**Course Sr. No. 16**

|  |  |  |
| --- | --- | --- |
| A. | **Name of the Institute** | Centre for Development of Advanced Computing, Mohali |
| B. | **Name/title of the Course** | **Specialized Training programme in Mobile Device Security** |
| C. | **Proposed Dates and Duration of the Course in weeks/ months** | Duration: **Eight weeks**  From: **21st Oct. 2019 to 13th Dec.2019** |
| D. | **Eligibility Criteria for Participants** | |
| 1. Educational Qualification | Technical Graduate (Computer Science/ Electronics/Telecommunications/ or equivalent) with working knowledge of computers. |
| 1. Work Experience | As per MEA guidelines |
| 1. Age Limit | As per MEA guidelines |
| 1. Target group (Level of participants and target ministry/department etc. may be identified) | Working Professional with knowledge of computers and mobile devices with some programming language exposure. |
| E. | Aims & Objectives of the Course | To develop in-depth knowledge and understanding of the mobile device security domain. Provides an introduction to mobile device architecture, malicious applications & it’s analysis, threats to mobile devices and security measures. |
| F. | Details / Content of the Course ***(please attach detailed Course Profile****)* | As per sheet attached |
| G. | Mode of Evaluation of Performance of the ITEC Participant | Theory, viva voce & Practical |

**Course Content:**

1. **Introduction to Mobile Operating System**

* Android Operating System: Framework, Architecture, Application design
* Android Virtual Machine-Dalvik Executable (DEX), Optimized DEX (ODEX)
* Android Security Model - UID Separation, Sandboxing
* iOS Operating System: Architecture, Security framework, device Jailbreaking, iOS privileges

1. **Understanding Executable Files and Vulnerabilities**

* Introduction to APK Structure - APK Contents, AndroidManifest.xml, Other Files
* Reversing APKs: Tools - Dex2Jar, Obfuscation;
* Application Structure- Java, AndroidManifest.xml, Deep Links- AIDL, Bound Services, onBind, Messenger, Binder
* Components- Activities, Services, Broadcast Receivers, Permission Models
* WebViews - JavaScript, JavaScript Bridge, Content Provider Access
* Brief Introduction of Android Malwares till date, Logging based Vulnerabilities, Bypassing SSL pinning, Exploiting weaknesses in mobile apps
* Introduction to Mobile Sensors

1. **Device and Data Security**

* Data Storage -Internal Storage, External Storage, Local Databases-Sqlite3
* Device Administration API- MDM Solutions, Root Detection
* Third-Party Code- SDK, Libraries
* Device Tracking

1. **Mobile Device Malware Threats**
   * Trends and popularity of mobile device malware
   * Mobile malware command and control architecture
   * Efficiency of Android ransomware malware threats
   * Hands-on analysis of Android malware

* Mobile malware defenses: what works, and what doesn't

1. **Static Code Analysis**

* Vulnerability Exploitation, Retrieving Android apps for reverse engineering analysis
* SQL Injection
* Vulnerable Activities, Vulnerable Receivers, Vulnerable Services
* Android application interaction and Intent manipulation with tools

1. **Dynamic Code Analysis**

* Debugging: debug gable, breakpoints
* Android Debug Bridge- ADB Commands, Activity Manager
* Additional Tools -Interacting with Databases, Android Device Monitor