TRIGENT

Best Practices in Enterprise Mobile Security

Anuradha Muralidharan

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

Introduction

Corporate IT managers face a challenge as more and more employees use a wide variety of devices and mobile apps to access enterprise data, interact and collaborate. The point to be remembered is, mobile devices were originally designed to address consumer needs and they therefore lack the stringent security required for enterprise collaboration. In fact, many of these devices are not under the control of the IT security teams, and therefore are not secure in the same way as laptops and desktops.

While security continues to remain a challenge, enterprises realize the value that comes with the Bring-Your-Own-Device (BYOD) approach. Tech Pro Research reports that 74 percent of organizations allow, or plan to allow, employees to use their personal mobile devices for work and employees prefer to use their own devices. To go a step further, it is becoming more and more difficult to contain and control devices in the workplace or the way devices are being used to access enterprise data.

Quick Facts -

The number of mobile devices on Earth has surpassed the number of people living on it.

In 2015 more Google searches occurred on mobile devices than on computers in 10 countries.

87 percent of time spent using mobile devices is spent using apps.

An average of 53,309 mobile apps were released on the Apple App Store each month in 2015.

Forrester predicted people would download more than 226 billion apps in 2015.

The malware-approach to address traditional security issues cannot work for mobility. Verizon's 2015 Data Breach Investigations Report confirms that “an average of 0.03 percent of smartphones per week-out of tens of millions of mobile devices on the Verizon network-were infected with 'higher-grade' malicious code.” Thus, it is clear that focusing on malicious apps leaves out too many important aspects of mobile security.

This whitepaper delves into the challenges associated with mobile application security and suggests steps that can be followed to curtail them.

Security Threats

According to Gartner, nearly 2.2 billion smartphones and tablets were sold to end users in 2014 with 75 percent of mobile security breaches the result of mobile application misconfiguration. With the number of smartphones and tablets on the increase, and a decrease in traditional PC sales, attacks on mobile devices are maturing. By 2017, Gartner predicts that the focus of endpoint breaches will shift to tablets and smartphones.

To begin with let us look at some of the vulnerabilities in mobile app security:

- Popular apps especially send user information to an ad network. The kind of information transmitted can include IMEI data, phone number, call logs, location. Apps also collect and transmit information such as user's location, personal contacts etc. A malicious hacker can not only gather this information, but can even monitor a user's activity.
- Personal cloud services can be misused for apps on smartphones and tablets. When these same devices are used for enterprise data, there can be leakage which organizations may not even be aware of.
- Removing app protections and 'sandbox' allows malware to be downloaded to the device. The goal of sandboxing is after all to improve security by isolating an application with the intention of preventing malware and intruders interacting with the app. It is an advantage for developers who do not want their app to be touched. However, sandbox can create interactivity problems if the app has to 'talk' to another resulting in lost functionality. Because of this issue, it is tempting to remove sandbox and app protections.
- Connection hijacking is possible when an employee accesses, say, SharePoint using a public Wi-Fi. Unknown to him or her, a person could watch and save the user's traffic in real time, accessing a large amount of sensitive data. For example, several cafes, hotel lobbies etc. offer free Wi-Fi connections. It is tempting to use them.

> According to a recent CoSoSys survey, 35 percent of enterprise employees think that data security is not their responsibility and 59 percent think that losing a mobile device or laptop with company data doesn't represent too much of a threat.

- Smartphones have limited resources, in comparison on desktop computers. Limiting factors such as CPU and RAM limit the sophistication of security solutions. Similarly, the battery of a mobile device severely limits the resources available for a security solution from the point of view of the general acceptance factor.
- Mobile apps store and transmit sensitive private user information. When this information is transmitted, security failures can happen. For example, fragmentation of the Android mobile operating system has already been discussed extensively. As a result of wide adoption of the Android operating system, vendors incorporate it in their products. However, critical items like security patches are released only later. 'Jailbreaking' on iOS and 'rooting' on Android where a user is escalated to be an administrator, enables users to access data, putting confidential information in real danger.

Defense Strategy

A recent study indicates that over 50 percent of enterprises have at least one non-compliant device. It is also a fact that employees have access to a lot of confidential data, more than probably the IT departments are even aware of.

Some enterprises have already incorporated best practices to ensure safety. They have a robust mobile device management (MDM) policy in place and this is backed by app shielding and 'containers' that protect important information. Others have a combination of MDM, MAM, MIM and BYOD which put together is known as EMM (Enterprise Mobility Management). Taking EMM a step further is MTD (Mobile Threat Defense).

Given below is a list of mobile security best practices for organizations to protect users from unwanted exposure as well as unauthorized disclosure of confidential company information.

Enterprise Mobility Management (EMM)

EMM suites enable organizations to integrate and manage mobile devices in their IT infrastructures. EMM suites configure devices and applications for enterprise deployment. These suites can verify compliance, mitigate data loss, theft, employee termination etc. It also

helps the IT team to troubleshoot device issues.

EMM's core capabilities:

- Mobile Device Management (MDM) is a life cycle management technology. It helps the organization's IT team to configure, provision and de-provision content. It also enables remote viewing and wipe out.
- Mobile Application Management (MAM) helps to apply policies and control functionality of individual applications which are delivered via an app store. It also provides analytics to help owners understand usage patterns.
- Mobile Identity (MI) helps to manage security by providing access to trusted devices and users.
- Mobile Content Management (MCM) lays down access rules for content distribution on mobile devices. It can enforce policies, content upload, download and distribution.

To summarize, EMM helps to address security concerns and a strong EMM strategy helps employees to be more productive by providing the tools they need but ensuring security is not compromised. However, seeing the potential of this space, a large number of vendors are entering the same with their offerings. There are easily over a hundred vendors in the market, and it is difficult to choose the best tools, technologies and techniques for cost-effective mobile strategy.

MTD (Mobile Threat Defense)

Gartner has recently published a report 'When and How to Go beyond EMM to Ensure Secure Enterprise'. This report underlines the fact that EMM helps to manage a mobile device fleet and enable security to a certain extent. However, EMM may not help to actively detect, analyze and respond to mobile attacks such as malicious apps, network attacks, vulnerabilities in apps and so forth. MTD or Mobile Threat Defense is equally if not more important to safeguard an organization's information security as it helps to protect sensitive data. Emphasizing its importance, in its report Gartner says, “The synergy between EMM and MTD tools allow for risk mitigation based on real-time information and intelligence sharing.”

Hotspots

Wi-Fi hotspots, a physical location providing Internet access is being adopted extensively. BYOD and advanced network infrastructure have also helped to propel the use of hotspots, compounded by the use of portable devices. There are both drivers and constraints influencing the hotspot space. One of the biggest concerns with hotspots is interception of cellular data transmission. For enterprises, especially those which encourage workers to bring their own devices to work, free Wi-Fi hot spots can be a serious security concern. For example if a worker logs in to the enterprise system from a hotspot, there is the possibility that a hacker can gain access to the entire corporate database. By combining two factor authentication and VPNs it is possible to secure business information. VPNs generally make it difficult for hackers to read passwords. Adding another line of defense ensures that even if the password is compromised, there is another level of defense in place. Employees who have data plans can also consider tethering their phone or device. Finally by encrypting data it is possible to defend data successfully.

Antimalware software

MTD brings us to the next pertinent point, i.e. anti-virus for mobile devices. Anti-virus is basically pointless as it works in an app-centric manner, i.e. anti-virus will not scan all the apps installed in a device. It will work only on a particular application. However, that does not mean that it is useless or unnecessary. The best method to ward off viruses is to keep the phones software up-to-date. Android and iOS are regularly updated for security purposes and users need to update their software whenever they are prompted to do so. This will help to some extent to ward off viruses.

Malware on the other hand can virtually take any action when running with high privileges. In the case of mobility, we need to worry about information or identity theft. This kind of behavior can be embedded in inconspicuous looking apps such as games, installed from third-party app stores. Since a smartphone is a personal device and moves around with the user, it becomes an ideal target to snoop private data, such as contacts, SMS messages and so on.

As the first step, every mobile device needs to be installed with antimalware software. In the recent past, Android, for example, has been targeted for malware. The organization must have a policy whereby anyone using their device for accessing official sites and information, must have antimalware software installed on the device. Not installing antimalware would mean that malware after an invasion has to be detected. This is extremely difficult. If before installation, the user notices unresponsive graphical interface or a faster battery exhaustion, the user has room to be suspicious that a malware has invaded his smart phone.

Secure Mobile Communication

It is a good practice that all mobile communications be encrypted, as wireless communications can be intercepted. For enterprises, the suggested strategy would be to go one step further, and insist on VPN access for a mobile device to connect to the company's network or to a cloud. VPNs come with strong encryption, they enable logging, management and authenticate users who wish to remotely access enterprise data.

Password Controls

Mobile devices today already have several inbuilt security options such as biometrics – fingerprint or iris scan, voice print recognition, orientation, proximity and so forth. However, even older devices have security measures such as one-time passwords. Organizations granting employees access to official data on their respective devices should ensure that they have a robust MDM policy in place and the security options comply with the organization's data policies. Going a step further, more than pre-determined number of failed log in attempts should cause the device to wipe its internal storage clean.

Limit third-party software

Organizations which encourage employees to carry their own devices to work, should have a sturdy policy to block or limit third-party software. This is, by far, the best way to prevent security compromise and avoid breaches.

A feature of smartphones is the ability to install all kinds of (closed source) 3rd-party software. Those applications may contain unwanted routines which are very hard to detect.

But even an unsuspicious looking weather application which requests forecasts over the Internet connection and which might automatically retrieve updates based on the current location (which is known through the embedded GPS sensor) is perfect to spy on the user. In order to detect such unwanted behavior, some research has been done on this topic. There exist a few frameworks for Android which decide on the basis of the stakeholders' policy invariants which application requests are granted or denied. The downside of this approach is that the source code is required and that it is solely for analysis purposes as no intervention is possible.

Default Configurations

Because smartphones deal with broader and broader application domains, their operating system and their programs become comparable to desktop computers. Both systems share the same architecture and in many cases even the exact same technologies, e.g., the operating system or web browser back end. Thus, their security can be tightened with the same technologies. A good example is the Android platform, where applications run with different UIDs and are further separated through their own JVMs. Virtualization in general may enhance the overall security of smartphones and these techniques should also be used at the heart of smartphone operating systems and include Address Space Layout Randomization, stack protection and non-executable writable memory. Mandatory Access Control lists may further enhance overall smartphone security. It is ongoing work to enable all these techniques on the different platforms. Smartphone services and applications should have sound default configurations and should only run when their services are required.

Secure Gateways

A suggested method is, employees can be given access to remote virtual work environment. The only information then that goes to the device is the screen output from work applications and the data therefore does not persist when the remote session ends. Also remote sessions are through VPN connections which are normally very safe and secure. It is also a great idea to prevent download of files to mobile devices.

It is vital that an organization clearly understand what are the systems and applications that an employee might need to access on his or her mobile device. If the mobile traffic can be managed through special gateways and firewalls, then this will help in filtering content and keep security measures in place.

Mobile Security Testing

At least once a year or maybe more often, organizations should conduct a security audit of mobile devices with penetration testing to see how secure their mobile security system is. This kind of audit helps to remedy and mitigate issues they may discover.

Summary

The fear around mobile security for enterprises is not exaggerated or unreal. The first step forward is for enterprises to acknowledge and accept the fact that mobile devices are very much a part of employees' lives. And whether we like it or not, employees do carry their smart devices to work and check it frequently when not in office. This essentially means that employees are already using their smartphones for official work. By having a BYOD policy, enterprises can benefit from increased productivity. BYOD should be seen as both a technology and a business strategy for its positive effects to be felt, and the results to be transformative. It enhances employee flexibility giving him the chance to work remotely and react quickly. The fact remains that any data out there, on a secured or unsecured network is vulnerable. So are the apps which employees download on to their devices. The way forward is to have stringent security policies in place and make this the right time to harness this trend in a secure manner. The other option of barring BYOD may not work in the long run.

About Trigent

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.