TRIGENT

How Secure is Your Mobile App?

Vijendra Kumar H.
Practice Head - Mobility

Trigent ■ 2 Willow Street, Suite 201, Southborough, MA 01745 ■ 1-877-387-4436 ■ www.trigent.com

Many companies are outsourcing their mobile application development for various reasons – cost reduction, skill unavailability, schedule constraints, etc. Consider a mid-sized company that wanted to monetize a great, unique idea by building a mobile app. This company did not have the necessary resources with appropriate skills to build this mobile application. They decided to outsource the development and evaluated multiple vendors. The company choose the one they thought fit their needs – primarily based on cost. The chosen vendor worked with the company to build the app and delivered it along with the server side components that integrated to the company's backend systems. The application worked as expected with pleasing user interface and the company successfully launched the Android app in the Google Play store.

Unfortunately, within a short period, many similar apps were launched in the Google Play store. Most provided same, if not better, features than the company's application, and with slightly modified user interface. In about a month, the company's server was attacked by hackers and crashed with the database wipe out.

This is an example how things can go wrong if proper considerations for application and data security were not made while building mobile applications. In this instance, the app development vendor had not taken care of even the simplest form of vulnerabilities like SQL injection, Input validation attack, etc., – to protect their backend systems.

The competitors had reverse engineered the android app, understood the business logic contained in the app, and rapidly built similar, competing apps with minimal effort.

While developing mobile applications, developers and architects with limited experience and engineering discipline may ignore many important aspects of security. Security is critical both on client and server side. Proper security measures must be built to protect the users' personal data, the company's intellectual property and hitherto sheltered backend systems. Failing to protect against potential security problems will erode into customer confidence in the company and will negatively affect revenue plans.

We present below some of the security issues that should be taken care while developing mobile applications.

Security On the client/App side

- ❑ Securing app's business logic: This should prevent users from reverse engineering the mobile application. It should not be limited to just using obfuscation tools. Many developers/architects assume that applying obfuscation alone will prevent reverse engineering. In reality, it only makes it marginally harder for the hackers.

❑ Securing data stored on client side i.e. on mobile devices
❑ Securing the communication channel used to interact with server
❑ Securing the data to be transmitted to the server

Security on the Server Side

❑ Securing server data
❑ Securing physical servers/cloud servers using additional hardware and/or software
❑ Securing servers from general attacks. Preventing unauthorized access to servers by identifying requests from hackers and blocking such requests
❑ Securing sessions and requests from clients
❑ Securing server from viruses, worms etc.
❑ Taking care of vulnerabilities in the code like SQL Injection/Query Poisoning, Input validation attack, Impersonation attack, Session Hijacking attack, Source code disclosure, Buffer overflows etc.

Security levels needed differs by application type, its specific functionality and the nature of the company's business. If the app handles financial transactions, higher levels of security measures should be implemented. Likewise, if the app is handling credit cards, more stringent set of measures should be followed.

Just using digital certificate for all communication with the server or using two factor authentication mechanism for authenticating the users is not enough for securing the mobile applications.

When you develop a mobile app, make sure the vendor has a team of experts who take care of security for all the mobile applications delivered from the company. They should analyze your environment, functionality of the mobile application to be built and recommend solutions while analyzing vulnerabilities that must be taken care under various circumstances and user scenarios. The vendor should not only deliver mobile applications in time but also fortify customers' business logic and intellectual property involved in such applications.

About Trigent Software Inc.

Trigent is a privately held, professional IT services company and a Microsoft Gold Partner with its U.S. headquarters in the greater Boston area and its Indian headquarters in Bangalore. We provide consulting services in various technologies including Microsoft Solutions. Our operating model is to conduct sales, customer relationships and front-end consulting (e.g., business case, requirements, architecture) onsite with our clients and perform the detail design, development, integration, testing and quality assurance offshore at our world class development and support center in Bangalore. We are a SEI CMM Level 4 company and is ISO 9001:2000 TickIT certified organization.

For sales contact sales@trigent.com or call 508-490-6000.

CERTIFIED ISO 9001:2008 COMPANY

SOFTWARE 500

Microsoft Partner
Gold Application Development
Gold Collaboration and Content