Engineering Staff College of India

Autonomous Organ of The Institution of Engineers (India)

Old Bombay Road, Gachi Bowli, Hyderabad – 500 032. TS, India

INFORMATION TECHNOLOGY DIVISION

Continuing Professional Development Programme

Wireless & Mobile Security

12 – 14 Feb, 2018

(An ISO 9001:2008 Certified, AICTE & CEA Recognized Institution)

Centre for Promotion of Professional Excellence

Introduction

Wireless & Mobile security is nothing but protecting computers, smartphones, tablets, laptops and other portable devices along with the networks they are connected to, from threats and vulnerabilities associated with wireless computing.

Mobile security has become increasingly important in Mobile Computing, because personal and business information now stored on Smartphones. More and more users and businesses use smartphones not only to communicate, but also to plan and organize their users' work and also private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

Objectives

- To develop skills in the area of Wireless & Mobile security.
- To learn Mobile Security best practices.

Course Coverage

- **Wireless Security Basics**
  - Wireless Security - Concepts
  - Wireless Security - Access Point
  - Wireless Security - Network
  - Wireless Security - Standards
  - Wi-Fi Authentication Modes
  - Wireless Security - Encryption
  - Wireless Security Break an Encryption
- **Wireless Threats**
  - Wireless - Access Control Attacks
  - Wireless Security - Integrity Attacks
  - Wireless - Confidentiality Attacks
  - Wireless Security - DoS Attack
  - Authentication Attacks
  - Rogue Access Point Attacks
  - Client Misassociation
  - Misconfigured Access Point Attack
  - Ad-Hoc Connection Attack
  - Wireless Hacking Methodology
  - Wireless Traffic Analysis(Sniffing)
  - Launch Wireless Attacks
  - Crack Wireless Attacks
- **Wireless Security Tools**
- **Wireless Security Pen Testing**
- **Wireless Security Useful Resources**
- **Introduction to Mobile Security**
  - Identifying components of a mobile Operating System
  - Recognizing application security challenges
  - Exposing the threats faced by mobile devices
  - Discovering mobile hacking tools
- **Developing a Mobile Security Strategy**
- **Defining the mobile threat model**
- **Creating a practical security policy**
- **Protecting Mobile Devices**
- **Securing the mobile endpoint**
- **Maintaining data confidentiality and integrity**
  - Applying whole disk and file encryption
  - hardware encryption techniques
- **Establishing secure communication**
- **Applying secure development guidelines**
- **Implementing mobile application security**
  - Protecting user interface data
  - Storing data in the Android and iOS Keychain
  - Enforcing user authentication
  - Defining trust boundaries
- **Standardizing permissions**
- **Promoting a Secure Environment**

Target Participants prerequisites:

- Participants should have basic **Computer Networking Skills**.

Methodology

Methodology of the programme includes class room sessions with hands-on practical, Lecture / Discussion with audio visual aid, bench marked video shows, Chalk & Talk sessions, group discussions, case studies, debates, sharing of experiences etc. All the sessions will be interactive demanding active participation from all the members.

Target Participants

- System Engineers, Network Engineers, System Administrators, Network Administrator, IT Managers,
- Scientists, IT Specialists, Communications engineers and System Managers working in the industry,
- Police Offices (ASP, DSP, ASP, SP or Above Rank Officers) / Defence Scientists
- Executives of Telecom, Government, Private and Public sector organizations.
- Faculty members and Technical staff of Engineering Colleges or MCA Colleges who would like to gain expertise in wireless technology and its security aspects.

Programme Venue, Dates & Timings

Venue: Engineering Staff College of India (ESCI) Campus, Old Bombay Road, Gachi Bowli, Hyderabad. 500032. TS, India.

Dates: 12 – 14 Feb, 2018

Timings: On the first day Registration will commence at 09:00 hrs. On all other days the programme timings will be from 09:45 – 17:15 hrs with breaks in between for tea and lunch.

Course Director

Mr. Syed Azgar , MBA(IT), RHCE, MCSA
Faculty & Manager-IT,
Information Technology Division,
Engineering Staff College of India, Hyderabad.

Course Fee

₹ **15,000/- (Residential Fee)** per participant. Fee includes course material, course kit, twin-sharing /single AC accommodation as per availability, Breakfast, Lunch, Dinner, Tea / Coffee and Snacks during the actual days of training programme.

Discounts

- **Non – Residential Fee** - 10% discount on course fee is allowed for non- residential participants
- **Group Discount** - Additional 10% discount for three or more participants if sponsored by the same organization

(All discounts are applicable only if fee is received at ESCI before commencement of the programme)

GST @18% is to be paid extra and above the training fee as training is also brought under the purview of Service Tax in Finance Bill 2010. **PAN Card No.** AAATT3439Q. **GST No: 36AAATT3439Q1ZV, HS No.: 999293** (under commercial training or coaching services – clause 65(105) (ZZC) of Finance act – 1994)

Programme fee is to be paid in in favour of **"THE INSTITUTION OF ENGINEERS (INDIA) – ENGINEERING STAFF COLLEGE OF INDIA"** in the form of demand draft payable at Hyderabad. Alternatively the payment may be made by **Electronic Fund Transfer (EFT)** to ESCI – **Axis Bank** A/c No. **912010049234564** with The Axis Bank Ltd, Old Mumbai Hwy, Cyberhills Colony, P Janardhan Reddy Nagar, GachiBowli Hyderabad-500032 by NEFT/ RTGS/ IFSC Code No. UTIB 0000733 – MICR No.500211020. **While using EFT method of payment, please ensure to communicate us your company name, our invoice reference and programme title.**

Register Online: http://www.escihyd.org/index.php/it-upcoming-trainings

To register manually please send your nominations giving details of name, designation, contact address, email address, mobile no, telephone and fax number of the participant along with the details of mode of payment of fee, addressed to :

Head
Information Technology Division
Engineering Staff College of India
Gachi Bowli, Hyderabad – 500 032
Phone: 66304100 (EPABX) / 040 – 66304123/24/25 (Direct), Fax: 040 - 23000336
Email: it@escihyd.org, Portal: www: escihyd.org

A Certificate of participation will be awarded to each participant on conclusion of the programme.

- ESCI encourages participants to present case studies from their respective organizations.
- For the convenience of outstation participants, ESCI will facilitate pick-up and drop from Airport / Railway Stations / Bus Stations, if travel plans are received at least 3 days in advance along with mobile number by fax or email. The charges shall be paid by the participant directly to the Cab.
- ESCI provides complimentary accommodation and boarding to the participants one day before commencement (Check-in 1200 h) and one day after conclusion (Check-out 1200 h) of the programme duration. Overstay charges will be applicable as per ESCI rules (subject to availability of accommodation)
- Well developed Information Centre and Internet facilities are available to the participants.