ISSW 2013
APRIL 19-21
AUSTIN, TEXAS

ADVANCED MOBILE HACKING
(Android and iOS)
HANDS-ON Training

By **XY|SEC**

Trainers

Aditya Gupta and **Subho Halder**

Prerequisite

The participants are expected to have a basic knowledge of Mobile Operating Systems. Knowledge of programming languages (**Java and C, and Python for scripting**) will be an added advantage to grasp things quickly.

Hardware Requirements

Minimum **2GB RAM** and **20 GB free Hard Disk space**
Android (preferably Rooted) >= 2.3
iPhone/iPad (optional)

Software Requirements

Windows XP SP2/3 or Windows 7 or Linux 2.4/2.6
Mac OSX 10.5/10.6
Administrative privileges on your laptop
Virtualization Software
Proper labs will be provided for exploitation
SSH Client

COURSE STRUCTURE

Day I (Android Exploitation):

Module 1:

Android Basics

- Introduction to Android
- Android Architecture
- Digging into Android kernel

Android Security Model

- Android Security Architecture
- Android Permission model
- Application Sandboxing
- Bypassing Android Permissions

HelloWorld : Android

- Android Application Components
- Android Debug Bridge
- Creating a Simple Android Application

Introduction to ARM

- Introduction to ARM
- Instruction set and Registers

- Debugging with GDB
- Stack Overflows on ARM
- Shellcoding on ARM
- Android root exploits

Module 2:

Setting up the Environment

- Setting up Android Emulator
- Setting up a Mobile Pentest Environment

App Kung-fu

- Application Analysis
- Reverse Engineering
- Traffic Interception of Android Applications
- OWASP Top 10 for Android
- Sniffing Application and phone's data
- Unsecure file storage
- Having fun with databases

Exploiting Logic and Code flaws in applications

- Exploiting Content Providers
- SQL Injection in Android Application
- Local File Inclusion/Directory Traversal
- Drive by Exploitation
- Tapjacking
- HTML 5 Attacks
- Phishing Attacks on Android

Module 3:

Exploitation with AFE

- Introduction to Android Framework for Exploitation
- Finding application vulnerabilities using the framework

- Creating a malware/botnet for analysis
- Crypt an existing malware/botnet to bypass Android Anti-malwares
- Extending the framework with custom plugins

Module 4:

Android Forensics

- Extracting text messages, voice mails, call logs, contacts and messages
- Recovering information stored in SD Card

Further Exploitation:

- Android Malwares and Botnets
- Cracking Android Applications
- Vulnerable Social Networking Application (xyShare)
- Creating and Exploiting custom ROMs
- Exploiting USB connections with Android

Being secure

- Android in the Enterprise
- Writing Secure Code
- Pentest before you publish
- Automated Pentesting environment

Day II (iOS Exploitation):

Module 1:

iOS Background

- Understanding iOS Architecture
- iOS Security Features
- iOS Application Overview

iOS Security Model

- Code Signing
- Sandboxing
- Exploit Mitigation
- Encryption

Setting up the Environment

- Setting up XCode
- Setting up iPhone/Simulator

Module 2:

iOS Hello-World

- iOS Application components
- Introduction to Objective C
- Writing a simple Hello World application in your own iDevice/Simulator

iOS App Analysis

- Reverse Engineering iOS Apps
- Decrypting Appstore Binaries
- Locating PIE (Position Independent Executable)
- Inspecting Binary
- Manipulating Runtime

Module 3:

Auditing Insecure API

- Evaluating the Transport Security
- Abusing Protocol Handlers
- Insecure Data Storage
- Attacking iOS keychain

App Assessments

- Setting up pentesting environment for assessment
- Passive app assessment
- Active app assessment
- Application analysis

App Kungfu

- Exploiting XSS in Apps (UIWebViews)
- Attacking XML processor
- SQL Injection
- Filesystem Interaction
- Geolocation
- Logging
- Background-ing

Memory Corruption Issues:

- Format strings
- Object use-after free

Module 4:

iOS Forensics

- Analysis of Backed up data in iTunes
- Extracting SMS, Call Logs, etc., from an iOS backup
- Imaging the whole device

Being Secure

- iOS App compliance checklist
- Writing Secure Codes
- Pentest your App before you publish