Mobile App Security Audit Framework

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

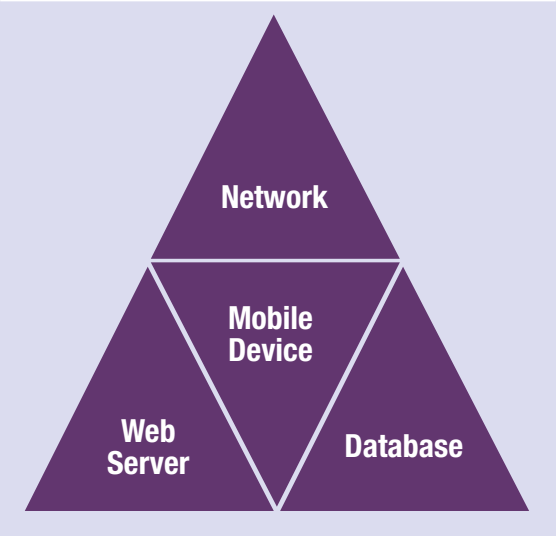
On 3 April 1973, Martin Cooper, a Motorola researcher and executive, made the first mobile call from a phone weighing a little over 1kg. Fast-forward to 2016. The average mobile phone is much lighter and faster than the 1973 version, it offers more functionality and it contains more computing power than the earliest personal computers. It seems clear that mobile technology is here to stay, as increasing numbers of consumers and enterprises alike adopt its convenience, speed and benefits. "As the number of people who own and use cell phones continues to grow, so does the use of smartphones. 91% of the US adult population currently owns a cell phone and of that 91%, 61% are smartphones."[1] With such technological change, especially at the enterprise level, IT audit and security professionals must adapt to the changing threat landscape created by mobile applications (apps) by getting ahead of the risk by putting proper controls in place and testing mobile apps from conception to release.

In order for the proper controls for mobile apps to be developed and tested, one must first dissect the layers of risk. As illustrated in **figure 1**, there can be multitudes of layers, but the basic risk segments can be divided into four main mobile app security categories:

- Mobile devices
- Mobile networks
- Mobile app web servers
- Mobile app databases

Mohammed J. Khan, CISA, CRISC, CIPM
Is a global audit manager at Baxter, a global medical device company. He works with the chief audit executive, chief information security officer and chief privacy officers. He has spearheaded multinational global audits in several areas, including enterprise resource planning systems, global data centers, third-party reviews, process reengineering and improvement, global privacy assessments (European Union and the United States), and cybersecurity initiatives in several markets over the past five years. Most recently, he has taken on further expertise in the area of medical device cybersecurity. Khan has previously worked as a senior assurance and advisory consultant for Ernst & Young and as a business systems analyst for Motorola.

Figure 1—Four Segments of Mobile Apps Security Risk



Source: Mohammed Khan. Reprinted with permission.

Building a Framework at the Consumer and Enterprise Levels

Enterprise or consumer-only apps share the same types of risk and threats. However, some enterprise risk factors are unique in their own ways and, to address this risk, one has to assess the business value proposition for creating enterprise apps. According to one article, "Mobile devices dominate consumer use to the point that enterprises are seeing the value of integrating them into the workplace as well."[2] There are three desired benefits:

- **Efficiency**—The ability of the workforce to perform tasks typically performed on a client-server platform should be replicated to be performed the same way on a mobile app to achieve maximum mobility and benefit from the growing Internet of Things (IoT) capabilities.
- **Services**—Employees must be able to maximize the service they provide customers by being empowered to conduct enterprise-level activities in the same way they are accustomed to working with desktop applications. The app must provide the same type of support and data availability as is expected from the non-app enterprise-level services.

- **Customer satisfaction**—It is critical to provide customers the same enterprise-level satisfaction and meet the key performance indicators (KPIs) that formed part of the reason the customer signed up for the enterprise solution in the first place.

One of the challenges facing auditors is specifically assessing how to go about tackling risk factors in mobile apps. The layers illustrated in **figure 1** help the auditor dissect the threat areas. Also, there must be some basic controls in place for more complex controls to be addressed and implemented. Although the testing framework proposed in **figure 2** does not encapsulate all complementary controls, it focuses on the key controls required to have a basic maturity level around strengthening mobile apps security.

Figure 2—Mobile Apps Audit Testing Framework

Threat Area	Control Topic	Control Test (Verify the Following)	Control Test	Risk Mitigated
Mobile device	Data storage	Data are stored securely to prevent malicious extraction from the app when data are at rest.	Encryption of the data at rest in the mobile device (app) is set to Advanced Encryption Standard (AES) 128, 192 or 256.	Data loss and disclosure
Mobile device	Data transmission	Mobile app data transmission is encrypted when data are not at rest (transferred).	Encryption of data is enforced for data in transit using Secure Sockets Layer (SSL) and strong security protocols such as: • Web access—HTTPS vs. HTTP • File transfer—FTPS, SFTP, SCP, WebDAV over HTTPS vs. FTP, RCP • Security protocols—Transport Layer Security (TLS).	Data loss and disclosure
Mobile device	Reverse engineering of app code	App code is protected from modification from unauthorized intruders through use of binary protections.	Binary protections are standard protocol for app development life cycle and enforced by the development team at time of app coding and maintenance.	User experience compromise, unauthorized access, data loss
Mobile device	App access management and security	App is configured to limit access and configured appropriately for limited authorized use.	Mobile application management (MAM) is utilized to manage access and deployment of the app. Additionally, proper whitelists (approved) and blacklists (noncompliant) are maintained. Examples of MAM services include MobileIron, Airwatch and Apperian, providing a central online location for distribution and tracking purpose.	Unauthorized access and fraud
Network	Wireless connectivity	Encryption is enforced when Wi-Fi connection is activated.	Transmission of data utilizes, at a minimum, SSL or TLS—both cryptographic protocols for secure transmission of data.	Data loss and disclosure
Network	Session hijacking	Prevent hijacking of a session due to insecure connection protocol.	Connection protocols for the uniform resource locator (URL) via TLS are through HTTPS rather than HTTP to securely connect to a URL.	Data loss and disclosure, unauthorized access

Figure 2—Mobile Apps Audit Testing Framework *(cont.)*

Threat Area	Control Topic	Control Test (Verify the Following)	Control Test	Risk Mitigated
Network	Domain Name System (DNS) spoofing	DNS is secured to avoid rerouting of data to another Internet Protocol (IP) address.	Proper packet filtering setup is built in to verify source address and blocking packets with conflicting source address. Utilization of TLS, Secure Shell (SSH) and HTTPS is enabled for secure communication protocol.	Data loss and disclosure, unauthorized access
Web server	Operations patch management	A process is in place to identify and apply critical system security patches and updates.	Processes exist for the deployment of system patches for all applicable systems. Processes exist for identifying new patches or for notification of new patches from vendors. The system is current with the latest patches prescribed from central IT. If any vulnerability scans have been performed, patches have been applied to address any identified issues. Missing patches are identified and compared against documented formal exceptions from security team.	Data loss and disclosure, unauthorized access
Web server	Access management	Roles and responsibilities for ownership have been established, documented and communicated.	All applicable web servers have been assigned both technical and business system owners, as required. The defined roles and responsibilities are adequate, especially for internal and third-party personnel.	Data loss and disclosure, unauthorized access
Web server	Brute-force attack	Management of denial-of-service (DoS) strategy encompasses proper programs to lock out unauthorized protocols.	Lock-out protocols are enabled for accounts with multiple incorrect password attempts. Utilization of CAPTCHA (program that distinguishes between humans and computers) is recommended to avoid DoS.	Unauthorized access and fraud, availability of app
Database	Privileged access	Elevated access to databases are properly secured utilizing best practices.	Access to database is limited to appropriate individuals, and proper access reviews and documented system accounts are kept on file. All default accounts and passwords are disabled by enforcing strict password controls.	Unauthorized access and fraud
Database	Structured Query Language (SQL) injection	Back-end database access is properly secured from vulnerabilities utilizing proper input validation techniques.	Input validation technique is in place; specifically defined rules for type and syntax against key business rules exist.	Unauthorized access and fraud

Figure 2—Mobile Apps Audit Testing Framework *(cont.)*

Threat Area	Control Topic	Control Test (Verify the Following)	Control Test	Risk Mitigated
Database	Validation of app (client) input	Data coming from mobile apps have to be vetted prior to trusting it to pull or push data to the database layer.	Sanitization of app user data coming from the mobile app is properly protected through embedded logic checks within the application. Proper implementation of logic checks is enabled at the server side.	Unauthorized access and fraud
Database	App database services	Database server software is updated to current secure versions.	The database server is properly tested and hardened against malicious attack. Login forms have HTTPS required. SSL connections are mandatory.	Unauthorized access and fraud
App management	App deployment administration	App store updates are properly governed utilizing a life cycle management methodology.	A governance structure is in place for mobile app life cycle management, specifically, the release of mobile apps to the app store and modification of future releases.	Unauthorized access and fraud
App management	App deployment source code management	Source code management is properly assigned prior to release.	The app is signed using the enterprise account of the company's enterprise account certificate.	Unauthorized access and fraud
App management	Remote wiping of data	Ability for remote wipe of the device/app data exists to mitigate risk of lost or compromised devices.	Enterprise apps that are released to company employees or contractors using company-owned devices utilize a remote mobile management software, such as MobileIron, to facilitate remote wiping.	Data loss and disclosure, unauthorized access

Source: Mohammed Khan. Reprinted with permission.

Conclusion

It is imperative that IT auditors work with all teams within the organization responsible for the development of mobile apps—business, IT development, IT security, legal and compliance. Auditors must facilitate the process of policing the efforts of mobile app development and implementing a basic robust framework that determines a minimum amount of security controls that allow mobile apps to withstand the risk of operating in a vulnerable mobile environment. In addition to the basic auditing framework laid out in this article, it is recommended to use a penetration testing framework that applies to all mobile apps prior to their release. In addition, penetration testing must be performed as the mobile app is updated and newer technology is put in place to support the app. This reduces the risk of external and internal vulnerabilities that can result in the compromise of data.

Endnotes

1 Collat School of Business, "The Future of Mobile Application," infographic, University of Alabama, Birmingham, USA, *http://businessdegrees.uab.edu/resources/infographics/the-future-of-mobile-application/*

2 Poole College of Management Enterprise Risk Management Initiative, "Managing Risks of the Mobile Enterprise," North Carolina State University, USA, 1 October 2012, *https://erm.ncsu.edu/library/article/manage-risks-mobile-enterprise*