Faculty of Computer Studies (FoCS)

Course Name: Mobile Applications Penetration Testing

(UG/PG): PG

Number of Credits: 2

Level: 3

Learning Objective(s):

The course aims in providing hands on approach to understand the concepts of Mobile Applications Penetration Testing. The Course is designed for covering various aspects of mobile platform and testing the security for different mobile application. It helps in studying the need for mobile penetration testing and testing with some hands on tools. To understand the mobile issues and development strategies. To understand the WAP and mobile security issues To understand the Bluetooth security issues.

Pedagogy:

- Lectures
- Class discussion followed by practical
- Hands-on Lab sessions

Course Outline

Sr. No.	Topic	Hours
1	Introduction to Mobile Security, Mobile Devices Issues Facing, Secure Data Storage, Strong Authentication with Poor Keyboards , Multiple-User Support with Security, Safe Browsing Environment , Cross-Site Request Forgery (CSRF), Location Privacy/Security, Insecure Device Drivers, Multifactor Authentication, Secure Mobile Application Development .	5
2	WAP and Mobile HTML Security :WAP and Mobile HTML Basics , Authentication on WAP/Mobile HTML Sites , Encryption , Application Attacks on Mobile HTML Sites, HTTP Redirects , Phishing , Session Fixation , Non-SSL Login , Mobile Browser Weaknesses, Handling Browser Cache , Wifi (802.11) Security.	5
3	Bluetooth Security: History and Standards , Bluetooth Versions Prior to v1.2, Bluetooth Versions Prior to v2.1., Common Uses , Alternatives , Future , Bluetooth Technical Architecture , Radio Operation and Frequency, Bluetooth Network Topology , Device Identification , Threats to Bluetooth Devices and Networks, Bluetooth Vulnerabilities ,	5
4	SMS Security: Overview of Short Message Service, Overview of Multimedia Messaging Service, Abusing Legitimate Functionality, Attacking Protocol Implementations	5

5	Enterprise Security on the Mobile OS: Device Security Options , PIN , Remote , 346 Secure Local Storage , Security Policy Enforcement ,Encryption ,Full Disk Encryption ,E-mail Encryption , File Encryption , Application Sandboxing, Signing, and Permissions , Application Sandboxing , Application Signing , Permissions , Buffer Overflow Protection ,	5
6	Case study on Mobile Application Security with respect to different Mobile platform	5
	Total	30

Taxonomy of Security Threats
Debugging
LogCat
DDMS
Memory Analysis
IPC Mechanisms and App Components
Manually Decrypt Applications Binaries
Traffic Sniffing

Books Recommended

1. Wei-Meng Lee, Beginning AndroidTM 4 Application Development, 2012 by John Wiley & Sons
2. "Mobile Application Security", Himanshu Dwivedi, Chris Clark, David Thiel, TATA McGRAWHill.
3. "Mobile and Wireless Network Security and Privacy", Kami S. Makki, et al, Springer.

Suggested Evaluation Methods:

- Lab based Evaluations
- Assignments
- Presentation

Parallel/Similar courses the existing curriculum:

S.No.	Name of the course	Institute where it was offered
	Mobile Application Development	College of Computer and Information Science Northeastern University

Name of Member	Prof. Harshad Gune	Dr. Tejaswini Apte			
Designation	Dy.Director	Domain Head			
Org. / Inst.	SICSR	SICSR			
Signature					

Name of the Expert:
Signature:
Date: