

Mobile Application Security Assessment

Mobile Banking Made Safe

Overview

Our client wanted to roll out mobile banking applications and automate some of its banking processes. They engaged Aujas to ensure these products were rolled out in a secure manner.

Aujas Solution

- ✓ **Secure data while in transit and at rest on devices or servers.**
- ✓ **Protect application code assets.**
- ✓ **Develop security measures so that bank was not relying on user's device for inbuilt security.**

Introduction

Our client is a large private bank with a revenue of \$6.5 billion last year. This bank had a national presence and a customer base of over 28 million. Our client wanted to make banking and other related services available to customer more easily and so has widely adopted mobile banking.

Our client has many of its products and services available on mobile and other similar devices. These include net-banking, micro-ATM services, value-added services for credit card holders, plus lead management and loan collection.

The Business Need

To compete more effectively in the marketplace, our client wanted to provide world-class and convenient banking services for its customers. It chose to make almost all of its banking services available on mobile devices so that customers could bank where and when they wanted to and not worry about opening hours or bank holidays.

With mobile banking comes threats to data and customers' money, so it was important that our client's mobile applications were tested for security loopholes. Our client also needed to follow the industry's RBI mandate for safe and secure services.

1. **Reach out to stakeholders** – It was important to involve all key stakeholders in the area of mobile banking or other services. The project objectives also needed to be communicated to developers and any third party vendors.
2. **Make security a top priority** – Most of the developers understood loopholes in web applications and were well versed in web security. Mobile applications and their eco-systems, however, are different and have their own security shortcomings.
3. **Develop security processes** – The bank's developers initially did not have a secure application development process specifically designed for mobile applications.
4. **Focus on mobile security** – Some security issues that were observed had not been explored during mobile application development. When we observed these issues, we worked with developers to resolve them.

About Aujas


 An IDG Ventures Company
 \$ 3 Billion Group
 Largest IT Media Company



- Offices in USA, India and UAE
- More than 300 clients and 500 projects across 23 countries
- Over 170 professionals



- Information Risk Advisory
- Security Intelligence
- Identity and Access Management
- Application Security
- Data Protection

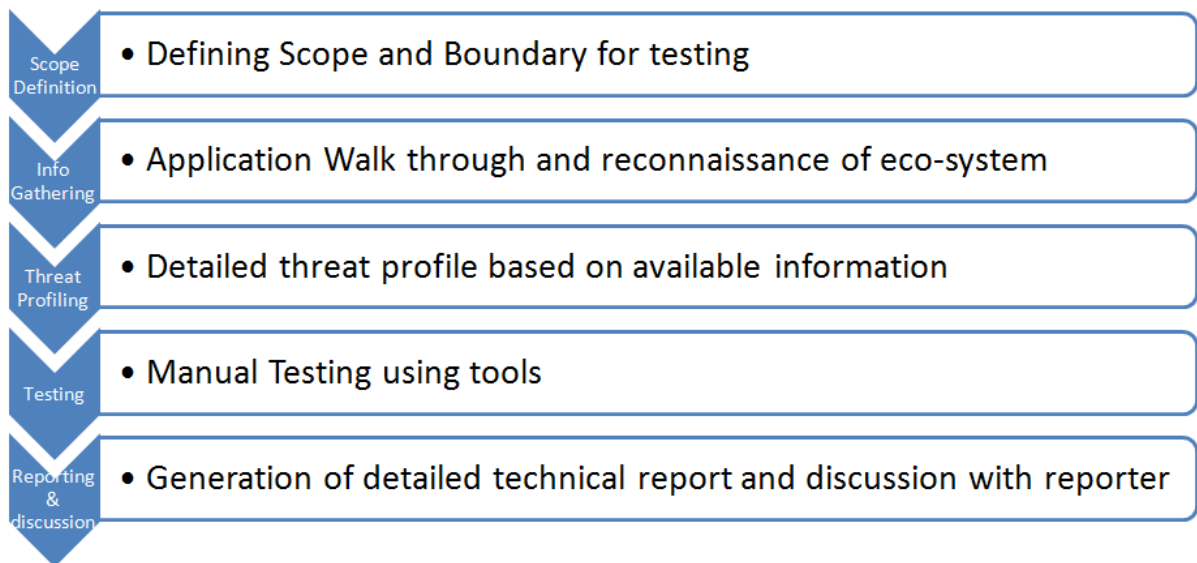
Aujas Solution

Our solution integrated all aspects of mobile application security:

1. **User** – He/she is the most important and yet the weakest link in mobile application security. Our aim was to make each mobile application secure in such a way that there would be little burden on user for security.
2. **Data** – Information needs to be protected when in transit and also when at rest. Mobile devices allow user to connect via WiFi hotspots. If hotspots are not safe, the user’s data may not be secure. So it was important to secure critical data when WiFi was in use. Also, the data at rest needed to be protected.
3. **Technology** – When a new operating system version is released, it typically offers more options to users – but can also provide a better attack surface to attackers.

Each application was tested based on the following methodology:

1. **Defining the Scope** – We defined the scope and boundaries for testing.
2. **Gathering Information** – We gathering working knowledge of mobile applications and devices, particularly Point of Sale (POS) devices.
3. **Profiling Threats** – Based on knowledge acquired in step two, we developed a detailed threat profile for every application.
4. **Testing** – Testing was conducted with reference to the detailed threat profiles.
5. **Reporting & Discussion** – we created a detailed technical report and communicated it to the developers.



Benefits and Learning

The Aujas team used its experience and expertise to understand and fulfill the bank’s requirements. In doing so, we

- Developed a process for more secure mobile applications and knowledge handover.
- Set up guidelines for secure development of mobile applications.
- Established an application security practice that is not dependent on the security features of any one device.

About Aujas



- An IDG Ventures Company
- \$ 3 Billion Group
- Largest IT Media Company



- Offices in USA, India and UAE
- More than 300 clients and 500 projects across 23 countries
- Over 170 professionals



- Information Risk Advisory
- Security Intelligence
- Identity and Access Management
- Application Security
- Data Protection