COURSE TITLE	**MOBILE APPLICATION & SECURITY**
COURSE CODE	**01CC0709**
COURSE CREDITS	**3**

Objective:

1 The objective of this course is to help students understand the security architecture of mobile platforms like Android and iOS, and to apply secure design principles in mobile applications. It focuses on identifying common vulnerabilities, performing security testing using various techniques, and understanding mobile device security features, management strategies, and emerging threats.

Course Outcomes: After completion of this course, student will be able to:

1 Explain mobile platforms, security models, and the mobile threat landscape, including OWASP Mobile Top 10 vulnerabilities

2 Apply secure design and development practices for mobile applications, including secure storage, communication, and authentication mechanisms.

3 Analyze mobile application vulnerabilities and exploitation techniques based on OWASP Mobile Top 10.

4 Analyze mobile applications using security testing methodologies such as static and dynamic analysis and reverse engineering techniques.

5 Evaluate mobile device security mechanisms, management frameworks, and emerging threats to recommend secure practices and compliance standards.

Pre-requisite of course: Proficiency in at least one object-oriented programming language (e.g., Java, Kotlin, Swift, or a strong ability to learn one). Basic understanding of operating system concepts. Familiarity with networking fundamentals (e.g., HTTP/S). Prior experience with mobile application development is beneficial but not strictly required if students are prepared for a fast-paced introduction.

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
2	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Introduction to Mobile Platforms and Security Models** Introduction to Mobile Computing and Applications, Overview of Major Mobile Operating Systems (Android and iOS architecture and ecosystem), Mobile Security Models (sandboxing, permissions, code signing, inter-component communication security), The Mobile Threat Landscape (unique threats to mobile devices and applications (malware, phishing, data leakage)), OWASP Mobile Security Top 10 vulnerabilities, Security Development Lifecycle (SDL) for Mobile Applications	6

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
2	**Secure Mobile Application Design and Development** Threat Modeling for Mobile Applications (identifying potential threats and vulnerabilities early in the design phase), Secure Data Storage (protecting sensitive data at rest (on the device file system, databases, keychains/keystores)), Secure Communication (implementing secure network communication (SSL/TLS best practices, certificate pinning), handling untrusted inputs), Secure Authentication and Authorization in Mobile Apps (implementing secure login, session management, and access control), Input Validation and Output Encoding (preventing injection attacks (SQL injection, XSS in WebViews))	8
3	**Mobile Application Vulnerabilities and Exploitation** Deep Dive into OWASP Mobile Top 10 (detailed understanding of each vulnerability category with real-world examples), Insecure Data Storage (exploiting vulnerabilities in databases, shared preferences, and external storage), Insecure Communication (intercepting and manipulating network traffic, bypassing SSL pinning), Insecure Authentication and Authorization (exploiting weak authentication mechanisms and authorization bypasses), Client Code Quality Issues (understanding vulnerabilities arising from poor coding practices (e.g., insecure randomization, hardcoded secrets)),Client Code Quality Issues (understanding vulnerabilities arising from poor coding practices (e.g., insecure randomization, hardcoded secrets)),, Code Tampering and Reverse Engineering (understanding how attackers can modify or decompile mobile applications)	6
4	**Mobile Application Security Testing** Mobile Application Security Testing Methodologies (static analysis (SAST), dynamic analysis (DAST), penetration testing),, Setting up a Mobile Security Testing Environment (emulators, rooted/jailbroken devices, proxy tools (Burp Suite, OWASP ZAP)),, Static Analysis of Mobile Applications (analyzing source code and decompiled binaries (APKs, IPAs) for vulnerabilities), Dynamic Analysis of Mobile Applications (observing app behavior at runtime, intercepting traffic, runtime manipulation tools (Frida, Objection)),, Reverse Engineering Mobile Applications (tools and techniques for analyzing obfuscated code and understanding application logic), Using Automated Mobile Security Scanners	7

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
5	**Mobile Device Security and Emerging Topics** Mobile Device Security Features (full disk encryption, secure boot, remote wipe), Mobile Device Management (MDM) and Mobile Application Management (MAM) (concepts and security implications), Rooting and Jailbreaking (understanding the security risks associated with compromised devices), Emerging Mobile Security Threats and Trends (mobile-specific malware analysis, supply chain attacks on mobile apps, privacy concerns), Security Considerations for Cross-Platform Development Frameworks (React Native, Flutter), Mobile Application Security Standards and Compliance (e.g., OWASP MASVS)	5
Total Hours		**32**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Setting up a Mobile Application Development and Security Testing Environment: Installing Android Studio/Xcode, emulators/simulators, and a mobile security testing proxy tool.	2
2	**Practical 2** Developing a Simple Vulnerable Mobile Application: Creating a basic mobile app with intentional vulnerabilities (e.g., insecure data storage, weak input validation) for testing purposes.	2
3	**Practical 3** Analyzing Mobile Application Permissions and Manifest Files: Examining the permissions requested by an Android APK or iOS IPA and understanding their security implications.	2
4	**Practical 4** Performing Static Analysis on a Mobile Application: Using tools like MobSF or online scanners to analyze the source code or binary of a mobile app for common vulnerabilities.	2
5	**Practical 5** Intercepting and Analyzing Mobile Application Network Traffic: Configuring a proxy tool to intercept HTTP/S traffic from a mobile app and analyze the data exchanged.	2
6	**Practical 6** Exploiting Insecure Data Storage: Accessing and retrieving sensitive data stored insecurely by a vulnerable mobile application on an emulator or rooted device.	2
7	**Practical 7** Implementing Secure Data Storage: Modifying the vulnerable application to store data securely using platform-provided mechanisms (e.g., Android Keystore, iOS Keychain).	2

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
8	**Practical 8** Performing Dynamic Analysis and Runtime Manipulation: Using tools like Frida or Objection to hook into a running mobile application and observe or modify its behavior.	2
9	**Practical 9** Analyzing a (Benign) Mobile Malware Sample: Using static analysis tools to examine the characteristics and potential behavior of a safe mobile malware sample (in an isolated environment).	2
10	**Practical 10** Implementing Certificate Pinning: Modifying a mobile application to implement certificate pinning to prevent Man-in-the-Middle attacks.	2
Total Hours		**20**

Textbook :

1 Mobile Application Security, Himanshu Dwivedi, Chris Clark & David Thiel, McGraw-Hill, 2010

References:

1 Android Security Internals: An In-Depth Guide to Android's Security Architecture, Android Security Internals: An In-Depth Guide to Android's Security Architecture, Nikolay Elenkov, No Starch Press, 2015

2 iOS Application Security: The Definitive Guide for Hackers and Developers, iOS Application Security: The Definitive Guide for Hackers and Developers, David Thiel, No Starch Press, 2016

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
0.00	5.00	10.00	40.00	35.00	10.00

Instructional Method:

1 The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

2 The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Instructional Method:

3 Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.

4 Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.

Supplementary Resources:

1 “Mobile Application Security and Pen Testing” – Coursera (IBM Skills Network) - https://www.coursera.org/learn/mobile-app-security

2 OWASP Mobile Security Lab (MobSF Live Demo & CTF) - https://mobsf.live/