ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Android Security: An Overview of Risks and Security Measures

A.J.Singh[1], Akshay Bhardwaj[2]

Professor, Computer Science, HP University, Shimla, India [1]

Student, Computer Science, HP University, Shimla, India[2]

Abstract: New technologies always create new areas of concern for information security teams. Usually early adoption of such products is slow and it allows some maturity to develop in the play store(previously Market), providing time for the development of effective security controls. Indeed often these new devices will be slowly introduced to the corporate/government environment as part of an internal strategy. The rapid growth of the Smartphone play store(previously Market) and the use of these devices for email, online banking, and accessing other forms of sensitive content has lead to the emergence of a new and ever-changing threat landscape. This combined with the fact that anyone can be user has led to smart phones appearing as part of the corporate/government estate before the appropriate controls are in place. Even without these technologies connecting to the corporate/government network, there are security implications brought about by their mere presence in an office environment. A malicious user or malware on the device can create a number of risks for an organisation, and so the fact that these devices are not necessarily connected does not translate to a lack of security risks. This paper will discuss why it is important to secure an Android device, what some of the potential vulnerabilities are, and security measures that can be introduced to provide a baseline of security on Google's mobile OS.

Keywords: android, security, hacking, smart phones, risks, measures.

I. INTRODUCTION

Initially fuelled by the introduction of the i Phone, the smart phone play store(previously Market) is growing exponentially, but there is one OS in particular that has been enjoying particularly rapid development recently. That system is Google's Android, which according to Gartner has grown from a 23% play store(previously Market) share last year, to become the dominant play store(previously Market)force from 38% in 2011[1] to more than 53%(more than 85% in developing countries). As the user base has grown so too have the risks associated with the OS. The reason for the rise of Android is choice – consumers are able to choose from a broad range of manufacturers and price levels opposed to Apple's mono-device approach (although an i Phone 'light' has long been rumoured). With so many connected devices entering pockets and handbags, what is the risk for employers? What measures can consumers and enterprises take to protect the information stored and accessed by these devices?

Despite some challenging the impact of mobile malware as overhyped, new figures would suggest otherwise. Mobile malware was always rife on Symbian but rapid adoption of mobile platforms by both personal and business users has seen to become more attractive to cybercriminals. In 2011, 20% of all cybercrime in UAE occurred on mobile devices[2] and Goode Intelligence found that up to 18% of organisations in the UK had experienced a mobile malware incident[3]. Such figures demonstrate that it is not just consumers who are at risk to such threats but enterprises too that are failing to implement effective mobile security measures. Trends in mobile threats have matched what we see at a wider industry level, with Android becoming the most-targeted of the mobile platforms, according to McAfee, much as Windows has on the PC. The number of Android devices under bot net control has peaked at 40,000 Android devices worldwide on several occasions[4], and the problem is getting worse with Lookout claiming 0.5-1 million users were infected in the first half of 2011[5]. In Q2 there were no new malware signatures detected for i OS , whereas there were 44 for Android in that same time period[6]. The threat is very real, and rapidly developing. In emerging as the top mobile platform, Google's little green Android has painted a big red target on itself.

The threats we see appearing on mobile, are not going to be a new concept to the security professional – root kits, Trojans, and even botnets are making appearances. Indeed the Spy Eye botnet has successfully transitioned from the PC to Android, highlighting the commercialisation of mobile malware. The Android incarnation of Spy Eye, Spitmo, utilises a familiar approach, namely convincing users it is a legitimate security measure for their device[7]. Mobile malware such as this strive not just to acquire data but also to monetise the attack by using the device to access premium SMS and voice services. The open nature of Android and its large user base have made it an attractive and profitable platform to attack. Common exploits and tool kits on the OS can be utilised across a wide number of devices, meaning that attackers can perform exploits en masse and re-use attack vectors. It is obvious why Android is a target, but why isit vulnerable? Google did take measures in the development of the

DOI 10.17148/IJARCCE.2015.4544

Android kernel to build security measures in; the OS is sandboxed, preventing malicious processes from crossing between applications. Whilst this attempt to eliminate the concept of infection is admirable in some regards, it fails to address the issue of inflectional together.

Android is a victim of its own success, not just in the way it has attracted malicious attention, but in its very nature. One of the reasons the OS has succeeded in gaining play store(previously Market) share so rapidly is that it is open source, it is essentially free for manufacturers to implement (patent settlements excluded!). Additionally this has led to substantial fragmentation of Android versions between devices and means that vendors have been reluctant to roll-out updates, presumably out of some concern regarding driving demand for future devices. There is little value to the manufacturer in updating a device, something that to date Google has tried to encourage but been largely un successful in doing so. Where updates do occur, manufacturer specific software on top of Android (such as HTC's Sense or Motorola's Blur) and even network provider bloat ware, serve only to further delay patch management. After Google release an update this must then be customised by the manufacturer and network before release, unless of course it is a vanilla device such as the Nexus range. As a result vulnerabilities are left un patched in stock ROMs, and advanced users are turning to flashing custom ROMs on their devices which raises a whole host of other issues. In an enterprise environment, who is responsible for patching a connected consumer device?. And what of the users? Increasingly employees want to be able to use their smart phones at work, they want to access their email on the go, may need to access a content management system, and might prefer to log on to the corporate/government network than use 3G. Where Blackberry went from enterprise to consumer in terms of play store(previously Market)penetration, Android is doing the inverse (much as iOS has) – consumers are buying these devices for personal use but wanting to utilise them in a professional capacity as well but without regard for the impact. So what does this mean for security? What threats are there to corporate/government information assets?

II. THREATS/WEAKNESSES

Taking specific malware out of the equation, what are some of the threats/vulnerabilities on Android devices that might be cause for concern? These certainly are not comprehensive, but do cover a significant range of the vulnerabilities and risks that may be exploited on the Android OS:

Admin powers to user

Install apps, grant app permissions, download data, and access unprotected networks - The user can reign free over their Android domain without restriction.

The Android Play store(previously Market)/Google Play Store

Google's verification processes for applications entering their play store(previously Market) have been shown to be woefully lacking over the last year or two, leading to a number of malware-infected apps and games being made legitimately available to users.

Access to PC

HTC devices have long been able to utilise a VPN, but increasingly other applications are becoming available for remote access – Go to Meeting, Team Viewer, Remote Rack space. Although secured, these third party services still provide a line in to the corporate/government network and may be implemented fairly easily on to an end point.Any Android device can be connected to a PC via a USB cable, laying out the contents of its SD card for read/write/delete. The SD card itself as removable storage can be easily accessed directly as well. Indeed these methods couldbe utilised themselves for bringing malware in to a corporate/government network, for downloading malicious content on to a PC or sucking up data as soon as it is connected.

App permissions

In the form of a pop up, the user may see these notifications as a nuisance, a delay in accessing the newly downloaded Angry Birds levels. Or they may simply not understand the nature of the requests. Common permissions that may (read: should!) raise an eyebrow would include 'Read/Send SMS', 'Access Fine Location', 'Access IMEI, phone identity', 'Brick' (required to disable the device in trace and wipe apps), 'Access camera', and so on. Such requests may be integral to functionality, but could equally be recording calls and transmitting sign-in credentials.

Malicious Apps

Data/process transfers between virtualised application environments are handled by a protocol of implicit and explicit intents. Transmission or interception of an intent by a malicious application can result in data being compromised as the target app will respond to the string, potentially resulting in data loss.

Third Party Applications

One of the great things about Android is choice in terms of standard functionality, such as address books, messaging, keyboards, etc. I'm sure no one in the information security industry would need an explanation as to why it might not be a good idea to use an un trusted third party keyboard or password manager. In a rapidly growing OS environment it can be difficult to identify reputable vendors, and considering the nature of the Android community, can you trust a bedroom programmer with your credentials? Even reputable services can get mobile applications wrong, both Face book[8] and Twitter[9] transmit mobile app data in the clear, i.e. without encryption, on nearly all devices. This happens despite the development of such security measures for web app versions.

Rooting

Rooting an Android device is akin to jail-breaking an i Phone, it opens out additional functionality and services

DOI 10.17148/IJARCCE.2015.4544

to users. The process of gaining root access, requires the device to be switched from S-On to S-Off (where S =security). Additionally, root is a common exploit used by malicious applications to gain system-level access to your Android. Droid Kung Fu is one such threat that can root a system and install applications at that level, it escapes detection by utilising encryption and decryption to deliver a payload[10].

Wi-Fi
The vulnerability of Android devices running from 2.3.3 to 4.2.1 compromise on unprotected Wi-Fi networks apparently came as a surprise to many –[11] it shouldn't have, when is this practice ever safe?! Beyond highlighting the need for better consumer security awareness, it leads to some other considerations around secure Wi-Fi access. Ideally sign in credentials should always be completed over a secured network, but sometimes this isn't enough. Face Niff is an easily downloadable application that allows the user to intercept the social networking logins of any Android on their network[12]. The only way this exploit won't work is if the user is utilising SSL. Furthermore, devices running 2.3(or rooted older devices) can act as a Wi-Fi hotspot – as an Information Security Manager, how happy would you be about unverified users and devices connecting to a smart phone with a corporate/government footprint?

Remote Installation
To users, the Android Web Play store(previously Market) is a blessing. Its introduction meant a much more accessible and digestible platform for discovering the latest applications. Additionally there's no need to go back to your device when you find something you want, you can simply install it remotely from a PC. Third party Android play store(previously Market), App Brain, also offers a similar service (and actually beat Google to it in the first place). All versions of Android were at one point vulnerable to the remote writing of malicious JavaScript to the SD card through accessing an infected web page[13] – an html download does not prompt for user confirmation on the OS, it simply happens. This is now restricted to versions 2.2 and below as the issue was addressed by Google in the Gingerbread (2.3) update. For devices still operating versions with this vulnerability, using Opera Mobile instead ofthe default web browser will trigger a confirmation when such download attempts begin, allowing the user to deny access.

Privacy
By default, all new devices (previously only HTC devices) geo-tag photos and Tweets. This is the primary issue with Android as a consumer device functionality over security. Other applications claiming localised services could utilise GPS permissions for location tracking.

Manufacturer/Vendor trust
Whatever their intentions, manufacturers play a significant role in user privacy. Uncovered recently is an application that sits at root level on new HTC devices (Evo, Evo 3D, Thunderbolt, Sensation) which collects and transmits a range of information on users including accounts, phone numbers, SMS, system logs, GPS locations, IP addresses, and installed apps[14]. It is bad enough that HTC feel it is appropriate to collect and use this data without notifying the user, it is even worse that it failed to secure it! Consequently any app with the 'Access internet' permission can access this data.

Cloud Updating
It suffers from the following shortcomings:

- Slow patching, if at all
- OTA updates
- A lot depends on forces outside of Google
- Some devices will not support 4.0
- Google releases the update or patch, device
- maker customizes it, then carrier customizes it as
- well.

III. SECURITY MEASURES

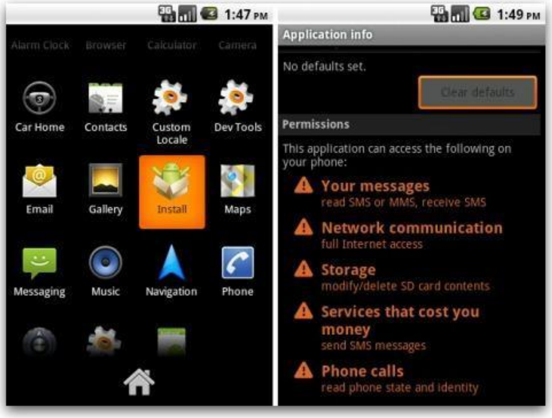
So now we know a little more about how an Android might be compromised, we can understand about some of the controls and mitigation processes we can take to protect the device and the information it may access. Some of this advice could be implemented by best practice, policy, or a user toolkit within the enterprise, but roll out to individual user devices should also be considered.

Root and S-off
An illogical suggestion, surely S-off isn't going to further security on a device? I argue otherwise, yes rooting a device opens up the root level to access, but it also allows the user to exercise control over it. Upon completion of the root process, the flashed Clockwork Recovery Mod will install the Super User application. Super User notifies on all requests for root access, asking for authentication of the process. Immediately threats such as Droid Kung Fu become less intimidating, it can do very little at a root level if that root is controlled and monitored.

Permissions management
Many of the attack vectors and vulnerabilities which might be considered feasible on an Android device, rely on being able to overcome the OS sandboxing.(Fig.1) The problem is, the user has only two options when they install new applications – accept the permissions and allow the install, or reject them and don't get the application. In all but the most security savvy of general users will the second ever really be considered. Some applications can act as somewhat of an application firewall and can solve this problem by granting the user the ability to block an application's individual permissions. I might be happy for a game to have internet access, but I can then block other permissions I feel unnecessary such as sending SMS or reading my phone number. These applications will only work on rooted devices, but are one of the most effective security measures you can take on Android. You can set permissions, and will be notified of any requests that you haven't already specified a preference for. Additionally

DOI 10.17148/IJARCCE.2015.4544

these applications keeps a full security log of every permission request made by every application – a realeye-opener and the first example of SIEM on Android?



No defaults set.

This application can access the following on your phone:

Your messages
read SMS or MMS, receive SMS

Network communication
full Internet access

Storage
modify/delete SD card contents

Services that cost you money
send SMS messages

Phone calls
read phone state and identity

Fig. 1. Fake Instagram App

Logging

The issue with new android devices logging and transmitting user data is a significant vulnerability and the only 'out of the box' option is to wait for a patch. This simply isn't good enough. If you are using a rooted device you have two options: 1) flash a non-stock ROM such as Cyanogen Mod, 2) navigate to system/app and delete the file com.htc. loggers.apk(in HTC) .For now this is as good as it gets for a fix. Even if you run this, it is not to say that the problem is totally solved. There are other preloaded system apps which raise an eyebrow, for example androidvncserver.apk which isa remote access tool – it could easily be innocuous or tied to functionality such as trace and wipe, but it is certainly something worth being aware of.

Remote Detection and data wiping

If your Android device is lost or stolen, you can use these applications to remotely ping the device for its location and/or instruct it to delete specific content. Manufacturers such as HTC provide such measures on their devices, but third parties and AV vendors provide similar services also. The only problem with a great number of these is the ability to prevent them – if you remove the SIM, wipe the phone, or kill the data connection there is nothing you can do. Taking out some of these 'trace and wipe' apps really is as easy as uninstalling them from the Application Management menu. Any solutions on that basis should be manufacturer implemented or be at root level, e.g. Theft Aware, to prevent them from being by passed. Theft Aware also does the obvious and conceals its identity with an innocuous name designated by the user; the hidden application remains visible but concealed until it is activated, at which point it disappears from the front end altogether.

Device locking

The reason for implementing some level of screen lock security on a smart phone should be pretty obvious to even the most novice user. Such a mass of personal data and material simply can not be left on a table, available to all who are willing to swipe to unlock. Off the shelf Android addresses the issue with two propositions – a PIN or familiar pattern (a la i P hone and GrID sure). Beyond the usual social engineering and finger smear tracing type exploits, this does a pretty competent job of preventing an unattended device relating in data loss. Other such solutions are available from the Play store (previously Market), with the most inventive of these being Hidden Lock. This app works by returning your locked device to the previous screen but with all the functions blocked – the device can only then be unlocked by correctly selecting the position of an invisible padlock.(Fig.2)

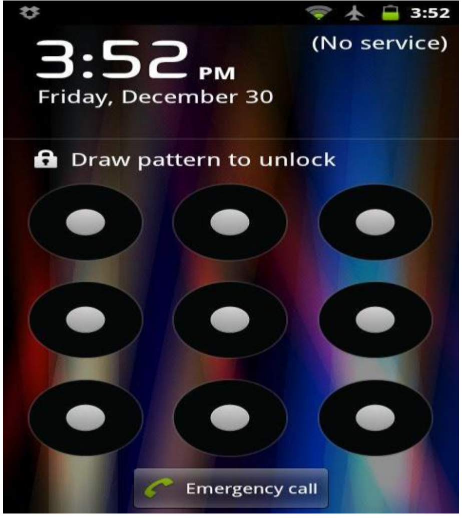


Fig. 2 Password Screen

Securing data

Firstly all the usual security rules need to be exercised, e.g. only connecting to trusted, secure networks. Beyond this though, the user needs to consider what the appropriate security measure is for whatever they're doing –encryption for data transmission, VPN for secure connection. Whisper Core provides full desk encryption and also retains an encrypted backup of all data on the device. The system is designed to be unobtrusive, keeping impact on users to a minimum. It encrypts at 256 bit AES. This is a great way to protect against data loss in the event of a stolen or missing handset, if trace and wipe fails, you can rest safe in the knowledge that any sensitive information or business assets are locked down. You'll want users to keep their encryption keys safe of course. With encryption implemented, mobile data is secure at rest. In order to keep it secure in transfer, then a VPN solution should be considered. This may be manufacturer specific (HTC), from a reputable security vendor (Astaro),or a specialist start up (Tunnel Droid). Encryption can be enabled as part of the VPN client built in to the OS, although a more controllable solution provides more powerful protection.

Installing trusted packages

Given the ability to install non-Play store(previously Market) applications on to a Google device off the bat (unlike i Phone where jail breaking is required), and the recent spate of malicious apps on the Android Play store(previously Market), it might be time to consider verifying contents of APK files. For the uninitiated, APK files are the standard Android install file format and are a variant of JAR. A program cal ed APK Inspector has been released that will scan the assets, resources, and certificates contained within the APK to ensure it is secure. This is available via http://code.google.com /p/apkinspector and could be utilised as part of the application install process to ensure all packages are verified before being flashed to the phone.

Anti-virus

Shutting the door after the proverbial horse has vaulted, anti-virus by itself is a great way to do security wrong. It is however a useful failsafe, and a must as part of a comprehensive security solution. The lack of malware signatures, hardware limitations, and an uncertain play store(previously Market) potential in the early days of Android meant that the big players were initially reluctant to enter in to the space with bespoke solutions. This left a gap for smaller niche players to gain some degree of play store(previously Market) share. Indeed even now mobile specific AV is available from some of the larger vendors only as part of a wider ‘all device’ package. Two of the most reputable AV packages on Android to date have been from start ups, and in the form of free download. The free price point helped Droid Security grow its install base to 4.5m users rapidly and led to its subsequent acquisition for $4.1m by AVG[15]. Another popular Android security vendor is Lookout which has raised $40m in its last round of VC funding[16]. In the mean while all the big security players have rushed to get their solutions to play store(previously Market), and so recently we have seen the likes of Norton, Kaspersky, and Trend Micro enter the space with offerings. Many of these applications are fairly comparable in terms of performance and detection, although there are several issues with the concept itself.

Firstly is the problem of where the AV scans, it covers the apps folders, SD card, SMS, and contacts typically. None of these apps are asking for root access, and therefore they are failing to search for infections on the area of the device thatis most targeted and vulnerable. With no root integration how useful can mobile antivirus be? It is comparable to only scanning Documents & Settings on a PC, ignoring altogether Program Files and System folders. This coupled with the fact that many of the household names’ Android AV packages are readily available in cracked versions on warez sites, is a significant cause for concern. If a security application can not maintain its own integrity, how effective can it be? Indeed there is even talk of an exploit on the OS that allows AV to be bypassed and deactivated altogether. We come back to where we started then, AV on Android must be part of a wider security solution.

Authentication

Much of the mention of authentication around Android comes in the form of using the devices as a means of authentication, like an OTP or token. What is often overlooked is authentication on the device itself. Google has recently taken to factoring this in to the latest update to the Play store(previously Market) (for those fortunate enough to get a push update or who have managed to do this manually), the user can now set a password which must be entered before any purchases are possible. Given that this is now essentially baked in to a system app, how feasible would it be for Google to implement this in to the Android framework. That way password protection can be integrated in to other processes such as updating corporate/government email, posting to company Twitter accounts, and so on. Some manufacturers are now starting to implement biometric authentication in to devices such as the Motorola Atrix, and a number of iris and fingerprint recognition applications are available on the Play store(previously Market). As with all personal data, and these physical traits are still information, vendor trust is imperative and the same questions that all security suppliers should expect are applicable: Who holds the data? How is it stored? Who has access to it, is it shared with 3rd parties? Is it destroyed if you opt out of the service? As secure a measure as biometric authentication can be, smaller suppliers must be scrutinised, if the technology becomes more widely used in the future then you will never be able to change your ‘password’ if it is compromised.

Link security

Users love to click links. Whether it be in a phishing mail/pop-up or on a friend’s Face book wall, malicious links are always loitering in the background waiting to seduce and ensnare hapless users. Awareness should cure this, but its one of those on-going struggles that I’m sure will be familiar to many internal information security departments. There are a number of vendors that have created link security applications for PC, and there are options available on Android too, albeit in fewer numbers. AVG with its Mobilation app, Prey and Lookout Mobile Security seem to be leading the way here, providing a solution for secure browsing. With AV limited on the Android platform, this holistic approach to security is certainly reassuring, and more vendors should be looking to integrate as much functionality in to their Android suites as possible.

Email security and mobile device management

How do you let mobile users access their corporate/government email on an Android device? Is it better practice to set up and secure an Active Exchange sync on the default mobile app, or encourage the use of a web service such as Mimecastor OWA? To-date, Exchange is really only an option on Android out-of-the-box through an HTC device, or use of a Sense-based ROM (the latter requiring root). The HTC Mail app can be set to automatically use an encrypted SSL connection for any transfer of email data. This is the only way to comply to the security protocols on Exchange, without sending encrypted messages through a VPN using another application. Mobile Device Management (MDM) and Mobile Email Gateway (MEG) products from the likes of Good Technology, Air Watch, and Echoworx allow enterprises to roll out email security solutions that are compliant to industry standards such as SOX and HIPAA.

DOI 10.17148/IJARCCE.2015.4544

Such packages monitor, securely configure, and enforce policy over the air. Tools within MDMs such as application management and blacklisting introduce effective controls, and key system data can be accessed. One feature of such products that does leave some area for questioning is the decision to blacklist and disconnect a rooted device. This decision to exclude the root level from considerations is reliant upon the on-going assumption that a rooting process must occur for a root exploit to run. There is significant value in utilising an MDM or MEG as an additional layer of protection between devices and servers. This technology is still somewhat in its infancy and so there are limitations. One such shortcoming is around the range of supported devices, this is fine if it is a business phone, a compatible device can be selected and rolled out by the organisation, however personal devices may cause issues here. Furthermore the question of ownership creates another barrier to implementation of these products – will users accept this on a personal device, especially considering some of the measures include blocking applications, tracking GPS location, and remotely locking and wiping the handset.

Of course there is always the problem of corporate/government email accounts sitting open on mobile devices, but hopefully users will implement other measures that mean this isn't possible. Certainly one such step that should be taken is to direct the attachment cache to store to the device's memory as opposed to the SD card, ensuring that data loss isn't quite as easy as plugging and playing a micro SD. Additionally there are other controls which could be considered - notifications can be disabled and the icon and name of the app on the menu could be edited to hide the asset; it is possible to limit the number of days displayed in the device inbox, here a trade off must be made between enabling mobile working and implementing effective security in the event of a misplaced or stolen smart phone.

Firewalls

Really products like Lookout, a sec firewall etc should be helping in scratching that firewall itch on Android, but the data that is transmitted from your smart phone should be monitored as well. This may seem superfluous but given that i Phone users' location data is tracked and sent unencrypted via iTunes, this might not seem like such an un necessary measure. Whisper Core Systems, which brought FDE to Android, also offers Whisper Monitor. All outbound data is monitored and the user is notified of any anomalies depending on the rule sets and exceptions that are set up. Furthermore, if there is any traffic causing concern, URLs can be blocked and ports closed via the app to prevent the process from continuing to run its course.

Secure storage and NFC payments

There are numerous applications available via the Play store(previously Market) offering secure wallets/folders and password management. This concept offers a theoretically secure and password-protected environment for sensitive assets. However there is always the issue of vendor trust when it comes to utilising such applications to protect information. Of course when Google Wallet rolls out properly to more than one Android device (i.e. Nexus S) it should theoretically prove a logical solution to secure storage, however it will also open up the potential implications of a security breach or lost device significantly. Losing a smart phone is already cause enough for concern, but going forwards there will be more significant financial implications, as the emergence of NFC-enabled devices will mean that this is now akin to losing a debit card or wallet. Inevitably the security controls Google implements around this transaction process and its Wallet application will be carefully scrutinised, not just from an assurance stand point, but also in their impact on user experience and speed of transaction. With the roll out at such early stages it is difficult to suggest how to protect these specific assets, however with all things security, best practice can only help us.

CONCLUSION

With such a rapidly developing environment, both in terms of product innovation and the threat landscape, other security considerations will rapidly develop in the months and years to come. The measures discussed in this text serve as a good starting point in providing a baseline of security on Android devices. The preferable solution would theoretically be not to allow personal devices on to the network at all, and this may prove an effective if sometimes unpopular decision. The risk-reward ratio is never going to be appealing to a security professional, however this is one of the lesser concerns amongst users.
There is no one-stop effective security measure that can be implemented on an Android device. Certainly when it comes to corporate/government devices then one of the emerging MDM products provides some much needed functionality to the mobile security tool kit. These solutions however are difficult for organisations to implement on personal devices, and don't really provide an effective solution on an individual handset. As a user then many of the actions described here can provide comparable functionality and protection.

In the absence of a holistic solution then the enterprise or user must create a comprehensive suite of security controls and applications. The challenge here is maintaining that balance whereby security is seen as an enabler and does not impact too significantly everyday use of the device – failure to do so will lead to circum navigation of security controls. As part of security education and awareness it would be advisable to discuss some of the core security implications associated with a smart phone. Providing a suite of tools which can be installed on to a device, or offering an encrypted preloaded SD card, will ensure that exponential growth in mobile malware does not affect your organisation. A company is only as secure as the weakest supplier or user, and mobile devices create all kinds of opportunities for malicious activity – for cybercriminals the path of least resistance is going to be

DOI 10.17148/IJARCCE.2015.4544

the most tempting, and in such a new technology area there are plenty of potential exploits and attack vectors, both known and unknown, to take advantage of. In addition we can have some "best practices" that can come in useful:

- You should always have a pass code
- You should require it immediately
- It should be > 4 characters, 6 is recommended
- It should be complex
- Enable lockout/wipe feature after 10 attempts
- For true Enterprise level management you must use
- a third-party MDM .

➢ Decide which type of enrolment is best for you
➢ White list approach may be best

- Allow only devices you have authorized.
- Don't allow rooting(Although this is debatable but rooting helps only advanced users. novices might end up damaging their phones instead of any useful contribution.)
- Removes some built-in security features and sandboxing
- Can leave you vulnerable to malicious applications
- Ensure third-party MDM solutions prevent or detect rooting/jail breaking
- Address this in your mobile device policy
- Enable Password Lock Screen vs.

Face Unlock or Pattern

- Disable USB Debugging
- Enable Full Disk Encryption
- Download apps only from official
- app stores

➢ Google Play
➢ Amazon

REFERENCES

[1]. Anon., 2011. 'Norton Cybercrime report reveals 76% of UAE residents have fallen victim to cybercrime in the last year', Albawala.Available at:http://www.albawaba.com/business/pr/norton cybercrime-report-reveals-76-uae-residents-have-fallen-victim-cybercrime-last-year

[2]. Ricker, T., 2011. 'Gartner: Android grabbing over 38 percent of smart phone play store(previously Market) in 2011 on Symbian's demise,' En gadget. Available at:http://www. engadget.com /2011/04/07/gartner-android-grabbing-over-38-percent-of-smartphone-play store(previously Market)-i/

[3]. Goode, A. 2010. 'm Security Survey 2010 Report', Goode Intelligence. Available at:http://www.goodeintelligence.com/report-store/view/msecurity-survey-2010-report

[4]. Westervelt, R., 2011. 'Study tracks first signs of Android botnet infections ', Search Security. Available at: http://searchsecurity. techtarget.com/news/2240081235/Study-tracks-first-signs-of-Android-botnet-infections

[5]. Anon., 2011, 'Lookout Mobile Threat Report', Lookout Mobile Security. Available at: https://www.mylookout.com/mobile-threat report# highlights

[6]. Westervelt, R., 2011. 'Android attacks now outpace all other mobile platforms, says McAfee', Search Security. Available at:http://searchsecurity.techtarget.com/news/2240063370/ Android-attacks-now-outpace-all-other-mobile-platforms-says-McAfee

[7]. Goodin, D., 2011. 'Android banking Trojan intercepts security texts', The Register. Available at: http://www. The register. co.uk/2011/09/14/spy eye_ targets_android_phones/

[8]. Goodin, D., 2011. 'Security shocker: Android apps send private data in clear', The Register. Available at: http:// www. The register. co.uk/2011/02/24/android_phone_privacy_shocker/

[9]. Pinola, M. 2011, 'Android data vulnerability: How to protect yourself', Life Hacker. Available at: http://lifehacker. com/5802682/android-data-vulnerability-how-to-protect-yourself

[10]. 10Anon. 2011. 'Android/Droid Kung Fu uses AES encryption', Fortinet. Available at: http://blog.fortinet.com/androiddroidkungfu-uses- aes-encryption/

[11]. Levine, B. 2011. 'Researchers find Android security vulnerability', Enterprise Security Today. Available at: http:// www. enterprise -security-today.com/ story. xhtml? story_ id=12200 BVWGTAI

[12]. O'Brien, T., 2011, 'Face niff makes Face book hacking a one tap affair', Engadget. Available at: http://www. engadget.com/ 2011/06/02/face niff- makes-face book-hacking-a-portable-one-tap-affair-vide/

[13]. Cannon, T., 2010, 'Android data stealing vulnerability', thomascannon.net. Available at: http:// thomascannon.net/ blog/2010/11/android-data-stealing-vulnerability/

[14]. Russakovskii, A., 2011. 'Massive security vulnerability In HTC Android devices exposes phone numbers, GPS, SMS, emails addresses, much more'. Available at: http: //www.androidpolice. com/2011/10/01/massive-security-vulnerability-in-htc-android-devices-evo-3d-4g-thunderbolt-others-exposes- phone-numbers-gps-sms-emails-addresses-much-more/#the-vulnerability

[15]. Horn, L., 2010. 'AVG buys Droid Security', PC Mag

[16]. McLaughlin, K. 2011. 'Start up Lookout Mobile Security scores $40 million in VC funding', CRN Magazine. Available at:http://www.crn.com /news/security/231601897/startup-lookout-mobile-security-scores-40-million-in-vc funding.htm ;j session id =OrhamS0WY

[17]. FaLo-ruIxqPyg**.ecappj01

DOI 10.17148/IJARCCE.2015.4544