Mobile Application Security
Helping Organizations Develop a Secure and Effective Mobile Application Security Program

by
James Fox
fox_james@bah.com
Shahzad Zafar
zafar_shahzad@bah.com

Booz | Allen | Hamilton
delivering results that endure
Mobile applications are software applications designed to run primarily on smartphones, tablets, and pocket PCs. They are distributed by application market places and are specific to the Operating System (OS) of the mobile devices. The four most popular mobile application distribution market places are (1) Apple App Store, (2) Google Play, (3) BlackBerry App World, and (4) Windows Phone Store. The Apple App Store provides applications for Apple’s iOS-based iPhones and iPads, the Google Play for Android-based OS mobile devices, the BlackBerry App World for the Research In Motion’s BlackBerry mobile devices and Windows Phone store for Microsoft’s Mobile Phones, tablets, and pocket PCs. Since 2009, thousands of applications that can be installed and used on mobile devices have flooded these application market places. These mobile applications have evolved from their initial use as productivity, entertainment, and utility applications. Now users, customers, and employees are conducting their day-to-day business transactions on mobile devices. Businesses need to develop and provide mobile applications to their employees and customers to keep pace with the changing business and consumer landscape. However, these mobile applications have also introduced major security concerns for businesses and enterprises as hackers and bad actors can exploit them to steal and harm customers and businesses.

Mobile application security protects an organization from potential threats, leveraging the customer-facing mobile applications an organization develops as attack vectors. Mobile application security covers mobile applications, communication between mobile applications and backend infrastructure, backend infrastructure, and the associated activities, processes, and work streams used to design, test, develop, deploy, operate, and maintain these technologies.

Understanding the Evolving Threat Landscape of Mobile Security Worldwide

In the Middle East and North Africa (MENA) region and around the world, an increasing number of businesses, consumers, and employees are using mobile applications to conduct daily business transactions using mobile devices due to availability, ease, and accessibility of mobile ecosystems. A recent survey conducted by Booz Allen Hamilton of consumers in the Kingdom of Saudi Arabia indicates that 83 percent of the population uses smartphones to conduct business or enterprise transactions. In addition, 64 percent of those surveyed use mobile devices to conduct banking. However, the survey also revealed that one in three people have experienced cybercrime in the past 12 months and close to 50 percent of the people surveyed lack a basic understanding of mobile security and proper cyber hygiene. This survey data indicates that the stakes are high when it comes to mobile security and risk levels are only going to elevate as more and more businesses enable mobile application-based transactions to attract a new generation of consumers.

While consumer confidence and awareness is a key driver for addressing mobile security, the stakes are even higher for businesses and enterprises. They are the ultimate victims of cybercrime that could occur from breach in mobile application security. This threat is especially high for financial institutions. Regulators and banks are starting to address this quickly evolving threat landscape facing mobile applications.

The Open Web Application Security Project (OWASP) is an organization that has focused on improving the security of software in general and recently emphasizing mobile application security. As illustrated in Exhibit 1, OWASP has released the top 10 mobile application vulnerabilities that organizations must address when it comes to providing security for mobile applications. Any one of these vulnerabilities can cause serious damage to a financial institution via loss of data, reputation, and consumer confidence—all of which lead directly and indirectly to financial losses.
Identifying Vulnerabilities and Malicious Mobile Exploits

Booz Allen Hamilton, a leading strategy and technology consulting firm, focuses on defining the vulnerabilities further and identifying the potential mobile security exploits that could harm or damage a business. Several potential exploits are illustrated in Exhibit 2. Our mobile security experts understand the implications these exploits can have on business and consumer confidence and how organizations can best protect themselves against them.

Any one of these exploits can lead to loss of private data; loss of usernames, passwords, and personal identification numbers (PIN); unauthorized access to private, business, and financial data; and theft and fraud. For example, a stolen device that may have unencrypted data stored on the device could easily give a bad actor access to a person’s private data. A malware on a mobile device could easily forward username and passwords of a banking mobile application to hackers that could result in loss of financial data. Man-in-the-middle attacks were a major threat to web-based and online transactions, but now, they are increasingly more common on mobile devices. Controls such as two factor authentication across same communication channels are helpless against a stolen device or a device with malicious malware. These sophisticated attacks to mobile applications are well orchestrated and must be defended against through a pragmatic and holistic approach to mobile application security.

Exhibit 1 | Top 10 Mobile Application Vulnerabilities

Exhibit 2 | Successful Exploits

Source: OWASP.org

Source: Booz Allen Hamilton
Applying a Pragmatic and Holistic Approach to Mobile Security

No single product, process, policy, or quick fix exists that organizations can buy or develop to address mobile application security. Booz Allen Hamilton utilizes a holistic risk-based approach that identifies the risks, threats, and vulnerabilities and their impact on the business. Once initial risk identification is conducted, organizations can then start to address the problem in a pragmatic fashion and focus the efforts and budget on the most important assets based on risk and impact profile.

Booz Allen Hamilton’s approach to an effective mobile application security program starts with addressing three primary pillars of mobile application security: (1) secure mobile applications, (2) secure mobile data transmission, and (3) secure mobile backend infrastructure (see Exhibit 3). All three must be assessed and addressed across all aspects of people, processes, and technology dimensions. Our mobile application security professionals help organizations—

- Develop an understanding of holistic solution and approaches to providing mobile application security
- Utilize the same basic principles that apply to web and online security to mobile application security

Our approach to assess and develop solutions for organizations across mobile applications, mobile data transmission, and mobile backend infrastructure addresses the following categories across People Process and Technology (PP&T) dimensions:

- **Vulnerabilities.** Identify vulnerabilities based on risk profiles across PP&T
- **Relevant Security Controls.** Identify and implement security controls across PP&T
- **Best Security Practices.** Identify relevant security best practices and institutionalize them
- **Useful Frameworks and Standards.** Identify and adapt where relevant the various articles, tools, frameworks, and international standards across PP&T

When addressing mobile application security, organizations should take into account the following key points:

1. There is no one quick and simple solution to mobile application security; address it in a pragmatic and holistic fashion
2. Use defense in depth with information security controls for each component
3. Follow a stringent systems development life cycle (SDLC) focused on developing secure applications and continually review new development environments (integrated development environment [IDE] and software development kit [SDK]) for easier security
4. Do not directly integrate mobile applications into the enterprise
5. Always conduct third-party code reviews and penetration testing and conduct annual third-party assessments

Exhibit 3 | Secure Mobile Applications

[Image of Exhibit 3: Secure Mobile Applications]

Source: Booz Allen Hamilton
About Booz Allen Hamilton

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for nearly a century. Today, the firm provides services primarily to US and international governments in defense, security, and civil markets, and to major corporations, institutions, and not-for-profit organizations. Booz Allen Hamilton offers clients deep functional knowledge spanning consulting, mission operations, technology, and engineering—which it combines with specialized expertise in clients’ mission and domain areas to help solve their toughest problems.

Booz Allen Hamilton is headquartered in McLean, Virginia, employs more than 23,000 people, and had revenue of $5.76 billion for the 12 months ended March 31, 2013. To learn more, visit www.boozallen.com. (NYSE: BAH)

For more information contact

James Fox  Shahzad Zafar
Senior Associate  Senior Associate
fox_james@bah.com  zafar_shahzad@bah.com
+971-56-688-6043  +971-56-688-3014

To learn more about the firm and to download digital versions of this article and other Booz Allen Hamilton publications, visit www.boozallen.com.