Publishing Enterprise Mobile Application Process

[1]Adel A. Marghalani, [2]Hafed A. Alghamdi, [3]Marwan A. Dulaijan, [4]Meshal K. Thuaini

[1,2,3,4]Information Technology, Saudi Aramco

***Abstract*: The recent exponential adoption of modern mobile device and application access management solutions brought a set of misperceptions, between information technology analysts and information security experts, regarding publishing IT services on mobile devices. Many large enterprises and organizations utilize more than one solution to meet business demands and increase employees' productivity. Deciding on which technology a mobile application should be published is still ambiguous. Therefore, this paper articulates the importance of having a standard process to be adopted by the enterprise, to streamline the process of publishing mobile applications on mobile devices. Enforcing this process will standardize the development of mobile applications within the enterprise, and ensure these applications are published on the most suitable and cost-effective mobile management platform. Only Android and iOS/iPad devices will be considered in the paper as Windows device management will be covered in another paper.**

***Keywords:* Mobile Device Management, Enterprise Mobility Management, MDM, MAG, EMM, MAM, BYOD, Public Stores.**

I. INTRODUCTION

A standardized process for publishing mobile applications is necessary for enterprises and organizations to roll out mobile applications on a suitable, reliable, and cost-effective platform. Without having a standard process, a mobile application can be hosted on an expensive platform such as Enterprise Mobility Management (EMM), or an unsecured platform, such as public stores based on the application's developer preference. For example, a mobile application that does not access sensitive information nor requires an access to enterprise resources can be hosted on a costly platform. An application that accesses an enterprise sensitive data and resources can be hosted on public app stores, exposing the enterprise data to potential security risks, or might violate the country's cybersecurity regulations. Many available management solutions such as public app stores, Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Access or API Gateway (MAG), and Enterprise Mobility Management (EMM) are available for hosting mobile applications, and its APIs where each of these solutions provides different levels of security controls. Some of these solutions offer security controls for the mobile applications' access and devices operating system to ensure having extra protection and control over enterprise data stored on these devices, such as adding device-level passcode or applying data leakage prevention (DLP) controls. In general, there are six popular methods for publishing enterprises' mobile apps will be presented in the next section. The primary purpose of this paper is highlighting the urgent demand for having a standard process that ensures each mobile application is analyzed promptly during the planning phase, in coordination with developers, security experts, and infrastructure analysts, to determine the best method for publishing the mobile application. Following this process should assist in having most enterprise mobile applications published in the most efficient solution with the minimum required security controls.

II. ENTERPRISE MOBILE DEVICE AND APPLICATION MANAGEMENT SOLUTIONS

Before diving into the development of the publishing mobile applications process, it is vital to have an overview of the most popular mobile application publishing solutions. There are six enterprise solutions most organizations consider for publishing mobile applications. The criticality of a mobile application, publishing costs, and the sensitivity of data it is accessing should determine the solution for publishing the mobile application. Some mobile applications can be published using more than one solution in sporadic cases, but in general, there should be one method to be used for publishing any mobile application. This section provides the advantages and disadvantages of publishing mobile applications on these solutions.

- ***Mobile Device Management (MDM)***

Mobile Device Management (MDM) solutions are mainly used to manage mobile devices running different Operating Systems such as Android, iOS, and Windows. Most MDM solutions share similar security controls. MDM solutions rely entirely on an agent installed on mobile devices to ensure corporate mobile profiles, policies, security controls, device restrictions, malware detection, monitoring, and tracking of these devices are applied. Although these solutions safeguard mobile devices by enforcing device-level encryption and access control to specific trusted networks to mitigate potential risks of data leakage, they do not provide management at the application level. Thus, publishing mobile enterprise applications on general stores becomes a requirement, and downloading them will be based on users' preferences. Although MDM solutions provide various controls over some native applications on devices, such as browser apps and email clients, they do not provide control over locally developed enterprise applications. It introduces security risks as these applications are hosted on public app stores. Such solutions can be deployed at a reasonable cost.

- ***Mobile Application Management (MAM)***

The Mobile Application Management (MAM) solution is similar to MDM; instead, it is only applied to a specific mobile application (Tse et al., 2016). The MAM solution handles application distribution through publishing apps on an enterprise private app store/catalog and avails the apps to registered users. Moreover, it can blacklist applications, whitelist applications, and generate application usage reports. In such solutions, the application access control and data security are achieved; however, it does not provide any controls over the device, leading to security concerns. For example, an inability to detect jailbroken devices as it requires MDM solution. It is a great solution when implementing the Bring Your Own Device (BYOD) concept. Moreover, MAM requires the Android Package Kit (APK) and iOS Application Archive (IPA) files; or at least having the application published on Public Google/Apple Stores to be availed on the MAM infrastructure. There might be some cases to have the application published on public stores and availing it in the enterprise private store, but this will defeat the main purpose of having a private enterprise mobile application store.

- ***Mobile Access Gateway (MAG)***

Mobile Access or API Gateway (MAG) is a middleware technology safely exposes an enterprise data as APIs to developers and mobile applications published on public or private app stores (Unified, 2020). Most of these solutions use a development tool called Software Development Kit (SDK) for the mobile application development process. The solutions introduce a secure access channel through published APIs to be used by users through a particular application using modern authentication techniques such as OAuth, SOAP and others. This will ensure that mobile application backends are accessed securely, but this solution does not provide any control over a mobile device’s operating system, nor provides an enterprise App Catalog for distributing mobile applications. Such solutions are costly and vary from one product to another, depending on the number of users or the number of transactions per application.

- ***Legacy Enterprise VPN Mobile Client***

The VPN client is a legacy technology and proved its capability over time in providing secure access to enterprises or organizations' sensitive data. Most VPN solutions enforce all mobile device communications to go through a secure channel. It brought drawbacks to usability aspects especially when BYOD concept is implemented. If a user is having personal applications installed and attempt to activate the VPN client on the mobile device, all installed applications will be enforced to connect to the internal enterprise network, and most likely will lose the connectivity with their backends, due to enterprise web access and network restrictions. Another concern related to security arises when a malicious app is installed on the device, while the VPN is connected to internal resources would put the enterprise data at risk. Despite previously mentioned limitations, some VPN solutions provide a Per-App-VPN technique that solves the previous security concern when a malicious app is installed on a mobile device. As long as there is no control over the device, the main problem of detecting compromised devices will still be a significant threat. The costs associated with such solutions are moderated and acceptable. Always, with the advent of the new mobility solutions that offer more outstanding enterprise capabilities, most enterprises are moving away from this type of solution, except in sporadic cases.

- ***Enterprise Mobility Management (EMM)***

In addition to Mobile Device Management (MDM) capabilities, EMM technologies entertain Mobile Content Management (MCM) and Mobile Application Management (MAM) to publish mobile applications through private app stores or what's called app catalog. These technologies publish mobile applications using standard methods, such as proxy tunnel, VPN tunnel, and app wrapping. It is essential to highlight that these technologies are very advanced and have evolved rapidly. Most of them have adopted modern technologies, such as the Per-App-VPN technique as part of their solutions. An EMM solution also offers more security controls over published applications, even if these apps are pushed from public App Stores, as long as it uses SDK or the application is AppConfig enabled (AppConfig, 2020). AppConfig provides a simple way to configure and secure mobile applications to increase mobile adoption in business. Moreover, EMM offers an MCM solution, through a published mobile application that allows enterprises to configure the component to provide access to business file-sharing systems. EMM solutions are relatively costly compared to the other solutions, and shall only be used for critical applications that access sensitive enterprise data.

- ***Public Mobile Applications Stores***

Microsoft, Google, and Apple provide public app stores. Enterprises and organizations sometimes develop their mobile applications and publish them on these public app stores to boost their sales or increase their customer base. Companies can use MAG solutions for secure access to enterprise data, if the application is accessing public enterprise data. If the application does not require access to enterprise data, then host the backend on public clouds. If the application is accessing enterprise sensitive data, then the backend has to be stored on the enterprise private cloud.

III. ENTERPRISE MOBILE APPLICATION BACKEND HOSTING

There are three main cloud models available in the market, presented as internal/private, public, and hybrid clouds. These clouds are being utilized by enterprises, and each has advantages and disadvantages from a mobile application hosting perspective. In this section, we will present the advantages and disadvantages of each cloud model.

- ***Enterprise Internal/Private Clouds***

An internal cloud is a cloud computing service model implemented within an organization's internal dedicated resources and infrastructure. A private cloud is similar to an internal cloud except its dedicated resources are hosted on a 3rd party provider. Internal/private clouds apply virtualization mechanisms, shared storage, and network resources to facilitate full control of an organization's cloud computing environment (Techopedia, 2020). Allowing published mobile applications on general stores to access the enterprise resources directly is hazardous. Therefore, it is recommended to publish mobile application restful APIs in an isolated perimeter zone, where all required security layers are available, including MAG, to inspect the incoming traffic from these applications. If the data accessed on this internal/private cloud is classified as sensitive data, it is recommended to use the EMM solution as discussed earlier.

- ***Public Clouds***

Cloud computing is an area that many enterprises endorse, and thus have migrated some of their systems to these clouds. Large enterprises are still fearful at the idea of hosting thir data on a third-party cloud solution, due to government regulations or security concerns (Srinivasan et al., 2015). Most of these enterprises are hosting none sensitive data on 3rd party cloud solutions via web browsers and mobile apps. The costs of these solutions in the absence of mobile management solutions are relatively cheap. These mobile apps will be published in public stores and downloaded by users to consume the enterprise resources hosted on the public cloud using published restful APIs. If the cloud provider is offering EMM or MAG services, it is recommended to use them to ensure protection of a sensitive enterprise’s data.

- ***Hybrid Clouds***

The hybrid cloud is primarily a private cloud that allows an organization to tap into a public cloud when required for information sharing. This model provides a more efficient means to maintain data and applications security (Srinivasan et al., 2015). This will enable the organization to keep sensitive data on a private cloud and share information publicly through public clouds, to benefit from the high computing resources that public clouds offer. Hybrid clouds will help enterprises and organizations to host their public mobile application backend that can be shared with the community as well as hosting sensitive mobile application backend on private cloud.

IV. POSSIBLE PUBLISHING METHODS FOR ENTERPRISE MOBILE APPLICATIONS

From the discussion in previous sections, we can highlight the most common publishing methods for mobile applications:

1- Mobile Application published on public apps or enterprise private stores, accessing public information hosted on a public or hybrid cloud

2- Locally developed mobile application using MAG SDK published on public apps or enterprise private stores, accessing enterprise non-sensitive data hosted on an enterprise private cloud

3- Locally developed mobile application using MAG SDK published on private app store/catalog accessing enterprise sensitive data hosted on an enterprise private cloud

4- Locally developed mobile application using MAG SDK published on EMM environment accessing enterprise sensitive data hosted on an enterprise private cloud

5- 3rd party application using Per-App-Vpn or proxy tunnel published through EMM solution and accessing enterprise sensitive data, hosted on an enterprise private cloud

6- Locally developed mobile application using EMM SDK published on EMM solution and accessing enterprise sensitive data, hosted on an enterprise private cloud

V. ENTERPRISE MOBILE APPLICATION PUBLISHING PROCESS

There are three main steps to be considered in the mobile applications publishing process. Developing a process and enforcing it through enterprise security policy to regulate the publishing of mobile applications will benefit the enterprise and expedite the publishing of mobile applications. The process will ensure hosting the mobile application on the best cost-effective environment, while maintaining the minimum required security requirement. Moreover, enforcing the process through a corporate policy will eliminate the possibility of debates between IT analysts and security professionals, in addition to accelerating the development and publishing of these mobile applications. The following are the three main steps:

1- Identify all evaluation elements for publishing mobile applications.

2- Develop a matrix to map the results of evaluation elements with previously highlighted possible publishing methods.

3- Enforce the utilization of mobile application publishing matrix and evaluation of each application through a corporate policy.

These steps will be discussed in details in the next sections.

1) EVALUATION ELEMENTS IDENTIFICATION FOR PUBLISHING MOBILE APPLICATIONS

There are many evaluation elements to be considered while developing the process. Each organization/enterprise will always have its own priorities and business dimensions for selecting IT services published on mobile devices — that makes it very challenging to standardize these evaluation elements. Therefore, enterprises/organizations should not be limited to evaluation elements introduced in this paper, and it is possible to define other elements based on the business nature and demand. The evaluation elements should consider all enterprise aspects that an organization needs to achieve its objectives in mobilizing IT services. In this section, we will provide the essential evaluation elements required for any mobile application, where these evaluation elements must be imposed on many IT entities, to evaluate each mobile application. The following are the most common evaluation elements that must be considered in any application evaluation.

- ***Business Demand***

Evaluating business demands for publishing an IT service on mobile devices is an essential measurement as many services can be published, and gets decommissioned because of little utilization from users, or availability of better off-the-shelf applications by the time the application gets published. Therefore, this is a very critical measurement and sometimes requires end-user involvement, to see how much the impact would be once the mobile application got developed and published.

- ***Targeted User Profiles***

The type of users the mobile application will be developed for should be considered as one of the most crucial evaluation elements before publishing the mobile application. Many user profiles do not require a device management system. An example is the development of a commercial mobile application that needs to be available publicly for anyone should be published in general stores, unlike other applications that are designed for enterprise employees, which require at least mobile application management to apply the minimum-security controls to ensure the enterprise data are protected. Some applications are designed to serve executive users, where exchanging data between applications needs to be treated with high confidentiality. Such applications will require device and application management, which in this case it has to be an EMM solution and sometimes a coexistence of EMM and MAG solutions.

- ***Data Classifications***

Classification of data plays a significant role in the evaluation process. The organization/enterprise needs to ensure the mobile application is published on a reasonably secured infrastructure by satisfying the confidentiality, integrity, and availability (CIA) triangle. Moreover, data classifications will determine the best publishing method for a specific mobile application. If the accessed data from the mobile application is classified as public use, then the application does not have to be published on managed devices through EMM. If the data accessed are classified as confidential, then a set of security controls, such as device encryption, enforcing device passcode, inability to access malicious websites, and detection of jailbroken/rooted devices, must be implemented, which will require an EMM solution.

- ***Devices Ownership***

In this section as mentioned earlier, we considered only iOS and Android devices. In general, there are four significant concepts when availing mobile applications on mobile devices. The first concept is available for devices that consumers/customers use to access enterprise public data for information. This type will not require device management since these devices are not going to access corporate data such as employees' salaries, medical records, etc. The second concept is Bring Your Device (BYOD), enabling employees to enroll their own devices while maintaining users' privacy. This concept is the most adapted in enterprises/organizations, as it offers flexibility and low costs since the employees or users will bring their own devices, and the organization will provide management solutions to manage these devices and access to internal resources (Tse et al., 2016). Enterprises are hesitant to enable Android devices, due to the variety of Android device manufacturers. Therefore, the third concept, Choose Your Own Device (CYOD), becomes a preferable option as it enables users to choose their own devices from an approved list of devices by the organization. This will limit the operational overhead when supporting users. The other concept is Corporate-Owned Devices (COD). This concept is very costly as it requires the organization to purchase special types of devices and manage them through MDM or EMM solutions. It is the most recommended approach for enterprises seeking high security to protect highly sensitive data, as users can be limited to access a single or a set of applications, based on authorization provided by the EMM solution.

- ***Type of Application***

There are three types of applications. One of which is an application developed based on EMM or MAG SDK. It will require the developer to utilize the SDK to bundle the application with predefined security controls and features that are compatible with the EMM or MAG solution that will be used for publishing the application. The application will be shared with the systems administrator to be posted to registered users or public app stores. EMM SDK will require a proxy tunnel component to ensure only approved traffic coming from these apps and registered devices. Similarly, the MAG SDK will provide only authorized traffic from approved applications to consume published APIs (Johnson et al., 2016). Another type of mobile application is the wrapped application, requiring the EMM wrapping engine to bundle the application and publish it to registered devices or users. Enterprises/Organizations are not comfortable with such a solution, since the application source code will be shared with the vendor though it may consist of sensitive information. Products offering such techniques are phasing out this problem, as SDK is much more reliable and provides more control over published applications. The third type of application is comprised by 3rd party apps that cannot be published using SDK nor app wrapping. These applications may require access to enterprise data, and therefore will require management. Some EMM and VPN providers offer a Per-App-VPN solution for such applications that are not compatible with SDK or cannot be wrapped.

- *Application Backend Access*

Mobile applications can be published to access enterprise data or without access to enterprise data. If the application requires access to corporate data, then there are only two backend hosting options that need to be considered in these evaluation elements.

- Accessing sensitive and non-sensitive data stored on enterprise private cloud
- Accessing non-sensitive data stored on enterprise public and hybrid clouds

2) PUBLISHING MOBILE APPLICATION MATRIX DEVELOPMENT

Developing a matrix — to map the results of identified evaluation elements with the most possible publishing methods highlighted in the previous section — is an essential step to be able to determine which method can be used for publishing the mobile application. It is entirely based on the results of elements evaluation. Each organization/enterprise has the freedom to come up with its own matrix based on its own priorities and business dimensions or alternatively can utilize the Mobile Application Publishing Adaptive Formula that will be introduced in another research paper.

3) ENFORCING CORPORATE POLICY FOR PUBLISHING MOBILE APPLICATIONS

After developing the Mobile Application Publishing matrix, an enterprise security policy must be well-defined to enforce the new procedure for publishing mobile applications within the enterprise. Failure to implement the system will retain this ambiguity between IT analysts and security professionals. The policy also must have a waiver for any mobile app that requires a different publishing method not resulted from the publishing matrix. The Enterprise Cybersecurity Steering Committee must approve the waiver for such an application. Of course, some of these applications sometimes require a different publishing method as needed for the business.

VI. SUMMARY

Organizations need to publish mobile enterprise applications most securely and cost-effectively for reliability. When an organization does not evaluate the application thoroughly based on available platforms, it could be published on unsuitable or unsecured platform that may be expensive or expose the corporate/enterprise sensitive data. The cheapest media are public ones, but they pose substantial security risks to organizational and personal data. Enterprise Mobility Management (EMM), Mobile Access Gateway (MAG), Mobile Application Management (MAM), Mobile Device Management (MDM), and public app stores are provided as examples of the available platforms, and each has their advantages and disadvantages.

The Mobile Application Backend can be hosted on one of three clouds, private, public or hybrid models. Each one has its advantages and disadvantages when it comes to publishing mobile applications. Enterprise sensitive data access from mobile applications should be hosted on a corporate private cloud to ensure having full control over the data and it is protected against cybersecurity threats. Moreover, public information can be hosted on public or hybrid clouds to get use of the high computing resources available on these public clouds, and also ensure the access to these data is isolated from the enterprise internal network. Public and hybrid clouds help organizations and enterprises to share public information with the community, without exposing corporate sensitive data to potential cybersecurity risks.

Publishing mobile enterprise applications takes a 3-step process. The first step is to identify the evaluation elements to be used for evaluating each mobile application. A set of mandatory elements were provided but organizations should not be limited to these provided elements. The second is to develop a Publishing Mobile Applications Matrix for proper selection of management solutions based on the results of evaluation elements. This will ensure that the application is published on the most efficient and secure platform. Finally implement the mobile application publishing policy to ensure that there is no conflict between information technology analysts and information security experts when it comes to publishing mobile applications.

REFERENCES

[1] AppConfig. (2020). AppConfig Community. https://www.appconfig.org/

[2] Unified. (2020). CA Mobile Access Gateway, Unified IT Services. https://www.utsin.com/ca-mobile-api-gateway/

[3] Johnson, R., Stavrou, A., & Sritapan, V. (2016). Improving traditional Android MDMs with non-traditional means. *2016 IEEE Symposium on Technologies for Homeland Security (HST)***.** https://doi.org/10.1109/ths.2016.7568883

[4] Tse, D., Wang, L., & Li, Y. (2016). Mobility management for enterprises in BYOD deployment. *2016 IEEE Trustcom/BigDataSE/ISPA***.** https://doi.org/10.1109/trustcom.2016.0120

[5] Srinivasan, A., Md, A., Vijayakumar,V. (2015). Era of Cloud Computing: A New Insight To Hybrid Cloud. *Procedia Computer Science 50 (2015) 42 - 51*. https://doi.org/10.1016/j.procs.2015.04.059

[6] Curran, K., Maynes, V., & Harkin, D. (2015). Mobile device security. *International Journal of Information and Computer Security*, **7**(1), 1. https://doi.org/10.1504/ijics.2015.069205

[7] ENISA. (2017). Privacy and data protection in mobile applications. *A study on the app development ecosystem and the technical implementation of GDPR***,** *1*(1), 8-70. http://www.enisa.europa.eu/

[8] OWASP. (2020). OWASP mobile security testing guide**.** *OWASP Foundation | Open Source Foundation for Application Security.* https://owasp.org/www-project-mobile-security-testing-guide/

[9] Palomba, F., Salza, P., Ciurumelea, A., Panichella, S., Gall, H., Ferrucci, F., & De Lucia, A. (2017). Recommending and localizing change requests for mobile apps based on user reviews. *2017 IEEE/ACM 39th International Conference on Software Engineering (ICSE)***.** https://doi.org/10.1109/icse.2017.18

[10] Sardasht, S., M., B., & M., R. (2016). Mobile application security platforms survey. *International Journal of Computer Applications***,** *133(*2), 40-46. https://doi.org/10.5120/ijca2016907736

[11] Sturm, U., Schade, S., Ceccaroni, L., Gold, M., Kyba, C., Claramunt, B., Haklay, M., Kasperowski, D., Albert, A., Piera, J., Brier, J., Kullenberg, C., & Luna, S. (2018). Defining principles for mobile apps and platforms development in citizen science. *Research Ideas and Outcomes***,** 4**,** 23394. https://doi.org/10.3897/rio.4.e23394

[12] Techopedia. (2020). What is an internal cloud? - Definition from Techopedia**.** *Techopedia.com.* https://www.techopedia.com/definition/26648/internal-cloud

[13] Zhou, Y., Su, Y., Chen, T., Huang, Z., Gall, H. C., & Panichella, S. (2020). User review-based change file localization for mobile applications. *IEEE Transactions on Software Engineering***,** 1-1. https://doi.org/10.1109/tse.2020.2967383

[14] VMware Enterprise Mobility. (2020). VMware, Inc. https://www.vmware.com/topics/glossary/content/enterprise-mobility