the associated mobile security challenges.	BTL-3	Applying
10	Analyze the security vulnerabilities of IoT devices connected to mobile networks and recommend appropriate countermeasures.	BTL-4	Analyzing
11	Evaluate different approaches for securing IoT devices in enterprise and consumer environments.	BTL-5	Evaluating
12	Explain the significance of security policies in Mobile Device Management and BYOD environments with suitable examples.	BTL-3	Applying
13	Analyze the relationship between MDM, BYOD, and organizational mobile security, highlighting their benefits and challenges.	BTL-4	Analyzing
14	Evaluate best practices for securing mobile payment systems and digital wallets against emerging cyber threats.	BTL-5	Evaluating
15	Explain the security considerations involved in integrating IoT devices with mobile platforms and discuss suitable protection mechanisms.	BTL-3	Applying
16	Analyze the role of Mobile Device Management, BYOD policies, mobile payment security, and IoT security in building a secure mobile ecosystem.	BTL-4	Analyzing

17	Evaluate a comprehensive enterprise mobile security framework by integrating Mobile Device Management, BYOD policies, secure mobile payment systems, digital wallets, and IoT security practices.	BTL-5	Evaluating
----	---	-------	------------