Ducara Info Solutions (P) Ltd.

C|MASX

Certified Mobile Application Security Expert

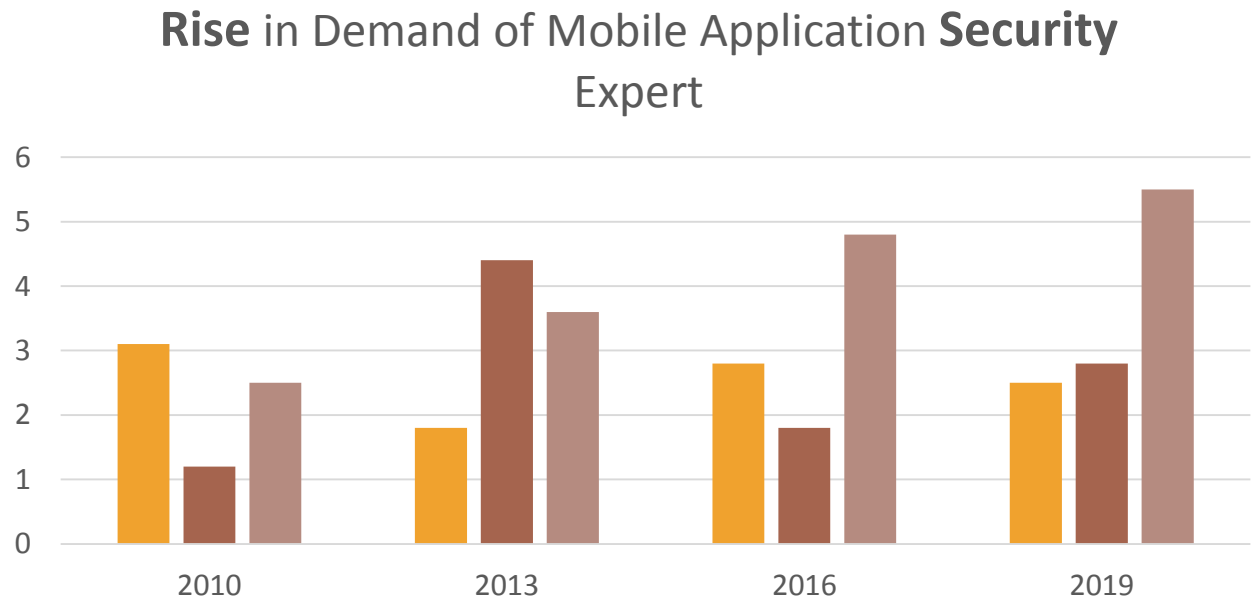
WHY C|MASX?

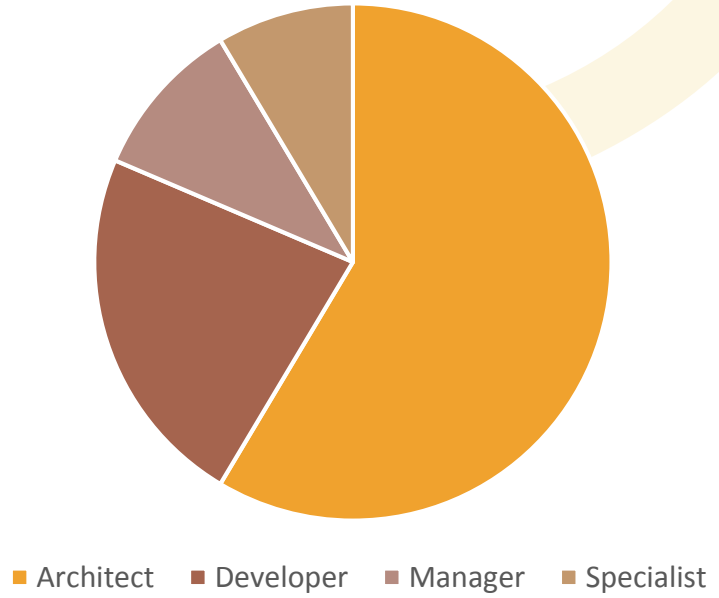
Mobile Application Security is about **Mobile Applications and Device Security** and it provides complete and current coverage of Mobile Application and Mobile Platform Security. The certification provides a solid foundation in basic Mobile Application Security terminology and concepts, extended and built upon throughout the engagement. Delegates will examine various recognized attacks against Mobile Applications.

WHAT TREND SAYS?

According to the first-quarter **2018 Nielsen Total Audience Report**, the average consumer spends an average of three hours and 48 minutes a day on digital media, and consumers spend **62%** of that time on apps and web usage via smartphones.

Unsecured productivity apps deployed by an organization pose as significant a threat to the business, similar to any customer facing app running in the wild. This threat creates a number of IT management issues in trying to find effective ways to deploy these apps to maximize adoption and maintain security and governance.





TARGET AUDIENCE

DURATION: 40HRS

SOFTWARE DEVELOPERS

APPLICATION ARCHITECTS

SECURITY ANALYSTS

SYSTEM ARCHITECTS

The certification provides security activity **Guidance**, **Checklists** and question lists for **Application Architects** and software developers who want to improve the security of the **Windows Applications** that they develop. **Software Developers** are the primary audience, but the **Security Engineering** activities summaries are designed to be used by team members from many different disciplines, including **Business Analysts**, **Architects**, **Developers**, **Testers**, **Security Analysts** and **Administrators**. It is centered on key security activities that you should perform at the various stages of the application lifecycle.

WHAT IS THE OBJECTIVE?

• Imagine an attack surface that is spread across your organization and in the hands of every user. It moves from place to place regularly, stores highly sensitive and critical data, and sports numerous different wireless technologies all ripe for attack. Such a surface already exists today: **mobile devices**.

• These devices are the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

• This course is designed to give you the skills you need to understand the security strengths and weaknesses in **Apple iOS** and **Android** devices.

• You'll leverage **automated and manual mobile application analysis tools** to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels.

• You'll safely work with mobile malware samples to understand the data exposure and access threats affecting **Android** and **iOS**, and you'll bypass lock screen to exploit lost or stolen devices.

• Understanding and identifying **vulnerabilities** and threats to mobile devices is a valuable skill.

• Learn how to conduct a mobile device penetration test.

TOPICS TO BE COVERED..

MOBILE APP PENETRATION TESTING AND ETHICAL HACKING	MOBILE THREATS, ATTACKS, VULNERABILITIES, AND COUNTERMEASURES	KEY SECURITY REQUIREMENTS IN THE MOBILE ENVIRONMENT	MOBILE APPLICATION SECURITY, PENETRATION, AND SECURE CODING
MOBILE APP SECURITY CONCEPTS	SECURING MOBILE APPLICATIONS	METHODS TO DECOMPILE CLIENT-SIDE CODE	VARIOUS VULNERABILITIES IN MOBILE ENVIRONMENTS
ADVANCED MOBILE APP SECURITY	MOBILE PAYMENTS, SMS, BLUETOOTH AND GEOLOCATION SECURITY	ENTERPRISE SECURITY ON THE MOBILE OS	MOBILE SECURITY PENETRATION TESTING TOOLS

WHAT YOU'LL LEARN

Mobile App Penetration Testing and Ethical Hacking

- The Attacker's View of the Mobile
- Overview of the Mobile Applications from a penetration tester's perspective
- Overview of the various mobile platform architectures
- Overview of different types of vulnerabilities
- How to define a mobile application test scope and process
- Types of mobile penetration testing
- Methodology to Improve mobile application security
- Knowing your threats
- Securing the network, host and application
- Incorporating security into your software development process
- Mobile Application Security Policy

Mobile Threats, Attacks, Vulnerabilities, and Countermeasures

- Asset
- Threat
- Vulnerability
- Attack (or Exploit)
- Countermeasure
- Application Threats / Attacks

Key Security Requirements in the Mobile Environment

- Certificate Storage/Management
- Storage/Management
- Digital Signature
- PIN/password protection
- Remote applet management
- Content storage/encryption
- Identity management
- Secure data exchange
- Authentication and Integrity management

Mobile Application Security, Penetration, and Secure Coding

- Mobile Applications Security Testing
- Application Penetration Testing & Ethical Hacking
- Language Specific Secure Software Development: Objective C, C/C++, Java/JEE, HTML5, ActionScript, Ruby, and CSS
- Digital Certificates, Digital Signatures, Keys, Trust Services, PKI, Keychain, Remote Transport Security, SSL And TLS
- Sensitive Data Unprotected At Rest
- Buffer Overflows And Other C Programming Issues
- Secure Communications To Servers.
- Patching Your Application

Key Security Requirements in the Mobile Environment

- Certificate Storage/Management
- Storage/Management
- Digital Signature
- PIN/password protection
- Remote applet management
- Content storage/encryption
- Identity management
- Secure data exchange
- Authentication and Integrity management

Mobile App Security Concepts

- Security in Mobile App Development Platforms
- Overview of iOS Security Architecture
- Overview of Android Security Architecture
- Overview of Windows Phone 7 Security Architecture
- Security features of iOS and Android
- Keychain Services
- Security APIs in iOS and Android
- Assets, Threats, and Attacks
- Security Technical
- Security Testing

Methods to Decompile Client-side Code

- Objective C
- C/C++
- Java
- HTML5
- ActionScript
- Ruby
- CSS

Securing Mobile Applications

- Access Applications
- VPN and Secure Storage of Data
- Protection of Downloaded and Broadcasted Content
- Mobile DRM
- Service and Content Protection for Mobile Broadcast Services
- Security Requirements
- Authentication Applications
- Extensible Authentication Protocol (EAP)
- Generic Bootstrapping Architecture (GBA)
- Public Key Infrastructure (PKI) and Certificate-based Authentication
- Identity Selection Applications
- Security and Trust Model of Identity Selector
- Mobile Applications Security Feature Requirement Matrix Overview of the infrastructure within the Mobile Application
- Overview of Wireless Networks: Access and Core
- Overview of Mobile Development Platforms
- Mobile Platforms Security Architecture
- SSL/TLS/DTLS Configurations and Weaknesses
- Google and Facebook Hacking
- Hacking to Social Networks

Various Vulnerabilities in Mobile Environments

- Information Leakage
- Username Harvesting
- Command Injection
- SQL Injection
- Blind SQL Injection
- Session Issues
- Hacking the Keys
- Fuzzing
- Attacking Web Services
- Malicious Applets And Objects
- Vulnerabilities In Mobile Application Through Discover Of The Client Components
- Methods For Attacking Mobile Services
- Methods To Zombify Browsers
- Using Zombies To Port Scan Or Attack Internal Networks
- Explore Attack Frameworks
- Walk Through An Entire Mobile Attack Scenario
- Exploit The Various Mobile App Vulnerabilities

Advanced Mobile App Security

- Application Threats / Attacks
- Input Validation
- Authentication
- Authorization
- Configuration Management
- Sensitive Information
- Session Management
- Cryptography
- Parameter Manipulation
- Exception Management
- Auditing And Logging
- Impact On Security On Performance
- Attack Types and Methods to Prevent

Mobile Payments, SMS, Bluetooth and Geolocation security

- Contactless Smartcard Payments
- Secure Element
- Secure Element API
- Google Wallet
- Apple Pay and Other Payment Methods
- Block Chain Security
- Overview of Short Message Service
- Overview of Multimedia Messaging Service
- Protocol Attacks
- Application Attacks
- Walkthroughs

- Overview of the Bluetooth Technology
- Bluetooth Technical Architecture
- Bluetooth Security Features
- Threats to Bluetooth Devices and Networks
- Bluetooth Vulnerabilities
- Geolocation Methods
- Geolocation Implementation
- Risks of Geolocation Services
- Geolocation Best Practices

Enterprise Security on the Mobile OS

- Device Security Options
- Secure Local Storage
- Security Policy Enforcement
- Encryption
- Application Sandboxing, Signing, and Permissions
- Buffer Overflow Protection

Mobile Security Penetration Testing Tools

- Mobile Platform Attack Tools and Utilities
- Browser Extensions
- Networking Tools
- Web Application Tools

THE TECHNOLOGY IS CHANGING EVERY DAY AND WE AT DUCARA ARE COMMITTED TO DEMONSTRATING VALUES. EMBRACING A DIGITAL TRANSFORMATION STRATEGY WHICH DRIVE RETURNS ON IT SECURITY INVESTMENT.

CONNECT US!

INFO@DUCARAINFO.COM

WWW.DUCARAINFO.COM