

Bachelor's Thesis (UAS)


Degree Program In Information Technology

Specialization: Internet Technology

2012

Gboyega James Akinbami

**Analysis and Evaluation of the Security
Concerns of VoIP Services on Smart Phones: A
Case Study of the Android-Based Phones.**



BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree Programme In Internet Technology

2012| 47

Instructor(s): Patric Granholm

Analysis and Evaluation of the Security Concerns of VoIP Services on Smart Phones: A Case Study of the Android-Based Phones.

Abstract

One of the major developments in the consumer technology market in recent years has been the explosion in the use of smartphones. The versatile devices have become very popular, with a whole host of functions being conducted on the platform, from social networking to e-commerce and internet banking. As the value of the transactions being conducted on these platforms increases, their attractiveness to cyber criminals has also increased. Amongst the smartphone platforms, the Android operating system looks poised to become one of the most popular platforms. Unique in its open source nature, this thesis examines the security concerns with the use of VoIP applications, a popular class of applications on this platform. Current literature on the security of smartphones, in particular the Android operating system, is examined. This is followed by testing an Android smartphone to determine the ease with which it can be compromised. Detailed analysis of the testing helps to highlight the areas of vulnerability, and what both users and manufacturers should do in order to ward off the threat from attackers. The examination helps to identify the particular vulnerabilities of the Android operating system on smartphones, as well as the threats that can materialise with the use of VoIP applications. The research also develops a set of recommendations for both the users and manufacturers, and identifies further areas of research in this rapidly developing area.

Keywords: VoIP, security, Android, smartphones.



FOREWORD

My profound gratitude goes to Almighty God for giving me wisdom and understanding to complete this work. I would also give thanks to my parents for the support that they provided to help complete my studies. This thesis is dedicated to the loving memory of my late mum.

The list of persons who have helped in one way or another to make this work successful is endless. However, I would give special thanks to my colleague, Mr. Yusuf Ogunjimi, who has taken his time to proofread this work and providing constructive criticism.

Finally, my gratitude goes to my supervisor Mr. Patric Granholm for his support during the course of this work.

2012, Turku.

Gboyega James Akinbami.

1. Introduction.....	1
1.1 ResearchBackground,Aims and obejectives.....	1
1. 2 Thesis Organisation.....	2
2. Literature Review.....	3
2.1 Growth in the use of Smart phones	3
2.2 The Android Operating System.....	5
2.3 Security Analysis of the platform.....	6
2.4 General Threats to Mobile Threats.....	7
2.5 Classifications of Mobile Threats.....	8
2.5.1 Man-in-the browser.....	8
2.5.2 Loss and Theft.....	8
2.5.3 Disposal.....	8
2.5.4 Spam.....	9
2.5.5 Network Connectivity.....	9
2.5.6 Multiple Identities.....	9
2.5.7 Software Vulnerability.....	10
2.6 Security Management.....	10
3. Research Methods And Methodology.....	12
3.1.Research Philosophy and Approach.....	12
3.2 Research Methods and Strategies.....	12
3.3 Test Cases.....	19
4 Findings And Discussion.....	26

4.1 Results.....	26
4.2 Discussion.....	31
5. Conclusions.....	33
5.1 Conclusions	33
5.2 Further Areas For Research.....	34
References	35
 LIST OF FIGURES	
Figure 3.2.1 Installation and preview of Logging Test App version 3.....	14
Figure 3.2.2 Installation of Balloon Game infected with Clounterclank.....	15
Figure 3.2.3 Installation of Fake Madden Nfl 12 infected with Android/Foncy.....	17
Figure 3.2.4 Installation of Fring.....	19
Figure 3.2.5 Installation and preview of Tango.....	22
Figure 3.2.6 Installation and preview of viber.....	23
Figure 4.1.1 HomeScreen Ads Shortcuts and push Notification Ads because of Android CounterClank.....	27
Figure 4.1.2 Executable files created by Android Os/Foncy.....	28
Figure 4.1.3 Executable files recreated automatically by Android/Foncy when deleted.....	29

ACRONYMS, ABBREVIATIONS AND SYMBOLS

3G – third generation standard for digital cellular communication or networks

API – Application Programming Interface

GPS – Global Positioning System

GSM – Global System for Mobile Communications, an international standard for second generation cellular networks

IDC – International Data Corporation

RIM – Research in Motion

SIM – Subscriber Identity Module, typically a chip (card) in a phone

VoIP –Voice over Internet Protocol

1. Introduction

1.1 Research Background, Aims and Objectives

The last few years have witnessed an explosive growth in the use of smartphones. These phones have significant computing power and can be considered to be mobile computing devices. They are able to support a large number of applications and provide users with enhanced functionality. However, the increased variety and value of the transactions conducted on these phones have made them lucrative targets for cyber criminals. Therefore, it has become important and necessary to examine the security of these devices.

The aim of the current research is to evaluate the security of VoIP services on the Android mobile phone platform. The research question can be framed as: How secure are VoIP services on smart phones?

The research objectives are:

To examine the range of security vulnerabilities of the Android platform on smart phones

- To examine the threats to smart phone security
- To evaluate the threat posed to users
- To evaluate the effectiveness of current security measures
- To evaluate the overall security of smart phones, especially on the Android platform

The chart in Chapter 2 shows the growth of the global smartphone market. Side by side with this growth in the use of smartphones is the growth of usage of Android phones, one of the most popular mobile operating systems. This growth of the use of Android phones makes them a very attractive target for attackers who wish to target relatively affluent people with smartphone. The Android operating system is open source software, and it is relatively easy to develop a wide range application on the platform, which is another reason to it. The wide use of these applications presents a vulnerability to the users. VoIP applications are a class of applications that are popular

because they help the user to reduce the cost of calls. In these applications typically the data is routed over the Internet using the mobile Internet rather than the mobile telecommunications network. The significant reduction in cost combined with recent notable improvements in VoIP technology suggest that VoIP is coming of age. More and more VoIP applications are being introduced for the Android and other related smartphone platforms. Users are attracted to the ease of use of these applications as well as the significantly reduced costs for making international calls (Maisto 2010). Combined with the explosion in the use of Android based smartphones, it is suggested that VoIP applications can become a major target for attacks. Hence research into this highly attractive target for attacks is both necessary and timely.

1.2 Thesis Organisation

The entire work is divided into five chapters. This first chapter has attempted to present a picture of the current situation in the market. It has shown how the growth of the smartphones market is being driven by the growth of adoption of Android phones, and explained the importance of VoIP applications on the platform. It has also identified the research aims and objectives. The next chapter, Chapter two, will examine current literature in the subject area. Chapter three will discuss the research methods and methodologies, identifying the test cases that would be used in the current research. Chapter four will present the results of the research and discuss the implications of the research findings. Chapter five concludes the research, presenting the overall research conclusions and identifying further areas for research.

2 Literature Review

2.1 Growth in the Use of Smartphones

In the last two to three years there has been an explosion in the growth of use of smartphones around the world and particularly in the UK. Arthur (Arthur 2011) reports that just under half of the population in the UK now own a smartphone, and furthermore, the sales of smartphones continues to grow very rapidly. The IDC expected that the worldwide smartphone market will grow by almost 50% in 2011 (Essany 2011). Amongst smartphones, Android is becoming one of, if not the most common operating system. This operating system developed by Google now powers half of all smartphones sold in the UK. Android is followed by RIM's Blackberry with 22.5% of the market and Apple's iPhone at 18.5%. A large number of smartphones today use the Android operating system. Amongst them are the HTC Desire HD, Sony Ericsson Xperia Ray, HTC Sensation, Samsung Galaxy SII, etc. The phenomenal growth in the use of Android phones is shown in Fig. 2.1 below.

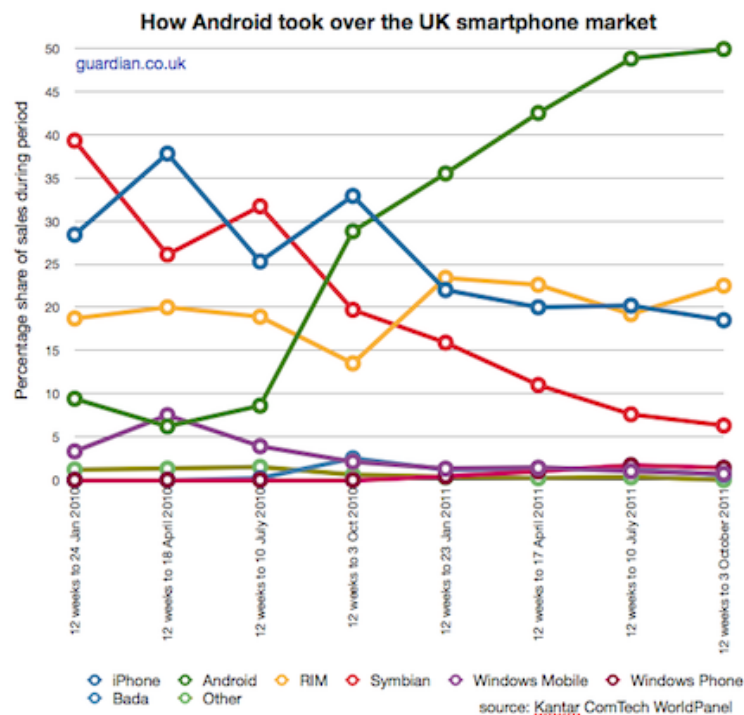


Figure 2.1. Growth in the use of the Android smartphones in the UK (Source: Arthur, 2011a)

In fact, comScore (2012) suggests that Android-based phones are the second most popular phones in the EU, next only to Symbian phones (Nokia), which is in fact experiencing a decline. Table 2.1. below shows the most popular smartphone platforms used in France, Germany, Italy, Spain and the UK (EU5). From this table it can be seen that Google's Android is the fastest growing smartphone platform across EU5.

Table 2.1 Top Smartphone Platforms in EU by Share of Phone Users (Source: comScore, 2011)

Top Smartphone Platforms in EU5 by Share of Smartphone Users*
 3 Month Average Ending July 2011 vs. July 2010
 Total EU5 (DE, FR, IT, ES and UK) Mobile Subscribers, Age 13+

	Share (%) of EU5 Smartphone Users		
	Jul-10	Jul-11	Point Change
Total Smartphone Users	100.00%	100.0%	0.0
Symbian	53.9%	37.8%	-16.1
Google	6.0%	22.3%	16.2
Apple	19.0%	20.3%	1.2
RIM	8.0%	9.4%	1.5
Microsoft	11.5%	6.7%	-4.8

In fact, such is the growth of the Android platform that comScore (ibid) suggest that the growth of smartphones is actually driven by the growth of adoption of Android

phones. One of the key features of the Android operating system is that it is an open source system. This means that the source code of the operating system is available to anyone. This availability makes it easier for developers to create new applications. In fact, it is suggested that Android phones have become popular because unlike many other phones, they are relatively easy to manipulate. This makes it easy for developers to develop a large number of applications and users to install a wide variety of applications (Android Phones UK 2012).

2.2 The Android Operating System

The Android operating system is essentially a free open source operating systems for mobile phones. This operating system therefore allows for the creation of mobile applications. Meier (Meier 2010) explains that the Android system also comes with a number of peripherals such as:

- i. A hardware reference design that describes the capabilities required for a mobile device to support the software stack
- ii. A Linux operating system that is optimised for mobile devices and allows for low level interface with the hardware
- iii. A host of open source libraries for application development
- iv. A run time used to execute and host Android applications, including the Dalvik virtual machine
- v. An application and user interface framework
- vi. Core applications
- vii. A software development kit

The application execution environment is sandboxed, and the only way the applications can interact with the phone is through the application programming interfaces (APIs). The applications are written in Java and run in the Dalvik virtual machine.

2.3 Security Analysis of the Platform

Shabtai et al. (Shabtai 2009) assess the various security aspects of the Android framework and identify a number of security vulnerabilities. Firstly, they explain that the platform is susceptible to all the problems associated with the Linux kernel. The Linux kernel itself is not a completely secure piece of software, as evidenced by the number of CVEs (Common Vulnerabilities and Exposures) entries logged. Within the kernel, the drivers and vendor specific additions are more vulnerable, because these run with the highest privileges. Shabtai et al. suggest that in order to minimise vulnerable code being submitted, there needs to be more robust checks on the code submitted to the kernel.

In terms of the Android platform, Google has added some extensions to the kernel in order to extend existing functionality. This has also added to the vulnerability of the platform. Commercial literature has covered the particular areas of vulnerabilities of the Android operating system in detail. For example, Diaconescu (Diaconescu 2012) points out that on the Android operating system, zero permission does not actually mean zero permission. He explains that when a zero permission application was created in order to determine the data that would be available for harvesting in such an application, it was found that the application was able to access the data in the privileged SD card access area. Unless the operating system protected each and every file, the application would be able to open the folder. Secondly, it was also found that the zero permission application was also able to determine the different applications that were installed on the device at the time of testing. The problem that arose was that the application would be able to determine the exact applications installed on the device, and in turn use the applications with weak permission vulnerabilities to harvest data or perform other malicious functions. Finally, he reports that any application can access key information about the device itself, such as the GSM and SIM vendor IDs. This information that is collected without permission can also be sent anywhere even if the application does not have Internet permissions. Diaconescu (ibid) also points out that it is widely accepted that Google Play, the market for Android applications is also a major source of viruses.

In addition to the vulnerabilities inherent in the Android platform, the modifications made by manufacturers of other phones can also introduce vulnerabilities to the operating system, as highlighted by Mello (Mello 2011). He highlights a case to point in

the HTC Android phones which have a major flaw in that they allow any application that has Internet access to also have access to a significant amount of sensitive information such as email addresses, GPS locations, phone numbers, system logs (which track what the individual applications do, including logging into secure locations) and text message data. This flaw was traced to the modifications made to the Android operating system by HTC, the phone manufacturer itself.

2.4 General Threats to Mobile Devices

Mobile devices are characteristically devices that are portable, personal and can be carried with ease from a place to another. The growth of interconnectivity of array of mobile devices as well as continuous mobile threats has made mobile device usability more challenging. Mobile devices such as Notebooks, smartphones, Tablets, Media Players and other portable devices are often deployed as integral components of mechanical, electronic and electrical systems. Connectivity to the Internet by these devices can either be wired or wireless (Muttik 2011). Many mobile platforms have their proprietary resource communities where guidelines about hardware, operating system updates and processes, and external resources such as applications can be accessed.

Threats are communicated intents to inflict harm or loss to a person, and then Mobile Threats are all communicated attempts to inflict harm or loss to a Mobile Ecosystem through mobile devices or physical means (Mitchell 2012). Cyber-crimes aimed at mobile devices usually do occur for different reasons ranging from hardware theft, information theft to denial of service. There are many facets to mobile device attacks which make it difficult to draw a line between criminality and terrorism. It is important to know that Mobile threats exist because there are some forms of human and system inefficiencies in design and decision making process. It is also important to know that Cyber-crime against Mobile devices cannot be completely eradicated but it can be greatly reduced after a while with concerted efforts and dissemination of proper knowledge about the tricks of the infiltrators. Sometimes the cost of production and prospects to have more applications on the Appstore make Mobile platform Vendors compromise security requirements.

2.5 Classifications of Mobile Threats

Mitchel (Mitche, I2012) generally classifies Mobile Threats into two broad categories but the author of this thesis added another category: Physical threats. This thesis hereby presents the general classifications of Mobile Threats: Communication-based, System-based and Physical means. All forms of Mobile Threats can be definitely classified into one of these threats families. Communication-based threats are network-oriented and include access network impersonation, mobile device impersonation, Man-in-the-middle attacks e.t.c, System-based attacks exploit the inefficiencies of the Operating system core and include all software vulnerabilities, side channel and social engineering attacks (including malicious applications) while physical attacks are hardware theft.

2.5.1 Man-in-the-browser

This kind of mobile crime is committed when malicious software steal or modify financial information from a browser during an online banking session. Sometimes these Trojans can completely hide malicious transactions from the user. On major mobile platforms, this mobile threat becomes impossible unless the Operating system itself is compromised and the malware runs as root.

2.5.2 Loss and Theft

The form factors in which various mobile devices are designed makes it easy target for theft. Also, the tendency of losing or misplacing these devices is very high as a result of the small sizes in which they come. In view of this, a lost or stolen mobile device can be compromised if it does not have adequate security measures activated, thereby sensitive data can be accessed or exposed to the public. Apart from unwanted data access, a mobile device owner can incur huge financial loss if unauthorized phone calls are made from a compromised device by unauthorized persons.

2.5.3 Disposal

There are risks inherently present when mobile devices are not properly disposed. The disposed device may continue to hold sensitive information and this information may end up in the wrong hands which may lead to serious security breach or privacy invasion. Resetting a device manually does not guarantee a total erasure of information on the phone. This act may physically remove the intended information but logically the erased information may still be present until it is overwritten by a new data. These days, there are software and hardware products that can be used to recover erased data from mobile devices in the market and this could be used otherwise if found in the possession of a Cyber Crime criminal.

2.5.4 Spam

Unsubscribed materials can be received by mobile devices users because of the operating system vulnerabilities and weak access network and security policies or protocols which make mobile devices share certain personal data (ITSEAG 2009). In addition to the annoyance of receiving undesirable and unsolicited materials, unsuspecting users can erroneously accept unintended charges on their communication services as a result of spam messages. In addition, spam messages are sometimes used as a tool for carrying out denial-of- service attack and introduction of malware targeted at mobile devices.

2.5.5 Network Connectivity

The majority of threats to mobile devices come from connectivity. Common threats like Man-in-the-middle attacks: stealing of data from an application interface or form due to neglect of software security measure during implementation, interception of backup data over a network, and persistent connection of pair-wise technologies such as Bluetooth and Infrared are perpetrated through the connectivity of mobile devices, even those exploited on the vulnerability of software still largely rely on the network connection for its optimal goal.

2.5.6 Multiple Identities

Many so called mobile devices that are supposed to be personal are not really personal as they are being shared by family members, friends and colleagues. This sharing feature increases the vulnerability of such mobile devices to theft and important information.

2.5.7 Software Vulnerability

Software vulnerability arise from lapses that are system based and such vulnerabilities may be found first with the core of the OS of the Mobile platform or with the user application because of the bridge in specified security requirements.

Some Mobile threats are exploited on the OS vulnerability. Designers of a Mobile OS might not have envisaged some certain security threats as at the time of release, which might make the platform very vulnerable. Mobile Threats thrive on the lapses in the OS architectural design which makes the Mobile device easily maneuverable. It is like a multiplier effect; once the OS core is corrupt, every application on the mobile device is made to act in tandem with the malicious software. The stability of a Mobile Ecosystem determines how well secured a mobile device is and the system security should not be compromised.

Mobile device vendors also tend to allow some quick and dirty solutions to be deployed which are usually inadequate. They do this because of the pressing needs to have a large base of applications to the users' taste. System Security and application base are trade-offs, which a Mobile platform vendor must strive to strike a balance in order to keep reputation, marketplace and satisfy its user community. Some applications on the Application store are easily attackable and carry some malware which can populate themselves on the resident mobile device, other connected device(s) and the Application store (Marketplace).

2.6 Security Management

Security management is usually a tedious exercise and costly if threats are allowed uncensored. The possible pain and losses incurred from Mobile threats might be unimaginable, so one needs to explore all possible measures to stop the Cyber criminals. Here are some tips for securing a user application in order to make it less vulnerable.

1. Eliminating unnecessary functionality (reducing the attack surface) can solve many problems
2. Following good software engineering practices can minimize the risk of buffer overflow vulnerabilities.
3. Use of robust crypto and sound security protocols that are widely available and standardized would safeguard the application.

In conclusion, the fight against Mobile threats must be collective. End users of Mobile devices must be security conscious and should suggest possible ways of tracking cyber criminals, because users seem to be more conversant with some of the tricks. The system designers and application developers must also uphold specified security requirements and keep thinking like cyber criminals too, because only someone with a criminal mind for good purpose can checkmate the actual cyber criminals.

3 Research Methods and Methodology

3.1 Research Methods and Strategies

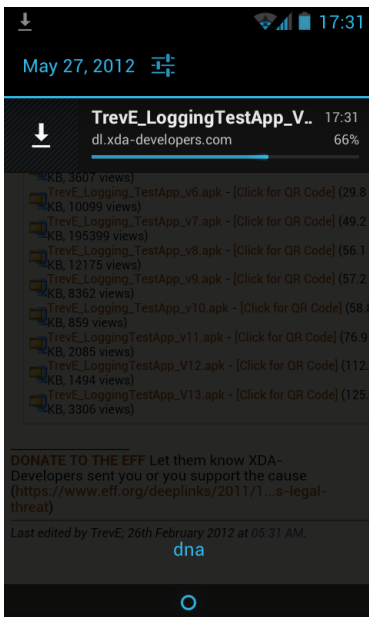
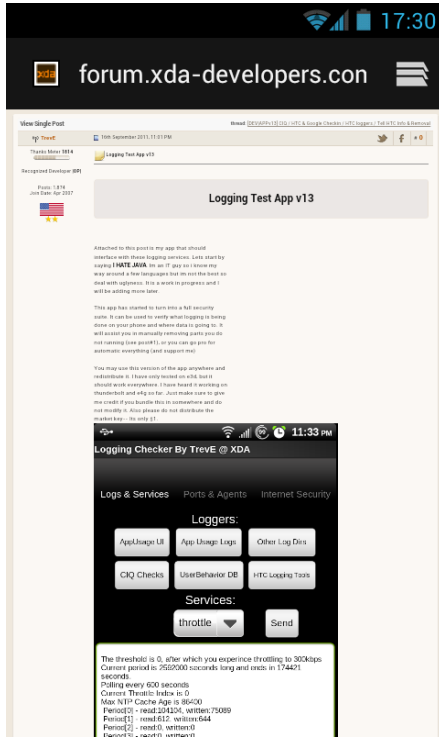
The research effort will examine secondary data from multiple sources and collate the results. These results will be analysed and the result will be given by a combination of induction and deduction. The Android platform is used as a case study for in depth study.

3.2 Test Cases

All the test cases were carried out in Google's Nexus S android smartphone with latest Android 4.0.4 (Ice cream sandwich)-based operating system.

For most comprehensive security testing Logging Test App version 13 will be used. Logging Test App was first developed when Trevor Eckhart, an IT enthusiastic came to know about Carrier IQ and the amount of information it collects. Carrier IQ is a California-based company which is supposed to provide diagnostic analysis to wireless industry from the data collected through smartphones. Carrier IQ was accused of collecting personal data from smartphones for example, logging SMS, key strokes and location data. So in the beginning Logging Test App was used to check whether a smartphone has been logged by Carrier IQ or not. Later on the developer expanded the functionality of the application to make it a powerful security testing application.

Logging Test App version 13 can be downloaded from the XDA Developers forum, after downloading it into the smartphone using the default browser; users have to enable "Unknown Sources" under security settings to install the application. After successfully installing the application, it should be given root (Super User) rights to gain access to all the logs file.



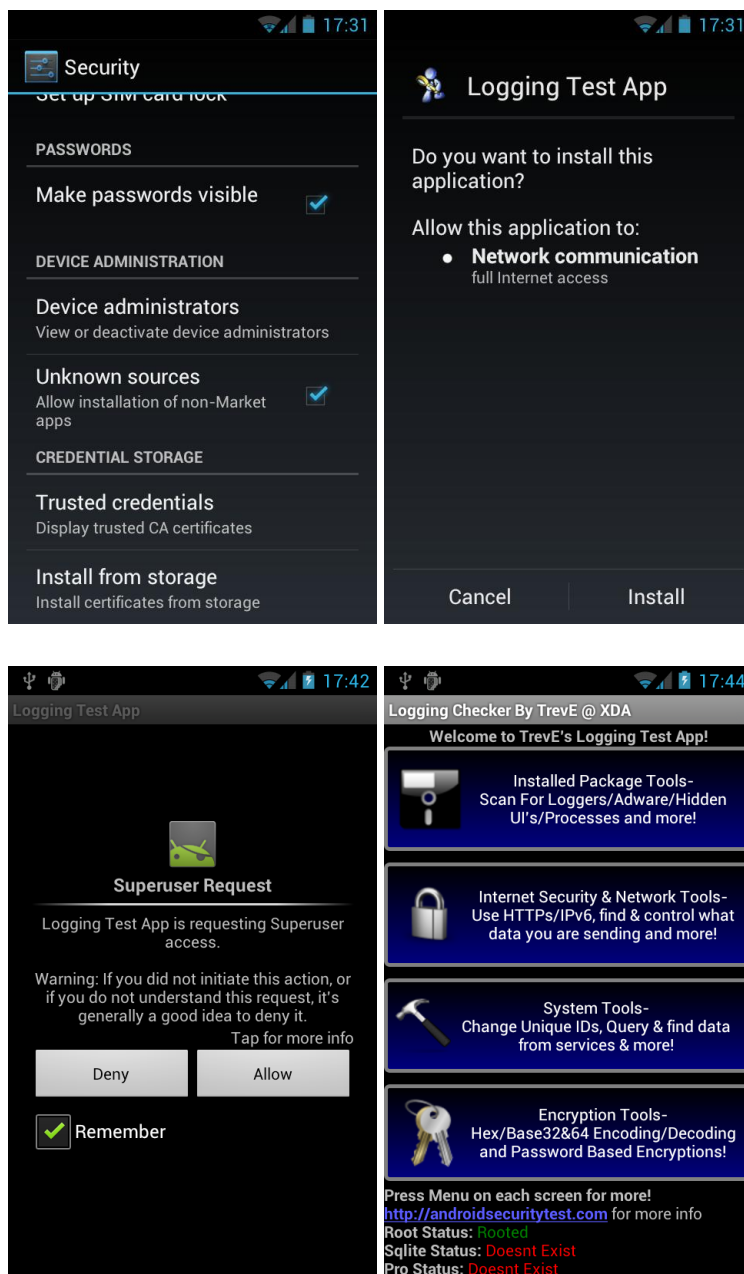


Figure 3.2.1. Installation and Preview of Logging Test App version 13

Logging Test App consists of 4 main tools among which only two of them are required for this test. “Installed Package Tools” to scan loggers, adwares and hidden processes and “Internet Security & Network Tools” for scanning cookies and other data which are sent from the device to the Internet.

For further research and details ADB (Android Debugging Bridge) was used. It is a comprehensive tool to manage and debug android device via PC. ADB comes with Android Software Development Kit package. After downloading the Android Software

Development Kit and installing it in the PC, ADB can be found under “platform-tools” folder which is inside the “android-sdk” folder. While installing the Android SDK, it also installs the entire required driver for a device to be controlled via ADB.

Test Case 1: Malware No. 1 (Android CounterClank Trojanhorse)

For Test Case 1, Android CounterClank Trojanhorse was installed on the Android phone. Since all affected application has been removed from Google Play Store, the affected application (in our case Balloon Game, from com.christmasgame.balloon) was installed manually. After downloading it and copying the file from the PC to device’s memory, the application was installed.

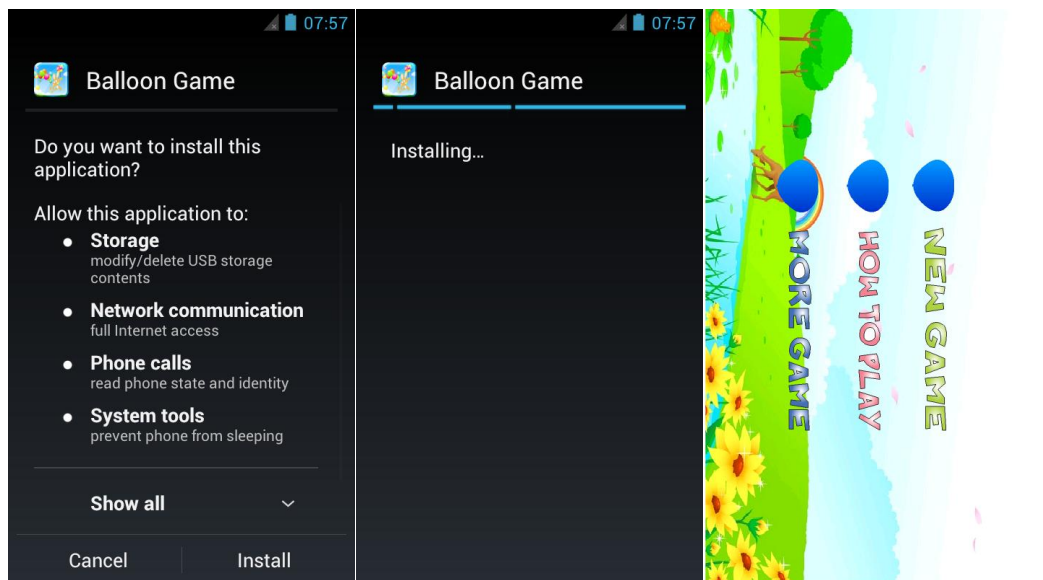


Figure 3.2.2. Installation of Balloon Game infected with ClounterClank

The application’s permission was carefully observed and has been listed below:

- Storage: modify/delete USB Storage

The application can read and write on USB storages and SD cards.

- Network communication: full internet access, view network state

The application can create network connection and check network status.

- Phone calls: read phone state and identity

They can be used to detect whether device is being used for calling or not, access to the information like phone number and device id.

- System tools: prevent phone from sleeping, install shortcuts, read Home settings and shortcuts, uninstall shortcuts

They can prevent the device from being idle (sleep), install or uninstall shortcuts in home screen and The application can read home screen settings.

The application was also observed under Logging Test App for further details. Being one of the widespread malware for android smartphones, detailed information about this malware was easily available, including information on how this application exploits notifications feature and home screen shortcut for advertisement purposes. All the key aspects about this malware were noted as posted in the Internet and similar tests were done using ADB.

Test Case 2: Malware Application 2 (AndroidOS/Foncy)

All the known Trojans are removed from the Google Play Store; therefore they should be installed in the device manually, similarly to the process of Test Case 1. This time also the AndroidOS/Foncy, an SMS Trojan, application was downloaded to a PC and copied to memory of the phone. After that, it was installed. The affected application that was used during this test is called Madden NFL 12 (Fake SuiConFo, com.android.bot). The differences between the malware in first test case and this malware will be observed.

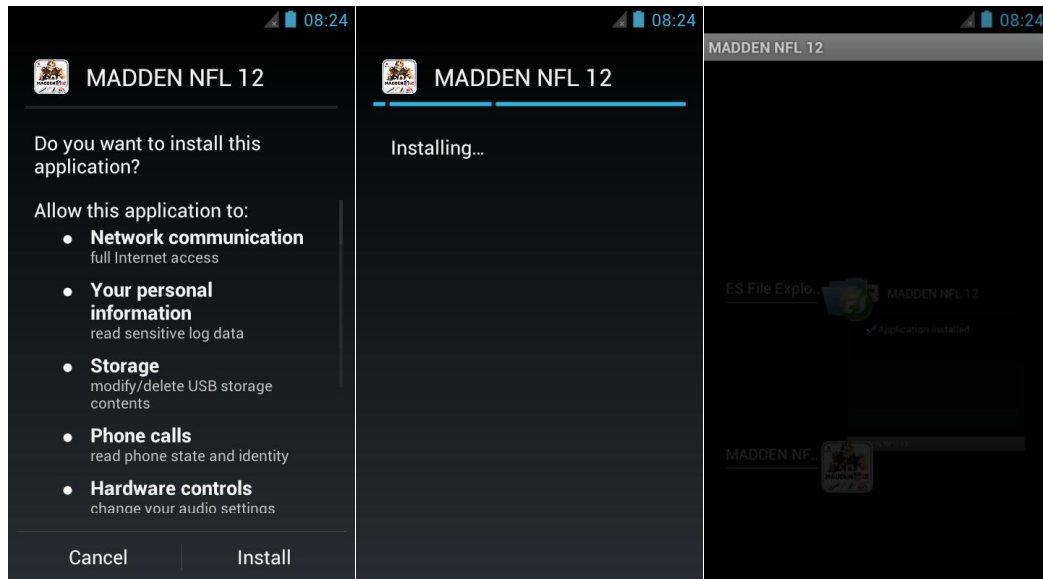


Figure 3.2.3. Installation of Fake Madden NFL 12 infected with AndroidOS/Foncy

These are the permissions required for this application:

- **Network communication:** full internet access, Google Play license check, view network state, view Wi-Fi state

It can create of network connection, check network and wifi status and also create new Bluetooth connection. Also users can check if they have purchased the application from Google Play store or not.

- **Personal information:** read sensitive log data

It can read different system logs which have general usage information of the device including personal and private data.

- **Storage:** modify/delete USB storage contents

It can read and write on USB storages and SD cards.

- **Hardware controls:** changer audio settings, control vibrator

It can change the vibrations, volume levels and other general audio settings.

- **Phone calls:** read phone state and identity

It can detect whether the device is being used for calling or not, access to the information like phone number and device id.

- **System tools:** change network connectivity, change Wi-Fi state, prevent phone from sleeping

They can connect to different wifi access point and change the configuration, change the network connectivity and prevent the device from being idle (sleep).

The application was also scanned via Logging Test App for other information. After that ADB was used to test the presence of any other malware files. As mentioned in several blogs and security research using ADB (adb shell), the following locations were checked:

- /data/data/com.android.bot/files/footer01.png
- /data/data/com.android.bot/files/header01.png
- /data/data/com.android.bot/files/border01.png

A test was done deleting these files to see whether the malware will create them again or not.

Test Case 3: Genuine Application 1 (Fring)

Fring is one of the highly used applications for communication between different platforms of smartphones. As from the description on Google Play Store, it is called “The Ultimate Video Chat App”. It allows users to have group video chat with other smartphone users around the world in real-time. One can install Fring very easily in the Google Play Market.

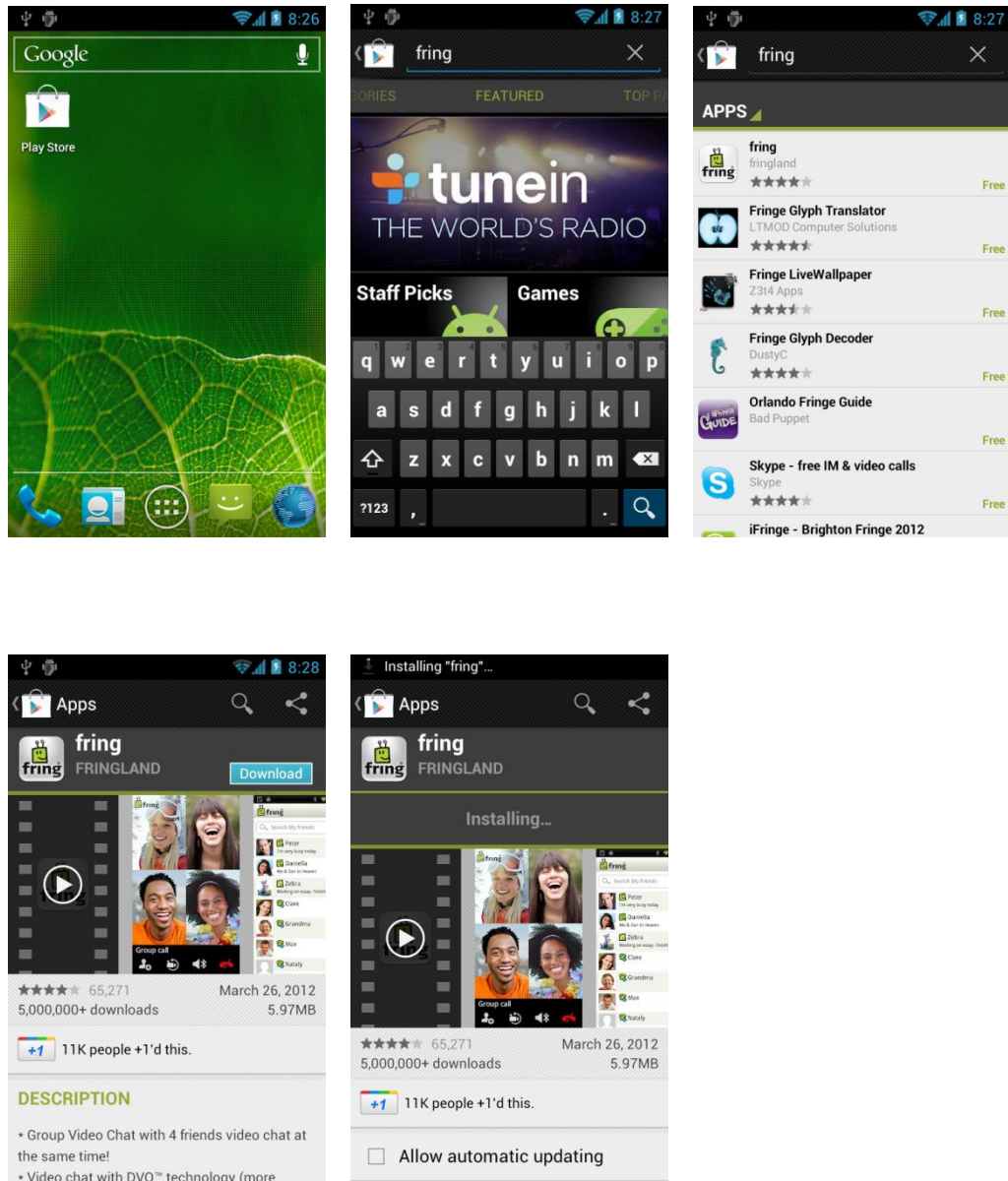


Figure 3.2.4. Installation of Fring

The list of the permissions of Fring from the android play store is mentioned below:

- Services that cost users money: send SMS messages, directly call phone numbers

They can call and send SMS to different phone numbers without a user interaction and confirmation.

- Hardware controls: change audio settings, record audio, take pictures and videos, control vibrator

They can change the vibrations, volume levels and other general audio settings, access to recorded audio files, take and collect images through camera without any user knowing it.

- Your messages: read SMS or MMS, receive SMS

Apart from sending SMS automatically, it can read all the old and new SMS stored in your device.

- Network communication: full Internet access, create Bluetooth connections, view network state, view Wi-Fi state

It can create of network connection, check network and wifi status and also create new Bluetooth connection.

- Your personal information: read contact data, read sensitive log data

It can read all the contacts and address information stored in the device. Also, the application can read different system logs which have general usage information including lots of personal and private data.

- Phone calls: read phone state and identity

They can detect whether device is being used for calling or not, access to the information like phone number and device id.

- Storage: modify/delete USB storage contents modify/delete SD card contents

It can read and write on USB storages and SD cards.

- System tools: change Wi-Fi state, prevent tablet from sleeping prevent phone from sleeping, disable keylock, retrieve running apps, modify global system settings, automatically start at boot

They can connect to different wifi access point and change the configuration, prevent the device from being idle (both sleep and keylock), access information about all the other running application in the system, access and modify the system settings and also start automatically when the device is booted.Fring was scanned with Logging

Test App and then also its privacy policy was also taken consideration for further research.

Test Case 4: Genuine Application 2 (Tango)

“Tango” is also another communication application similar to Fring. It can be installed from Google Play store like Fring. All the test cases were conducted with similar communication applications to make the report fairer. Description from the store says that Tango is only application that lets a user send free video messages, video calls and phone calls. Since Tango is available in multiple platforms, it is one of the highly used communication applications. Currently Tango is operating in nearly 190 countries with tens of millions of users, security concerns in this kind of applications is very important.

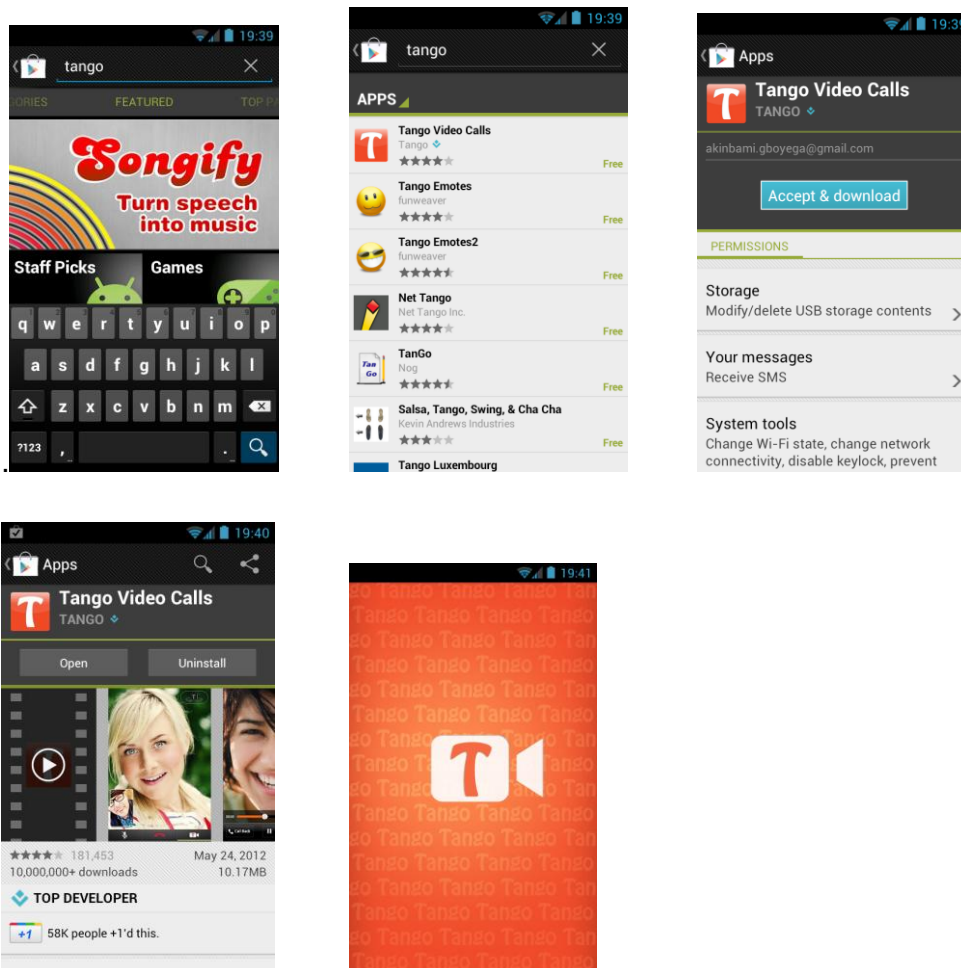


Figure: 3.2.5 Installation and preview of Tango

Here is the list of permissions that Tango allows

- Your accounts: manage the accounts list, act as an account authenticator, discover known accounts

This can manage and modify accounts, use account authenticator of “AccountManager” to create accounts, get and set the password.

- Hardware controls: record audio, take pictures and videos, change your audio settings, control vibrator

They can change the vibrations, volume levels and other general audio settings, access to recorded audio files, take and collect images through camera without any user knowing it.

- Your messages: receive SMS

It can retrieve the messages and use them.

- Network communication: full Internet access, create Bluetooth connections, view Wi-Fi state, view network state, receive data from Internet

It can create of network connection, receive data from the application server, check network and wifi status and also create new Bluetooth connection.

- Your personal information: read sensitive log data, read contact data, write contact data

It can read and modify all the contacts and address information stored in your device. Also, the application can read different system logs which have general usage information including lots of personal and private data.

- Phone calls: intercept outgoing calls, read phone state and identity

They can detect whether device is being used for calling or not, access to the information like phone number and device id. They also can modify the dialled number for outgoing call and manipulate them.

- Storage: modify/delete USB storage contents modify/delete SD card contents

It can read and write on USB storages and SD cards.

- System tools: prevent tablet from sleeping prevent phone from sleeping, disable keylock, change Wi-Fi state, change network connectivity, write sync settings, automatically start at boot, read sync settings

They can prevent the device from being idle (both sleep and keylock), read the sync setting of the device and also start automatically when the device is booted.

- Default: Market billing service

It can let the users make app purchase within this application.

Tango was scanned with Logging Test App and also similar to Fring, its privacy policy was also taken into consideration. There was no past research into its security issue.

Test Case 5: Genuine Application 3 (Viber)

Alike the two previous test cases, “Viber” is also another communication tool for smartphones. It is also available in multiple platforms and offers services like text messages and free calls to other Viber users globally. Viber have stated that currently there are nearly 40 million Viber users around the world. It is being used more than both of our test cases around the world across different platforms.

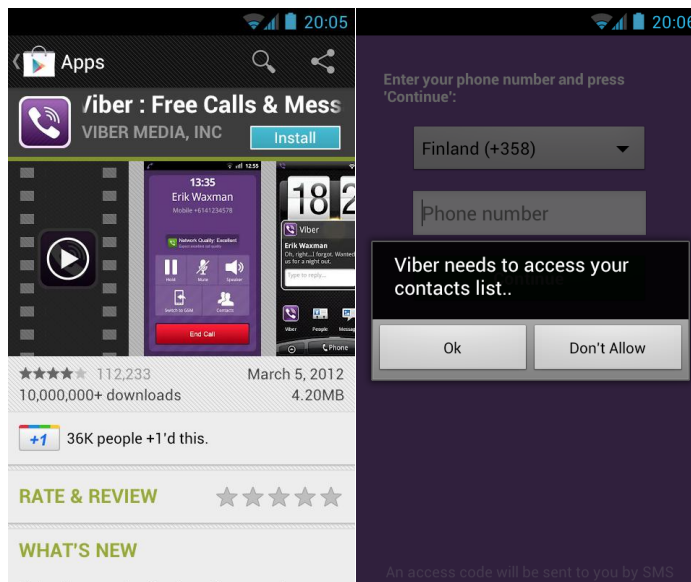


Figure 3.2.6. Installation and preview of Viber
The permissions that Viber needs are:

- Your accounts: act as an account authenticator, manage the accounts list, discover known accounts

This can manage and modify accounts, use account authenticator of “AccountManager” to create accounts, get and set the password.

- Services that cost money: directly call phone numbers, sending SMS messages

They can call and send SMS to different phone numbers without a user interaction and confirmation.

- Hardware controls: change audio settings, record audio, take pictures and videos, control vibrator

They can change the vibrations, volume levels and other general audio settings, access to recorded audio files, take and collect images through camera without any user knowing it.

- Your location: fine (GPS) location, coarse (network-based) location

It can access the exact or coarse location of the user either using GPS or connection.

- Your messages: receive SMS

They can retrieve the messages and use them.

- Network communication: full Internet access, create Bluetooth connections, receive data from Internet, view network state

It can create of network connection, receive data from the application server, check network status and also create new Bluetooth connection.

- Your personal information: read contact data, write contact data, read sensitive log data

It can read and modify all the contacts and address information stored in the device. Also the application can read different system logs which have general usage information including lots of personal and private data.

- Phone calls: read phone state and identity, modify phone state

They can detect whether device is being used for calling or not, access to the information like phone number and device id. It also can modify the dialled number for outgoing call and manipulate them. Also, they can modify phone networks without user noticing.

- Storage: modify/delete USB storage contents modify/delete SD card contents

It can read and write on USB storages and SD cards.

- System tools: prevent tablet from sleeping prevent phone from sleeping, Bluetooth administration, disable keylock, change network connectivity, modify global system settings, retrieve running apps, write sync settings, kill background processes, set wallpaper, read sync settings, read sync statistics, send sticky broadcast

They can prevent the device from being idle (both sleep and keylock), read and modify the sync settings of the device, administrate the Bluetooth of the device, change

network state, access information about all the other running application in the system , kill background processes, set system's wallpaper and send sticky broadcasts.

Default: directly call any phone numbers, disable or modify status bar, power tablet on or off power phone on or off

It can call any numbers (including emergency) without user knowing it, automatically turn on and off the device, add or remove system icons and also can disable the status bar.

This application was also scanned via Logging Test Application; also its privacy policy was researched carefully for any security loop hole.

4 Findings and Discussion

4.1 Results

The findings from the secondary data are presented with a discussion of the implications of the findings. It is expected that the research will be able to present a snapshot of the state of security of smart phones, particularly on the Android platform. The findings from the case study are subsequently generalised and compared with other platforms in order to arrive at the overall research findings.

Before any other applications were installed, Logging Test App showed few logs and loggers which already exist in the device.

- /data/anr/: A directory where all the Application Not Responding data with details about it are saved.
- /data/tombstones/: A directory used to save system dump when an app crashes in Linux system.
- /data/system/throttle/: A directory that has files about the logs of 3G usage created by services.jar
- /data/system/dropbox/: A directory for the log of all the session details from when the phone started to when it ended.
- /data/system/usagestats/: A folder containing logs of application usage
- Market Feedback Agent: Known logging agent, Android application store's feedback agent.

As mentioned above, in a normal device there is presence of all application crash logs and statistics, application usage statistics and other general session information which are vulnerable to attacks. This information can be accessed with a normal application with specific permissions which could lead to serious security issues.

Test case 1:

Android CounterClank Trojanhorse appeared to be more of an adware than malware itself. However, it compromises the device id and saves the user information like IP address in remote server. Basically, it can be called as aggressive adware because it installs third party “Mobclix” adware logger for advertising and pushes advertisement in the notification bar and installs different advertisement shortcuts in home screen. By reading some security blogs, it was known that this malware also sends user IMEI (International Mobile Equipment Identity) information to its server for identifying the unique user. Because of constant “push notification”, making numerous shortcuts in home screen and also making different bookmarks of advertisements in browser, some consider this as malware while others just an aggressive adware.

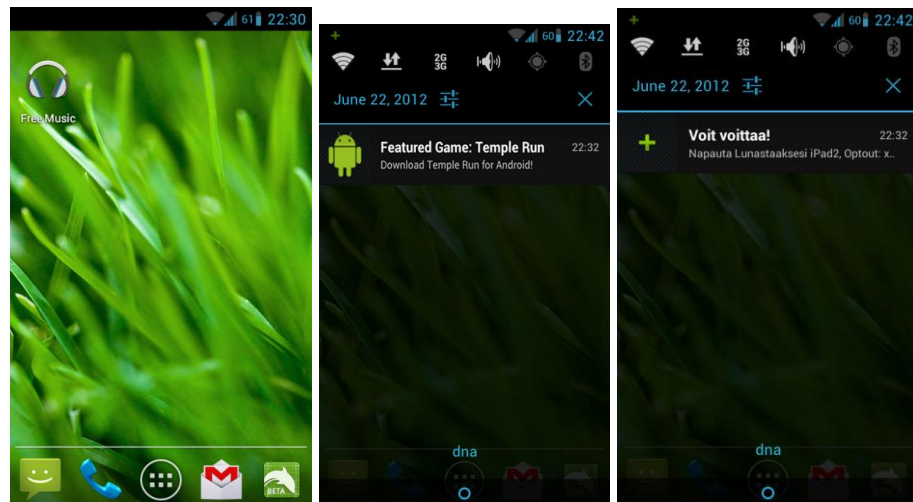


Figure 4.1.1. Homescreen Ads Shortcuts and Push Notification Ads because of Android CounterClank

All the functions that this application did were listed under the permission list. It was clearly stated that it will read device id and number, will install home screen shortcuts and also have permission to read home screen settings. But since it was using them aggressively and annoying the user with lots of advertisements, it can be considered as aggressive adware acting as malware.

Test case 2:

AndroidOS/Foncy did not show anything on Logging Test App but it was running in the background as the name com.android.bot. It appeared to be copying three executable files in main system.

- /data/data/com.android.bot/files/footer01.png
- /data/data/com.android.bot/files/header01.png
- /data/data/com.android.bot/files/border01.png

```
C:\>adb shell
root@android:/ # cd data/data/com.android.bot/files
cd data/data/com.android.bot/files
root@android:/data/data/com.android.bot/files # ls
ls
border01.png
footer01.png
header01.png
root@android:/data/data/com.android.bot/files #
```

Figure: 4.1.2 Executable files created by AndroidOS/Foncy

Among these three files, two of them (footer01 and header01) could enable a remote user to gain root access, send personal information to remote servers, compromise the device and run different commands on it, while the third one(border01) was responsible for sending SMS to different international numbers.

```

C:\>adb shell
root@android:/ # cd data/data/com.android.bot/files
cd data/data/com.android.bot/files
root@android:/data/data/com.android.bot/files # ls
ls
border01.png
footer01.png
header01.png
root@android:/data/data/com.android.bot/files # rm border01.png
rm border01.png
root@android:/data/data/com.android.bot/files # ls
ls
border01.png
footer01.png
header01.png
root@android:/data/data/com.android.bot/files # ls
ls
border01.png
footer01.png
header01.png
root@android:/data/data/com.android.bot/files # rm border01.png
rm border01.png
root@android:/data/data/com.android.bot/files # rm border01.png
rm border01.png
rm failed for border01.png, No such file or directory
255!root@android:/data/data/com.android.bot/files # ls
ls
footer01.png
header01.png
root@android:/data/data/com.android.bot/files # ls
ls
border01.png
footer01.png
header01.png
root@android:/data/data/com.android.bot/files # █

```

Figure 4.1.3. Executable files recreated automatically by AndroidOS/Foncy when deleted

The test fake application had the same name as the real genuine application (which costs), which led many users to download the application and get their devices infected. The entire permission list included and shown while installing the application was just a clone of real application, it did not have anything to do with the malware itself. The malware was just gaining the access to the device with a security hole and using those three files mentioned above to cause all the attacks.

Test Case 3

Fring is a verified application and is easily available from Google Play market. Among its entire permissions list, almost all of these permission are an issue of privacy and security for users. As we can see from the permissions list, Fring can read the device identity, contact details, read sensitive log data, read and sendSMS, directly call phone numbers. Also from Fring's privacy policy it has been stated that Fring does not share personal data like contact details but since they are using third party for advertising, it is stated that Fring might save

cookies, web beacons and similar technologies for better advertisement. Since Fring uses Google's third party advertisement system, Logging Test App showed it on the list of Google Adwares. One noticeable detail while opening Fring for first time was that it asked a permission to read contacts. Its privacy policy was also detailed in mentioning that Fring do not sell any personal information to any third party.

Another noticeable detail was that Fring is a genuine application but taking reference to its permission lists if it was not then verified as genuine application below are some of the risks to a user, it may:

- Cost a user money by sending messages without the user's confirmation.
- Monitor a user' messages or delete them without showing them to the user.
- Cause unexpected calls on the user's phone bill.
- Read your confidential messages.
- Use internet connection to send the user's data to other people.
- Use personal or private information.
- Discover private information about other apps.
- Corrupt system configuration.

Test Case 4:

Tango asked for permission to read the contacts as Fring did. But what was different in Tango was that it synced the contacts between the server and the device. Also, in its privacy policy, Tango failed to mention about not selling or renting or providing those information to any third parties alike Fring's privacy policy where it was specified, which indirectly might mean that in some cases Tango may sell those information. Since Tango does not have any third party ads services neither does it do some suspicious logging so it did not appear anywhere in Logging Test App, but Tango have stated themselves that Tango will collect data like calls, numbers of calls made by members, call durations, usage by geographies, device and connection information, IP address, device

capability, bandwidth, statistics on page views, network type from the device for better performance.

Similarly to Fring, we will have to consider the risk of Tango too, if it was not a verified application and taking consideration the permissions lists, it may:

- Cost the user money by sending messages without the user's confirmation.
- Monitor user messages or delete them without showing them to the user.
- Cause unexpected calls on the user's phone bill.
- Read confidential messages.
- Use internet connection to send the user's data to other people.
- Cause excess data usage.
- Use personal or private information.
- Use this to erase or modify the user's contact data.
- Discover private information about other apps.
- Corrupt system configuration.

Test Case 5:

After installing Viber, the functionality was much similar to Tango and Fring combined, but in a sense that it also synced contacts with server and device similarly to Tango. Viber's privacy policy stated that it will not sell or rent or share any personal information stored in Viber servers. However, Viber have mentioned that they will record the IP addresses of the users for different demographics. One notable statement in case of Viber is about call detail record which means Viber records call time, call quality, destination and number of calls for quality assurance. For all of those activities the permission was granted from the users, that is why it also did not appear in Logging Test App.

Some of the risks that users have to consider having Viber in the system and giving all the permission required by Viber, it may:

- Cost the user money by sending messages without the user's confirmation.

- Monitor user messages or delete them without showing them to the user.
- Cause unexpected calls on the user's phone bill, also to emergency services.
- Use this to determine where the user is, and may consume additional battery power
- Cause excess data usage.
- Use internet connection to send user data to other people.
- Use personal or private information.
- Use this to erase or modify user contact data.
- Discover private information about other apps.
- Corrupt system configuration.

4.2 Discussion

It is clear that all applications have some risks in them but the difference is whether the application is genuine or not. Being a genuine application, it always gives users a chance to complain to someone or for someone to look into in the case of attacks. In case of application infected with different malwares a user will not even notice anything, not even the theft of their personal and private data.

Between two malware: Android CounterClank which is not much of a threat to users, and AndroidOS/Foncy which poses a significant threat in every possible way, it gives access to remote users to access the device, it compromises all the personal data. It also sends different SMS around the world to different numbers creating costs to user without asking for the permission of the user.

In the case of the genuine application test cases, the conditions were much different. The application data, and clarifications regarding what permissions are required and their significances are definite and well specified. By going through the privacy policy of respective application it was also clear what they will do with the store private information like personal call log, call recordings, text messages, contact addresses and other device settings.

5 Conclusions

5.1 Conclusions

The use of smartphones is expanding at a phenomenal rate. The Android platform is one of the most popular platforms for the new breed of smart phones. This makes it a prime target for developments in the area of smart phone security. The current research is important because it will help identify the potential and most likely areas of vulnerability, assess the current and likely future level of threats against smart phones, and give users guidance on the issue. It will also help to raise awareness as to the areas which industry efforts have to be concentrated on in order to improve the security of the platform.

By this research it is confirmed that no matter what there is always threat to users' personal data if either the device is full of infected application or full of genuine application. The only difference is that if the personal data is compromised because of malwares, then it is the user who is to be blamed, otherwise it is those application development firms which were storing the data. In this technologically advanced world once the data is out, there is nothing one can do to erase it forever and user's private information will be public.

We are assured by the research that the malware infestation can cause a lot of data usage, calls and SMS messages to different unknown phone numbers which results in huge phone bills which cannot be a least of concern. Losing money and private information at the same time is an important issue for a general user. At this growth rate of smartphone usage and at the same time numbers of malware in the market, it is certain that nobody is secure enough. Users do not have that much of a choice, they have to use smartphone and its applications, and with the increment of infected application and new malwarem there is no company that can actually prove and satisfy their customer in this sector.

Although we can see a lot of mobile antivirus in the market, they can only disinfect a device from the infection that has been detected already but not the one that is being developed. Since android applications are really easy to build and it does not take that much time for a developer to build an application that can violate some security hole that is discovered. Until the infection is massive and is clearly researched by a security expert, no one sees an antivirus that can disinfect the infection.

In the end it all depends on user what to save in their beloved smartphone and study what application are they installing in their system. Also a user cannot assure the security of an applications' server, so it depends on the user whether to believe what a website says or not. It is better to know for sure what one is doing before complaining about it to other institutions.

5.2 Further Areas for Research

This research is a really a very minuscule part of whole security research on smartphones as it only consisted android smartphone and very few test applications. To obtain a clear idea about security issues on android, research needs to be conducted on large scale with different and huge amount of application in different version of androids, as they have different security issue within them. Using old antiviruses and using new malwares, testing them will give a whole new perspective

Apart from that we can carry out similar tests in different platform not just only android. There are other platforms like Apple's iPhone, Symbian, Windows Phone 7 and Blackberry's RIM which have significant market shares. Only after all this research has been carried out, can one get a gist about how vulnerable users are in this technological world and what are the measures they can take to prevent themselves for these kinds of infection and data leakage.

REFERENCES

Android Phone UK, 2012. Available at: <http://androidphone.org.uk/guides/what-is-an-android-phone/> [Accessed Mar 20, 2012]

Arthur, C. 2011a. Half of UK population owns a smartphone. the Guardian. Available at: <http://www.guardian.co.uk/technology/2011/oct/31/half-uk-population-owns-smartphone> [Accessed March 20, 2012].

Arthur, C, 2011b. How Android swallowed the UK smartphone market in 18 months. The Guardian. Available at: <http://www.guardian.co.uk/technology/2011/oct/31/android-uk-smartphone-growth> [Accessed March 20, 2012].

Android CounterClank Research Blogs <http://www.appriya.com/blog/android-security.php/google-android-market-is-infected> , <http://blog.mylookout.com/blog/2012/01/27/lookout%E2%80%99s-take-on-the-%E2%80%98apperhand%E2%80%99-sdk-aka-android-counterclank/> , <http://nakedsecurity.sophos.com/2012/02/02/android-counterclank-is-not-malware/> [Accessed on May 27, 2012]

Android Foncy Research Blog <http://stratsec.blogspot.com/2012/01/butterfly-effect-of-boundary-check.html> [Accessed on May 27, 2012]

Android Debugging Bridge, <http://developer.android.com/guide/developing/tools/adb.html> [Accessed on June 1, 2012]

Android Software Development Kit, <http://developer.android.com/sdk/index.html> [Accessed on June 1, 2012]

Barrera, DGunes Kayacik, H, van Oorschot, P.C and Somyaji, 2010. A methodology for empirical analysis of permission-based security models and its application to android. In *Proceedings of the 17th ACM conference on Computer and communications security NY, USA*. October 04 - 08, 2010. pp. 73–84.

Bickford, J. O'Hare, R, Baliga, A, Ganapathy, V and Iftode, 2010. Rootkits on smart phones: attacks, implications and opportunities. In *Proceedings of the Eleventh*

Workshop on Mobile Computing Systems & Applications. NY, USA. February 22 - 23, 2010. pp. 49–54.

Chang, Y.F., Chen, C. & Zhou, H., 2009. Smart phone for mobile commerce. *Computer Standards & Interfaces*, 31(4), pp.740–747.

comScore, 2012.

[http://www.comscore.com/Press Events/Press Releases/2011/9/Android Captures number 2 Ranking Among Smartphone Platforms in EU5](http://www.comscore.com/Press%20Events/Press%20Releases/2011/9/Android%20Captures%20Number%20Ranking%20Among%20Smartphone%20Platforms%20in%20EU5) [Accessed Mar 20, 2012]

Diaconescu, A., 2012. For android apps, ‘zero permissions’ does not actually mean zero permissions. Available online at <http://www.androidauthority.com/android-apps-zero-permissions-75001/> [Accessed Apr 14, 2012]

Download Links for Malwares <http://contagiominedump.blogspot.com/2012/01/android-counterclank.html> [Accessed on May 27, 2012] ,
<http://contagiominedump.blogspot.com/2011/12/fake-suiconfoapk-foncy-android-trojan.html> [Accessed May 27, 2012]

Enck, W. D, McDaniel, P. and Chaudhuri, S., 2011. A study of android application security. Available online at http://static.usenix.org/event/sec11/tech/full_papers/Enck.pdf [Accessed Oct 18, 2012]

Enck, W., Gilbert, P., Chun, B.G, Cox, L.P, Jung, J., McDaniel, P. and Sheth, A.N. 2010. TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones. In *Proceedings of the 9th USENIX conference on Operating systems design and implementation*. Vancouver, Canada. October 4–6, 2010. pp. 1–6.

Essany, M., 2011. IDC Estimates 50% Growth in Worldwide Smartphone Market in 2011. Available online at <http://www.mobilemarketingwatch.com/idc-estimates-50-growth-in-worldwide-smartphone-market-in-2011-14227/> [Accessed Mar 20, 2012]

Fring on Google Play Store, <https://play.google.com/store/apps/details?id=com.fring> [Accessed on May 27, 2012]

IT Security Expert Advisory Group (ITSEAG), 2009: Mobile Device Security information for CIOs/ CSOs, Trusted Information Sharing Network (TISN), <http://www.tisn.gov.au/Documents/Mobile+Device++CIO+Paper++Web+Version.pdf>, p. 3

Landman, M., 2010. Managing smart phone security risks. In *2010 Information Security Curriculum Development Conference*. October 01 - 03, 2010. pp. 145–155.

Logging Test App main download forum, XDA Developers, <http://forum.xda-developers.com/showpost.php?p=17612559> [Accessed May 27, 2012]

Maisto, M., 2010. Android Smartphones Get VOIP Apps from Fring, CounterPath - VOIP and Telephony - News & Reviews. eWeek.com. Available at: <http://www.eweek.com/c/a/VOIP-and-Telephony/Android-Smartphones-Get-VOIP-Apps-from-Fring-CounterPath-595477/> [Accessed March 20, 2012].

Meier, R., 2010. Professional Android 2 Application Development, London: Wiley and Sons.

Mobile Malware Mini Dump, <http://contagiominidump.blogspot.com> [Accessed on May 27, 2012]

Mulliner, C. & Miller, C., 2009. Injecting SMS messages into smart phones for security analysis. In *Proceedings of the 3rd USENIX Conference on Offensive Technologies*. Berkeley, CA, USA, August 10–14, 2009. pp. 5 – 5

Muttik, I, 2011. Securing Mobile Devices: Present and Future, McAfee Labs, <http://www.mcafee.com/us/resources/reports/rp-securing-mobile-devices.pdf>, p. 12.

Mitchell, C, 2012. Cyber Crime Threats on Mobile Devices, <http://www.chrismitchell.net/Papers/tcctom.pdf>, p. 2.

Ongtang, M., Mclaughlin, S, Enck, W. and Mcdaniel, P., 2009. Semantically rich application-centric security in android. In *Computer Security Applications Conference, 2009. ACSAC'09. Annual*. pp. 340–349.

Portokalidis, G , Homburg, P., Anagnostakis, K., Bos, H., 2010. Paranoid Android: versatile protection for smartphones. In *Proceedings of the 26th Annual Computer Security Applications Conference*. Amsterdam, The Netherlands. December 5–9, 2010. pp. 347–356.

Privacy policy of Fring, <http://info.fring.com/privacy/> [Accessed on May 27, 2012]

Privacy policy of Tango, <http://www.tango.me/privacy-policy/> [Accessed on May 27, 2012]

Privacy policy of Viber, <http://viber.com/privacypolicy.html> [Accessed on May 27, 2012]

Schmidt, A.D, Schmidt, H.G., Clausen, J., Yuksel, K.A., Kiraz, O., Camtepe, A. and - Albayrak, S., 2008. Available online at http://xml.csie.ntnu.edu.tw/JSPWiki/attach/Lance/android_security.pdf [Accessed 18 Oct., 2012]

Schmidt, A.D., Peters, F., Lamour, F., Scheel, C., Camtepe, S.A. and Albayrak, S., 2009. Monitoring smartphones for anomaly detection. *Mobile Networks and Applications*, 14(1), pp.92–106.

Schmidt, A.D., Schmidt, H.G., Batyuk, L., Clausen, J.H., Camtepe, S.A., Albayrak, S. and Yildizli, C., 2009. Smartphone malware evolution revisited: Android next target? In *4th International Conference on Malicious and Unwanted Software (MALWARE)*, 13-14 October, 2009. pp. 1–7.

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y. and Dolev, S., 2009. Google Android: A state-of-the-art review of security mechanisms. Arxiv preprint arXiv:0912.5101.

Shabtai, A. Fledel, Y., Kanonov, U., Elovici, Y., Dolev, S. and Glezer, C., 2010. Google Android: A comprehensive security assessment. *Security & Privacy, IEEE*, 8(2), pp.35–44.

Tango Video Calls,

<https://play.google.com/store/apps/details?id=com.sgiggle.production> [Accessed on May 27th 2012]

Threats <http://dictionary.reference.com/browse/threat> [Accessed on 1st July,2012]

Viber on Google Play Store,

<https://play.google.com/store/apps/details?id=com.viber.voip> [Accessed on May 27, 2012]

Zhou, Y., Zhang, X., Jiang, X., and Freeh, V.W., 2011. Taming information-stealing smartphone applications (on Android). *Trust and Trustworthy Computing*, pp.93–107