International Journal of Engineering & Technology, 7 (2.7) (2018) 1030-1033

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Intercepting the malevolent sms in android devices

A. Lashya Pravallika [1] *, B. Bhargavi [1], Ch. Harshit [1], Dr. K. V. D. Kiran [2]

[1] IV/IV B. Tech CSE Students Professor4 Department of Computer Science & Engineering, K L E F Deemed to be University, Vaddeswaram, Guntur Dt, Andhra Pradesh, India

[2] Department of Computer Science & Engineering, Professor4 Department of Computer Science & Engineering, K L E F Deemed to be University, Vaddeswaram, Guntur Dt, Andhra Pradesh, India

**Corresponding author E-mail: lashyapravallika@gmail.com*

Abstract

Currently, In the mobile operating system Android is trending in the whole world.Though the designers of Android are working much on the security there are few attacks on the messaging framework which are really dangerous. In this paper we also present these attacks. Our focus is on SMS, USSD, and the evolution of their associated security in Android and accordingly the development of related attacks,Also we discuss here the main features and vulnerabilities of Android OS that allow the development and infection by SMS malware.If the SMS is considered as the normal, then it does not take any action and it send to the end user after the delay expires. To deal with this type of issues,we proposed a method where the end user behaviour can be adjusted to prevent the totally malicious SMS.

Keywords: *Malicious; SMS; Android Devices; Framework.*

1. Introduction

The most popular mobile device for all the users is Android operating system. Smart phones have become an essential part of our lives along with their excessive capability.In this paper mainly discuss about the vulnerabilities of the operating system of Android device that allows the development and the infection of the SMS malware.According to the F-Secure address most of the appeared threats were protected with the help of antivirus for the mobile devices is F-Secure. With the help of F-secure we can verify the Android malware where it is used to perform the SMS sending methods and it is also called as SMS based attacks. We discuss here about some attacks SMS malware propagation,SMS spam,SMS privacy attack, Short Message Service (SMS) flooding attack and also the premium rate fraud of the SMS. In addition, we will present a new attack on unstructured supplementary service data (USSD) transfer.Most operators are built on USSD is used to perform many operations such as recharging,credit transfer,balance checking and also having the so many operations. For this reason, USSD represents a high value target to the hackers in order to reap great benefits similar to the ones seen in SMS attacks. The Android applications are used API's to admittance for some resources like telephone, Short Message Service (SMS) and another system functions. By using the API's can be protected by using the security mechanisms these are called as permissions. The main aim of the paper is used to find out the inequality among the Android device state and the end user behaviour.The majorimprovements of this paper are as follows:

- By using mobile devices we can find out the arrival state of the end user.
- We must recognize the main arrivals by defining the state of the Android device.
- Here we introduce an algorithm which is used to detect that any differences among the Android device state and the end user while processing the Short Message Service transfer operations. Therefore these types of algorithm are used to avoid the happening of the first SMS threat.
- If SMS match is identified, then the end user has to make sure out that the Short Message Service (SMS) do not arrivefrom the second Short Message Service (SMS) threat. For that, we postponed the SMS transfer operations and the end uses job is inform to engage in case the SMS is malicious.
- We examine the resilience of Android next to attacks and calculate its recognition efficiency.
- We introduce the modification policy for the end user behavior in charge to avoid totally spiteful SMS operations.

2. Literature review

Here we discover various vulnerabilities in executions of SMS which are utilized by a significant number of the trademark telephones in the market that has comparable working framework. It was demonstrated how the vulnerabilities could separate the telephone from organize framework, prematurely end calls, impact and reboot. Now and again because of DoS before the affirmation is sent, the system believes that the message did not get conveyed and continues retransmitting the message. Moreover, he showed how an endorser personality module (SIM) data download (an administration apparatus utilized by administrators to remotely oversee SIM cards), through which SMS is straightforwardly sent to SIM (or USIM, the SIM card utilized as a part of third era or 3G systems), can be controlled so the assaulted telephone will send SMS from the telephone to any number the assailant determines, a procedure through which clients' units/credits can be depleted gradually. Additionally this component helps in completing a DoS assault on specific portable number. It was exhibited that SMS can be vindictive and destructive to the system. Numerous portable administrators are giving Internet-based SMS benefit utilizing which clients can send messages specifically to versatile associat-

Copyright © 2018 A. Lashya Pravallika et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ed arrange from a web. This administration, if abused, can prompt DoS assaults, and along these lines keeping versatile clients from making telephone brings in a focused on city. Mulliner and Miller displayed a general structure that can be utilized particularly with advanced mobile phones for testing and checking of SMS messages. Albeit numerous cell phones were researched to, our greatest advantage is the Android-basedones.

3. Existing system

In this paper the principle existing approach will be identified as an Short Message Service (SMS) malware on the Android device and that would be categorized according to the basis of two analysis: Static analysis and Dynamic analysis. In this static examination approach the application static data which are taken out from the binary code or the basis, which issued to verify that the function may contain malicious code or not. In the dynamic examination approach application behaviour is examined through its implementation process to identify on the off chance that there are any irregularities with the ordinary conduct. The trouble by this approach is that the estimation cost and the likelihood of dodging the discovery. In past sort of methodologies called approach authorization, the conduct of an honest to goodness work should take after the specific imagine rules. In the event that a control infringement is discovered, the capacity is considered as pernicious.The approach execute progresses are characterized into preventive and adjusting. The adjusting methodology couldn't keep the assault however fundamentally recognize it, as the administer in disrespected must be seen after the assault has been done. Then again, the preventive approach can be utilized to keep the event of the assault.

3.1. Attack model

A SMS strike is said with make productive if those malignant SMS could attempt insane of the device. We consider two sorts for SMS assaults:

3.1.1. First strike demonstrate

Those malicious arrangement conceals its SMS-sending practices beginning with the client, Also just sends malignant SMSs.

3.1.2. Second strike demonstrate

Those client presents an exchanged off SMS function, i.e., SMS-sending hones need support not to conceal information from the customer, yet the request in like way cryptically sends noxious SMSs. This sort of hazard happens when an assailant repackages a real game plan and moreover installs malignant code under it.

3.2. User behaviour

We consider that those customer direct with reverence to those adaptable device will be shapedby two main features.

3.2.1. End user accessibility

This trademark require two modes: available and unavailability. Those customer is said should be available with the respect of mobile device if he/she is near the device. i.e., the customer might be not faraway from the mobile device and can listen the sounds generate by it. Expecting that those end user is faraway from those mobile device then it is considered as unavailability.

3.2.2. End user activity

With the help of end user when it is interacting with the mobile device it performs the actions like: reading data,and touching the screen.

Android plays out the accompanying advances every time the SMS application calls one of the three SMS-sending strategies said above:

1) Stop the beheading of the application.
2) Suspect if lead is satisfied.
3) Square running the application if the rule is disregarded,Or else, the SMS-sending is postponed for T time units.

In the Table 1 it demonstrates the diverse guidelines is to apply each time a SMS-sending rules is asked. Android needs to check that if there is any mismathces between the clients conduct and the gadget state.If the typical gadget is consisitent with the any sort of end user,which is utilized to send the SMSs through with the assistance of a SMS applications.it comprises of the accompanying:
Screen State: The screen need be on.
Device Lock State: The gadget should be opened.
Function visibility: Application should keep running in the fore front.
Function status: Application should have a place with the Known SMS applications.

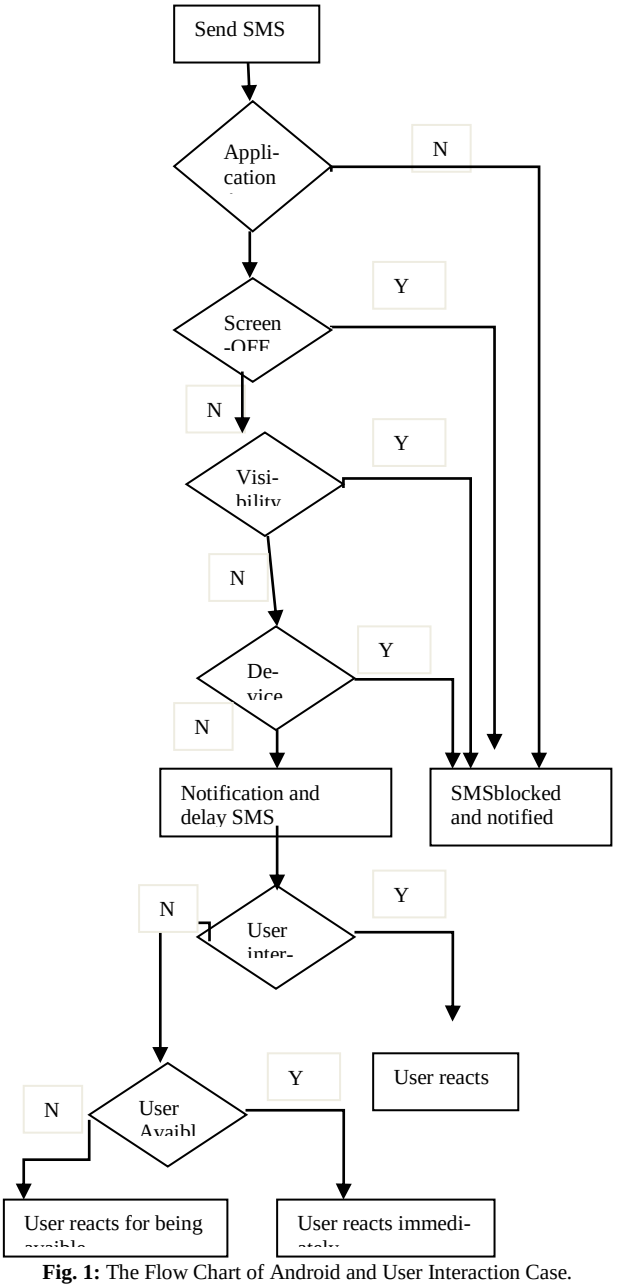


Fig. 1: The Flow Chart of Android and User Interaction Case.

Where apply the balance equations.We denoted by PON, PN, and POFF the constant state probability that the end user is at states ON Active, ON Inactive N, and OFF respectively. We have:
b PON = c POFF

a PN = b PON
c POFF = a PN
PON + PN + POFF =1
With the help of the above equations,we can solve:

PN = (c/a) / (2+(b/a))

PON = c /b(2 +(b/a))

POFF = 1/(2+(b/a))

We caluculate the detection ability of Android supporting the following three types of end user availability schemes:

1) The familiar layover times in PON and POFF states are equal(i. e., b = c)
2) The familiar layover times in PON state is greater than that in state POFF (i. e., b < c).
3) The familiar layover times in PON state is less than that in state

POFF (i. e., b > c).

Table 1: SMS Sending Methods of Android

Cases	Screen State	Function Visibility	Device Lock State	Authorized	Action State
Case 1	OFF	Backdrop	Cloosed	Y/N	Block
Case 2	OFF	Backdrop	Opened	Y/N	Block
Case 3	OFF	Fore part	Closed	Y/N	Block
Case 4	OFF	Fore part	Opened	Y/N	Block
Case 5	OFF	Backdrop	Locked	Y/N	Block
Case 6	OFF	Backdrop	Unclocked	Y/N	Block
Case 7	OFF	Fore part	Locked	Y/N	Block

Table 2: Observation Scale (0.5 <=A<=0.9)

a	b=c			b=1		c=1	
	1	0.1	0.01	c=0.1	c=0.01	b=0.1	b=0.01
0.5	0.2	0.971	0.9996	0.714	0.961	0.92	0.992
0.6	0.35	0.979	0.9997	0.791	0.973	0.93	0.993
0.7	0.47	0.987	0.9998	0.847	0.980	0.94	0.994
0.8	0.55	0.989	0.9998	0.875	0.984	0.95	0.995

Table 3: Observation Scale (1 <=a<=9)

a	b=c			b=1		c=1	
	1	0.1	0.01	c=0.1	c=0.01	b=0.1	b=0.01
1	0.66	0.9991	0.99990	0.916	0.990	0.966	0.996
2	0.87	0.997	0.99997	0.9777	0.997	0.987	0.998
3	0.93	0.998	0.99998	0.989	0.998	0.993	0.99993
4	0.95	0.999	0.99993	0.994	0.993	0.995	0.9995

Table 4: Observation Scale (10 <=a<=100)

a	b=c			b=1		c=1	
	1	0.1	0.01	c=0.1	c=0.01	b=0.1	b=0.01
10	0.99	0.9999	0.99999	0.990	0.9999	0.999	0.9999
20	0.99	0.9999	0.99999	0.999	0.9999	0.999	0.9999
30	0.99	0.9999	0.99999	0.999	0.9999	0.999	0.9999
40	0.99	0.9999	0.99999	0.999	0.9999	0.999	0.9999
50	0.99	0.9999	0.99999	0.999	0.9999	0.999	0.9999
60	0.99	0.9999	0.99999	0.999	0.9999	0.999	0.9999
70	0.99	0.9999	0.99999	0.999	0.9999	0.999	0.9999
80	0.99	0.9999	0.99999	0.999	0.9999	0.999	0.9999
90	0.99	0.9999	0.99999	0.999	0.9999	0.999	0.9999
100	0.99	0.9999	0.99999	0.999	0.9999	0.999	0.9999

4. Proposed system

In addition to the existing system we proposed an algorithm to prevent malicious SMS in android devices.Android delivered the brand new SMS premium-price policy within the Android 4.2.2, and, on the time of scripting this work, as few as 4.0% of used gadgets have this model of the OS. hence, the sizable majority of users are still at risk of SMS-primarily based attacks. And, as turned into verified, the few using the 4.2.2 are nonetheless at some chance based totally on those records, we advise an intrusion detection system99(IDS) with a purpose to discover malicious apps. Our IDS is rarity-based totally and works as a software (on the app degree) without any excessive lisence, which does it appropriate for those kind of OS model and tool. The IDS contains specifically of 4 additives: a statistics collector, an occasion collector, an app profiler, and a detector. considering that our IDS is anomaly-based totally, a studying segment is required whereby apps are monitored to be able to study their related behaviors.This behavior is quantitative and the collected values are used inside the detection section. under is a description of every element accompanied by using the set of rules description.

4.1. The observation algorithm

The essential intension of the Observation calculation is to utilize the heaped up information at some phase in the acing stage so as to unearth if the pernicious SMS progressed toward becoming despatched. The arrangement of standards opportune tests SMS that is being sent from cushion like clockwork. The intension of the review is reality that the cradle continually holds a follow that a SMS was sent. particularly two exact tickets are continually blessing: RILJ identified with the Radio Interface Layer (RIL), and SMS. it's miles more prominent e orderly to benefit the SMS ticket because of the reality less logs are available which calls for substantially less memory and handling at each check.
At the point when the SMS was found in the support, a test is done to the despatched SMS database. What's more, if a relating SMS transformed into included, we can express that there is no danger in light of the fact that the application that despatched this SMS had not endeavored to cover it.
However,when an SMS turned into now not added, all those appswhich have the access to send SMS are verified.
The following notations are used during the data collection step:

i) Operative Action(P) ;
ii) CPU usage U per process P of application X in snapshot as(Up,e);i
iii) Pile of CPU Usages (U p,e) is set C'

We suspect MIN to be the negligible measure of CPU consumption needed to deliver a SMS message. can be estimated in an independent supplier by really calling the "sendTextMessage" without doing each other calculation or apportioning any protest. We experience the pool of applications in C' : for each related admission C p,e that is superior to MIN , we proceed with what's more appraisals, and we assign the pool of such applications as the compelled pool (R).
We characterize MIN and MAX to be the base and greatest sums, individually, of CPU utilization for a particular application in R inside a specific time window. For each application, we figure the distinction among these qualities, which need tosuggest how much intrigue this application has embraced on this specific window.From this point on, a rating is processed for each application in R principally in view of its CPU utilization organize, amount of Licenses required, show state, and foundation/frontal area country. each application score is a summation of three parts.

1) Absolutely the estimation of the difference |MAX-MIN|:
i) if the application is in frontal area, this esteem is increased with the guide of a constriction segment a so one can push off the GUI affect and subsequently get a more attractive assessment; the charge of an is registered as the qualification amongst MIN and the negligible admission cost watched while the application is in chronicled past; ; and If a cost isn't accessible, we take a default expense of 1;
ii) The final value in all instances (heritage/foreground) is equalized to a most of one.
2) The scope of Licenses utilized:
i) If this assortment is bigger than 6.18 [22], a unit is brought;
ii) Otherwise, an esteem same to is presented.
3) If screen is OFF, a unit is conveyed

Hence, the appraisals gained are isolated by utilizing (the amount of score parts thought about inside the summation). This standardization advance to the assortment of makes it simple to incorporate into the calculation additional elements later on. From the variety of evaluations, the best two applications having values higher than the half limit could be hailed as being likely noxious.

5. Algorithm

If a log shows an SMS was sent then
If the SMS sent was not added to data store then
For each $U_{p,e}$ in C
If $U_{p,e}$ is greater than MIN then
If R is in backdrop then
Counr(R)+= Equalize (MAX-MIN)
Else
Count(R)+= Equalize (MAX-MIN)
If has "number of licences" 6.18 then
Count(R)+=1
Else
Count(r)+= number of licences/ 6.18
If screen state is OFF then
Count(R)+=1
Count(R)=count(R)/N
Flag top two R where count(R)>50%

6. Conclusion

In this work, we are mainly targeting the attacks in Android smartphones. Firstly introduced that the sending SMS in the backdrop and for this we have to propose the prevention system of Android against for the both outgoing and incoming malicious SMS in Android device. Next attack uses a simple phone dialer app in which that uses the USSD protocol in the background is used to target end users. For each of these attacks we have to determine for each fundamental of Android operating system, it is responsible for such type of attacks. Finally inorder to prevent the incoming malicious SMs for this we must use the Intrusion Detection System(IDS).This IDS is used to defeat the SMS basing attacks, and also used to detect the 87% of cases with no false positives.

Acknowledgement

The paper intercepting the malevolent android devices is supported by the Department of Computer Science and Technology, India through the fund sanctioned for improvement of Science & Technology infrastructure, at department of CSE, K.L University, by order number SR/FST/ESI-332/2013.

References

[1] Mao, Qiushi. 2015. Experimental Studies of Human Behavior in Social Computing Systems. Doctoral dissertation, Harvard University, Graduate School of Arts & Sciences.
[2] Al-Omany, M., Al-Muhtadi, J., & Derhab, A. (2015). Detection of SMS spam Botnets in mobile devices: Design, analysis, implementation. In LAP LAMBERT. Academic Publishing.
[3] Allalouf, M., Ben-Av, R., & Gerdov, A. (2014). Storedroid: sensor-based data protection framework for android. In International wireless communications andMobile computing conference (IWCMC 2014).
[4] Almohri, H. M., Yao, D. D., & Kafura, D. (2014). Droidbarrier: know what is executing on your android. In Proceedings of the 4th ACM conference on data and application security and privacy (CODASPY'14) (pp. 257e264).
[5] Arzt, S.Rasthofer, S., Fritz, C., Bodden, E., Bartel, A., Klein, J., et al. (2014). Flowdroid:precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. ACM SIGPLAN Notices, 49(6), 259e269.
[6] Batyuk, L., Herpich, M., Camtepe, S., Raddatz, K., Schmidt, A.-D., & Albayrak, S.(2011). Using static analysis for automatic assessment and mitigation of unwanted and malicious activities within android applications. In 6th international conference on malicious and unwanted software (MALWARE 2011) (pp. 66e72).
[7] Bierma, M., Gustafson, E., Erickson, J., Fritz, D., & Choe, Y. R. (2014). Andlantis: large-scale android dynamic analysis. In Security and privacy workshops: Mobile security technologies (MoST).
[8] Crowdroid: behavior-basedmalware detection system for android. In Proceedings of the 1st ACM work-shop on security and privacy in smartphones and mobile devices (SPSM '11) (pp15e26).Cloudmark.
[9] K.V.D.KIRAN,"Integrated Distributed Architecture to Integrate Wireless Sensor Networks (WSN) with Grid for Healthcare," International Journal of Bio-Science and Bio-Technology", Vol.7, No.3 (2015), pp.243-250, ISSN: 2233-7849 IJBSBT.
[10] K.V.D.KIRAN,"A Critical study of information security risk assessment using fuzzy and entropy methodologies," International Journal on Computers and Communications", Pages: 17-22,Vol1,Isuue1,Dec-,12, ISSN: 2319 – 8869.
[11] K.V.D.KIRAN," "Literature Review on Risk Literature Review on Risk and their Components" International Journal for Research in Emerging Science and Technology (IJREST) ",Volume-1, Issue-6, November 2014", (e-ISSN 2349-7610)..
[12] K.V.D.KIRAN, "Performance Analysis of Layered Architecture to Integrate Mobile Devices and Grid computing with a resource scheduling algorithm", IEEE CS'07, SIVAKASI, TAMIL NADU, India.
[13] Khodor hamandi, Ala Salma, "Messaging attacks on Andriods vulnerabilities and intrusion detection", Feb 2014.