International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-6 Issue-5, June 2017

Hardening of Android Based Devices & Plugging the Common Vulnerabilities

Manish Kumar Rana, Hemant Narayan

Abstract: ***Technology has developed at a fast pace in last two decades. With the paradigm shift in technology, it has changed the way humans think and simultaneously posed certain challenges to be dealt with in greater depth. While the earlier impetus was on having single window dispensation, however it is being seen that the single window will also not be required and people will have all digital clearence for any service or transaction. With advent of smart devices, the task has become rather simpler, however challenges of personal data safety and related cyber aspects acquires comparatively larger domain to deal with. This paper deals with hardening of ANDROID OS based communication devices by even a novice user. It attempts to throw light on genesis of ANDROID OS, the commonly known vulnerabilities, their threats and strengthening of these devices against hackers of comparable skills. The paper also attempts to touch as to how these ANDROID OS based communication devices, which are potential tools of being soft targets in cyber domain, can be technologically exploited.***

Keywords: ANDROID OS, Technology, vulnerabilities, communication

I. INTRODUCTION

Operating Systems for Smart Devices

A mobile operating system, also called a *mobile OS*, is an operating system that is specifically designed to run on mobile devices such as mobile phones, smart phones, PDAs, tablet computers and other handheld devices. The operating system is responsible for determining the functions and features available on your device, such as thumb wheel, keyboards, WAP, synchronization with applications, email, text messaging and more. The mobile OS will also determine which third-party applications (mobile apps) can be used on your device. While there are many mobile operating systems readily available in the market, some of the popular ones are listed below:

1.1. Android OS (Google Inc.)

The Android mobile operating system is Google's open and free software stack that includes an operating system, middleware and also key applications for use on mobile devices, including smartphones.

1.2. Bada (Samsung Electronics)

Bada is a proprietary Samsung mobile OS that was first launched in 2010. The Samsung Wave was the first smartphone to use this mobile OS.

Manuscript published on 30 June 2017.
***** Correspondence Author (s)
Mr. Manish Kumar Rana, Student, Masters of Technology, CBS Group of Institutions, Maharishi Dayanand University, Rohtak (Haryana), India. E-mail: manishrana@rediffmail.com
Mr. Hemant Narayan, Professor & Head, Department of Electronics and Communication Engineering, CBS Group of Institutions, Maharishi Dayanand University, Rohtak (Haryana), India.

1.3. BlackBerry OS (Research In Motion)

The BlackBerry OS is developed by RIM (*Research in Motion*) as a proprietary mobile operating system for use on BlackBerry smartphones. It is a sophisticated OS with full feature applications and advanced functionality for daily use.

1.4. iPhone OS / iOS (Apple)

iOS is a mobile operating system exclusively developed by Apple Inc for use on its iPhone devices. It is based on Mac OS X operating system which powers many of Apple devices including the iPhone, iPad, iPad 2 and iPod Touch.

1.5. MeeGo OS (Nokia and Intel)

A joint open source mobile operating system which is the result of merging two products based on open source technologies: Maemo (Nokia) and Moblin (Intel).

1.6. Palm OS (Garnet OS)

The Palm OS is a proprietary mobile operating system (PDA operating system) that was originally released in 1996 on the Pilot 1000 handheld. Garnet OS, renamed from ACCESS was extended for support for enhanced multimedia capabilities and wireless connections. ACCESS Linux Platform was launched as successor of Garnet OS.

1.7. Symbian OS (Nokia)

Symbian is a mobile operating system (OS) developed by Symbian Ltd. Ans primarily used by NOKIA targeted at mobile phones that offers a high-level of integration with communication and personal information management (PIM) functionality. Symbian is known to have least consumption of power thereby increasing the usage time of device.

1.8. webOS (Palm/HP)

WebOS was developed by Palm as a mobile operating system that runs on the Linux kernel. Hewlett Packard acquired Palm in 2010 and after the failure of TouchPad, HP made it an open source. Later in 2013, it was purchased by LG.

1.9. Windows Mobile (Windows Phone)

Initially launched as PocketPC 2000 in year 2000, it was renamed as Windows Mobile in year 2003. Windows Phone was announced by Microsoft to succeed Windows Mobile after loosing popularity to rival OSs like Android and iOS.

II. GENESIS OF ANDROID OS

It was Andy Rubin who created Android with other founders with a vision of revolutionizing the mobile industry. Android was initially built with focus on digital cameras. When Google acquired Android in 2005 and since then it was Larry Page, the Google co-founder who fostered it and made it what it is today. **Android Inc.** was founded in Palo Alto, California in October 2003 by Andy Rubin, Rich Miner, Nick Sears, and Chris White. Android was developed keeping in mind to tap digital camera market, however, lately it was realized to divert its efforts toward producing a smartphone operating system that would rival Symbian and Microsoft Windows Mobile since the smartphone market was growing exponentially and the market for digital camera and other devices were loosing their relevence to smartphones.

Android was unveiled in 2007, along with the founding of the Open Handset Alliance – a coalition of hardware, software and telecommunications companies. T-Mobile was the fortunate firm to release first Android phone with release of T-mobile G1 in October 2008. Android has revolutionaized the world digital domain as various real life interfaces are already developed and more are being developed based on Android. Some of them are Android TV for televisions, Android Auto for cars, and Android Wear for wrist watches. Each of these are having a specialized user interface. Further developments are already under progress to acquire domains like Artificial Intelligence, Medical and others.

Android is Moving Beyond Phones and Tablets to Other Areas, Like Wearable Technology. The future of Android is extremely bright. Android seems to be putting an emphasis on wearable technology and other aspects of everyone's life that consumers may not realize could be improved with the addition of a powerful mobile operating system.

While numerous vulnerabilities in Android OS exists, key points are enumerated below:

(i) A Smartphone is just as good as a laptop/desktop in your hand.

(ii) It is always connected to the internet either through Wifi or cellular network.

(iii) Risks of getting infected are doubled.

(iv) A smartphone with a malware can act as a bug.

(v) Multiple services running and permissions escalated to different apps.

(vi) Easy to locate geographically.

(vii) Users do not have administrator level priveledges.

(viii) Difficult to track malicious activity.

While proliferation of smartphones and smart devices is incresing exponentially, it is essential that potential vulnarabilities be addressedbefore hackers make it a bug being assisted by human carrier. These vunarabilities are addressed in succeding paras:

2.1. Turn off location service

Image 1: Location services

Image 2: Screenshot of location service

When location Service is enabled it allows installed applications, which have been given permission to access by default and various visited websites, which have location access enabled, to request user's current location. An application may request data again at any time with no further notification to users if the access has been granted by default. Any service provider can tell user's location through the mobile signal from mobile signaling towers closest to the user. Malware could turn the phone into a bug. With location services enabled, mobile is sending out constant signals of location.

Image 3: SMS and MMS services.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

2.2. Limit no of MMS and SMS saved

It may be well appreciated that physical security of smartphone has also been a major concern, therefore, limiting the number of SMS and MMS messages saved per conversation thread may reduce the likelihood of information disclosure in the event of loss or device compromised. While spoofing of SMS and MMS is less likely, the saved thread of SMS and MMS may contain information of interest.

Android has a massive security bug in a component known as "Stage fright." Just receiving a malicious MMS message could result in your phone being compromised.

2.3. Forget Wifi Networks

Image 4: Wifi Networks.

When a connection is established to connect to wi-fi by providing the password, Android device, by default will remember the password of the wi-fi and automatically rejoin networks that it has previously associated with. In this case if the wi-fi network is unauthenticated then it may likely be spoofed. Further, if previously joined network has a common SSID, such as "test" or "sample", the device may encounter an untrusted instance of a same-named Wi-Fi network and automatically join it thereby broadcasting internet traffic for everybody nearby to see. Malicious individuals may be able to intercept and modify traffic to your computer (by tricking you into connecting to a spoofed WiFi network).

2.4. Disable Network Notifications

Image 5: Smartphone Screenshot for Network Notification.

When a network notification is enabled, Android devices, by default, will present a list of detected wireless networks from an icon in the status bar that users may attempt to connect to however the networks might not have been connected previously r when a wireless hotspot is active, a poorly configured or insecure network can be joined easily which could allow a malicious user on that same network to intercept, capture, and alter any network traffic sent by a user.

2.5. Update the Operating System to Latest Version

An update should take care of all the problems of previous update, in addition to include new things and patch older vulnerabilities and issues. Primary Purpose of OS update is to repair errors, but also to have new features.

Image 6: smartphone screenshot for OS update.

2.6. Do not root the device

One should understand that by rooting device, one can gain complete access to the smartphone. While a user may not be careful all the time, the complete control over the device can be mused which, is turn, increases the responsibility for securing the device and protecting from malicious software.

2.7. Enable device Encryption

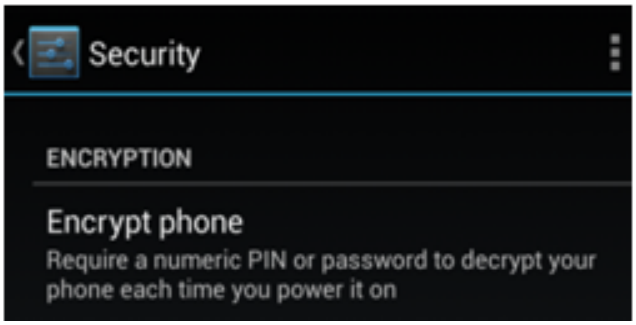

Image 7: screenshot of phone encryption.

It is essential to enable the device encryption. For encryption, Android uses passcode or password of the user to generate an encryption key and the same encryption key is used to encrypt the device.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Therefore whenever the device is powered ON the same passcode/pasword is required every time. This protects the data stored on the device from unauthorized access in the event that it is lost or stolen as physical security of smartphone has also been a major concern.

2.8. Do not install applications from third party sources

Image 8: various app stores.

while installing applications it is essential to check the source of the application. Number of times the source is found to be unauthentic which may lead to installation of the application which may be showing desired actions on the front end however would be performing various operations not supposed to be carried out or stealing data withour permission of the user. Therefore installing application from other sources is riskier since there is no way of knowing how the stores are managed.

2.9. Control App permissions

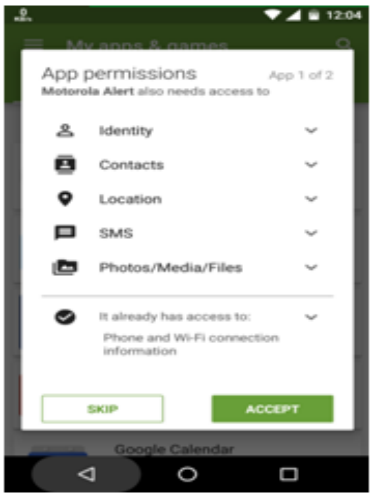

Image 9: App Permission Screenshot.

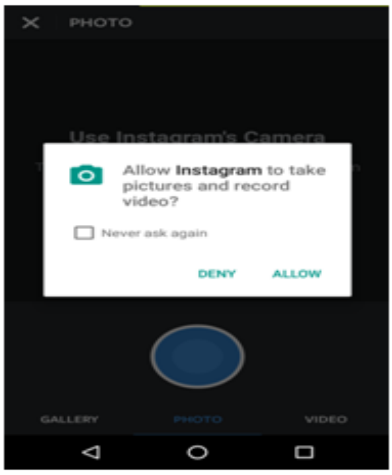

Image 10: permission to a perticular app.

While Android OS upto version 5 does not provide option to control your app permissions, Andriod Version 6 and above have embedded this feature. It is essential to know that all apps whether default or user installed, do not require access to all feature of the phone to function appropriately.

2.10. Disable Developer Options

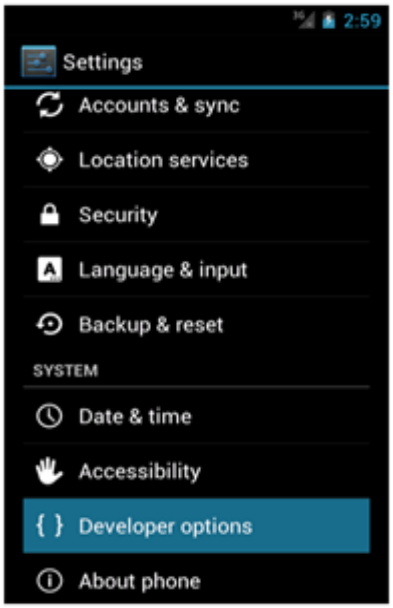

Image 11: Disabling Developer Options.

Developer option, in general understanding, provides a set of tools for developers who create and then need to test and debug a software. In Android, it provide a set os tools to create, test and then debug the android apps. While some of the Android phones have it natively turned on, a common user does not require it to be enabled. When enabled, it is possible to completely control a device through this interface.

2.11. Use Remote Wipe Functionality

Image 12: Feature of Remote Wipe.

with the kind of data generation, Physical security of smartphone has been a major concern. Using remote wipe functionality, when turned ON, it is possible to remotely ring, lock, or erase the device with Android Device Manager, however, having a Google account is must for that. When the remote wipe feature is disabled, these operations are not possible in case of loss or theft of the device.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

2.12. Enable Android Device Manager

Image 13: Android Device Manager.

Enormous data is being generated by each user everyday, which calls for a concern for safety of data from being misused/manipulated. Physical security and mususe of Android device needs to be ensured. Users can track and remotely lock or erase an Android device by using Android Device Manager which is a service provided by Google for Android devices. A Google account is required to use the device manager.

2.13. Set A Pin and Lock The Phone

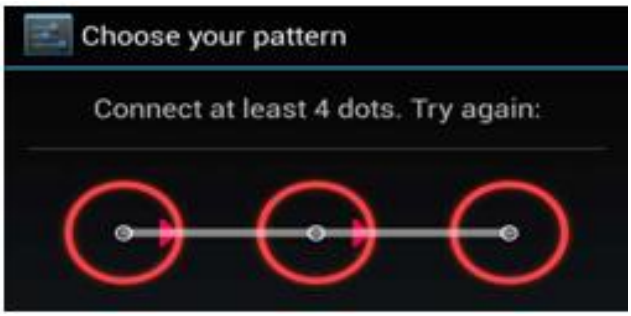

Image 15: Setting up Unlock Pattern.

Casual unauthorized access may lend misuse of Android device or theft of data. Therefore setting a PIN on the device ensures prevention of casual unauthorized access to a device. A PIN (or a password) is considered to be more secure than a pattern as curious and keen observation by people around can decode the pattern of a user patterns and cases have been reported wherein using the fingerprint smudges on devices have been used to derive lock-screen patterns.

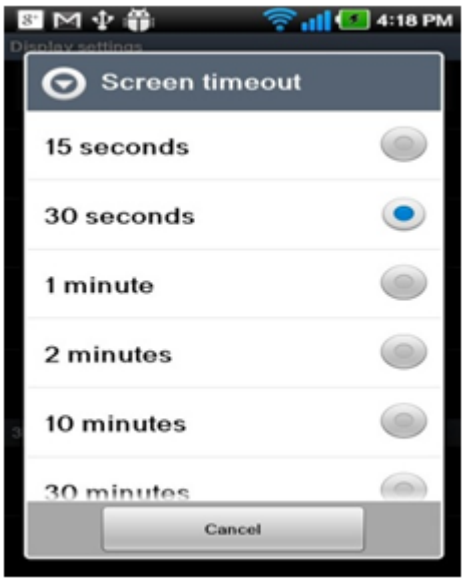

Image 16: Timeout Feature.

2.14. Set Autolock Timeout

when an autolock is disabled, the Android device may assumed as an open box of personal or official data of sensitive nature setting up an autolock time out ensure that the device is automatically locked when the device is inactive for the specified amount of time.

Image 17: Disabling Password Visible.

2.15. Disable Make Passwords Visible

There is no security ensured by using password if make password visible is not disabled as there is no secret in your password which is visible. Disabling this feature increases security by making it harder for people around or have the physical access to your device, to learn your passwords by observation.

2.16. Erase Data Upon Excessive Passcode Failure

Android does not natively provide this functionality, but there are a number of third party applications, some of which were mentioned earlier, which can.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

2.17. Disable Form Auto fill

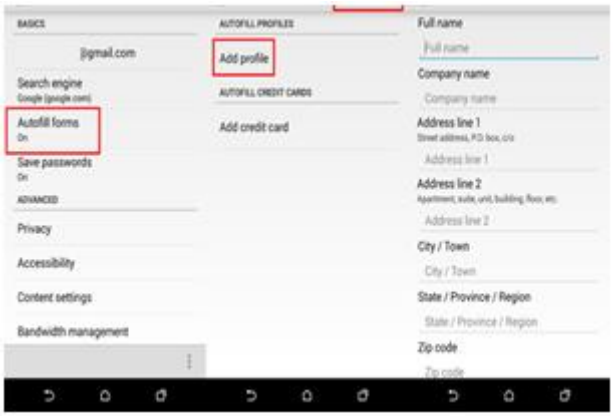

Image 18: Disabling autofill feature.

In order to achieve a little ease to operate the device and internet access, Automatically filling in web forms is used which gives out one's personal information in a public domain and results in the unintentional disclosure of sensitive data to unauthorized people.

2.18. Turn Bluetooth off When Not In Use

Bluetooth should be enabled only when it is actively being used and at all other times it should be disabled.

2.19. Follow Safe Browser Practices

(i) Close the redirected websites and avoid clicking any link on malicious websites to save from cross site scripting and phishing attacks.

Image 19: Malicious Websites.

(ii) Look for https or SSL verification padlock on the address bar while opening any web link.

Image 20: Secure Net Surfing Practices.

III. CONCLUSION

while the information about hardening of Android based devices given in preceding paragraphs covers many common vulnerabilities, it does not make your system entirely safe. It takes a lot many other things to secure it further. perhaps you need to Google for that please.

REFERENCES

1. http://www.useoftechnology.com/ technological-advancements-effects-humanity/
2. https://www.infosec.gov.hk/english/ yourself/vulnerability.html
3. https://blog.lookout.com/stagefright
4. https://www.pcauthority.com.au/ Feature/447215,10-ways-to-harden-the-security-on-your-android-phone.aspx
5. https://www.slideshare.net/anupriti/ android-device-hardening
6. https://www.shoutmeloud.com/top-mobile-os-overview.html

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)