IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Method & Implementation to Stop Sim Tool Kit Application Messages

Sushma Singh[1], Ranjit Singh Chauhan[2]

Research Scholar Dept of ECE, Seth Jai ParkashMukund Lal Institute of Engineering &Technology, Yamuna Nagar

Asst. Professor Dept of ECE, Seth Jai ParkashMukund Lal Institute of Engineering &Technology, Yamuna Nagar

Abstract: This paper describes how we can track the messages (SMS) which were automatically send through the cell phone without the user's consent and how to make the phone to restrict such operations. This software is a tool that works like a spy or surveillance program that silently runs in your mobile device. As long as the software is installed in your device, the installed program will continuously run in the background as it logs the information it can retrieve from the cell phone. It is an Android based software once is installed in phone, then it will run in background continuously and tracking every message which are coming from network. When any message is automatically sending in the response of any attacker SMS it will generate a pop up window for the confirmation if we really want to allow our phone to send SMS. For this, it uses Eclipse tool with ADT bundle.

Keywords: Eclipse, ADT, OTA, SIM, STK etc.

I. INTRODUCTION

Today, mobile phone has become popular to everybody since it is very convenient. The most advantage of having a mobile phone is you can communicate to your family and your friends no matter what where you are. For instance, you can contact easily to your friends by calling or sending messages everywhere without electricity. It is maybe the main reason why almost all people today choose to own a mobile phone. From the customer's point of view, it is obvious that mobile phones assist you in business a lot, such as, make schedule of working, surf the internet, and keep in touch with their companies. Moreover, you can relax with mobile phone's applications, for example, play games, listen to music, or chat with your friends .Mobile applications are increasingly applied with the rapid development in mobile communication and terminal technology.Since the first SMS (Short Message Services) message was sent in the UK in 1992, the SMS has become a mass communication tool. At the end of the year 2006 there were over two billion mobile phone users in the world. More than 455 million of these users were in China and more than 389 billion SMS messages were sent in China in 2006[2]. The mobility, ubiquity and low cost of SMS messages make it become a very attractive bearer for mobile business applications. SMS spam is an emerging problem in the Middle East and Asia, with SMS spam contributing to 20–30% of all SMS traffic in China and India (GSMA, 2011b). As an example, these Chinese mobile subscribers received 200 billion spam messages in one week in2008.While it is estimated that in North America the current level of mobile spam is currently only 0.1% of all messages per person per day (GSMA, 2011a), 44% of mobile device owners surveyed in the US reported receiving SMS spam.STK was developed as a way for running applications in the SIM card. It was introduced in 1995 for the first time. Since 1998 almost all of the mobilephones produced have been STK enabled, today every phone on the market STK supports. In these applications, security issues such as user authentication or confidential user data protection are becoming critical. Because an attacker can send a cleverly crafted silent binary SMS update message over-the-air (OTA) to the mobile phone, even without knowing the private signing key. Attackers can force mobile phones to send premium-rate SMS messages or prevent them from receiving messages for long periods of time by leveraging a logic flaw in mobile telecommunication standards, like you download games which needs automatically updates results in downloading content from their website .Automatic Replies by Default Leads to Automatically Subscription or downloading results in deduction of balance amount from mobile phone.SMS spoofing service in which hidden SMS sent and receive on mobiles. Preventing the subscriber from receiving legitimate messages.STK can change the settings of mobiles so that they will not receive important messages or can forward the message to other number. Account Hacking (Face book, Gmail etc.) as in case of we can lose our account info due to STK Attack.

OTA Technology OTA is based on a client/user architecture where at one end there is an operator back-end system and at the other end there is the SIM card. The operator's back-end system sends service requests to an OTA Gateway that transforms the requests into Short Messages to be sent to the SIM card. The OTA architecture is shown in Figure below.

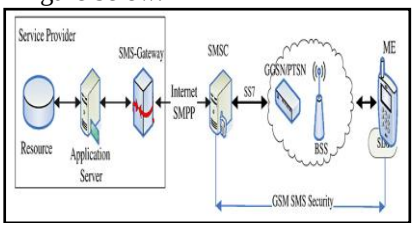

Figure 1: Architecture of Short Message Service

DOI 10.17148/IJARCCE.2016.5623

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

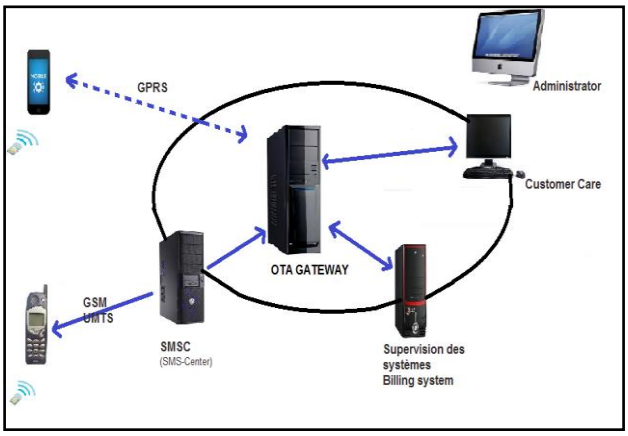

Figure 2: OTA Infrastructure

II. LITERATURE SURVEY

The authors highlighted the technical details of sendinga silent SMS, furthermore sending multiple incessant silent SMSsperforming A silent SMS denial of Service (DoS) attack. Thesestealth messages are not only used to perform DoS attacks butare increasingly sent in order to force the continuous update ofsubscriber location information. It describes from a forensic perspective, how a silentapplication-generated SMS (attack) is discovered. We then investigate the possibilities of retrieving silent SMS evidence at boththe handset and network level.

Author explained that Mobile or SMS spam is a real and growing problem primarily due to the availability of very cheap bulk pre-pay SMS packages and the fact that SMS engenders higher response rates as it is a trusted and personal service. SMS spam filtering is a relatively new task which inherits many issues and solutions from email spam filtering. However it poses its own specific challenges. In this work, it motivated work on filtering SMS spam and reviews recent developments in SMS spam filtering. It also discussed the issues with data collection and availability for furthering research in this area, analyzed a large corpus of SMS spam, and provides some initial benchmark results.Authors presented our efforts towards a framework for exposing the functionality of a mobile application through a combination of static and dynamic program analysis that attempts to explore all available execution paths including libraries. It verified their approach by testing a large number of Android applications with our dynamic analysis framework to exhibit its functionality and viability. The framework allowed complete automation of the execution process so that no user input is required. It also discussed how our static analysis output can be used to inform the execution of the dynamic analysis.

Author realized a secure SIM card, named PK-SIM card, which is a standard SIM card withadditional PKI functionality; based on the PK-SIM card, they presented a security framework offering solutions for the development of secure mobile business applications using SMS as bearer. The security framework consisted of a client device, in which a PK-SIM card was used to store security credentials, a Secure Access Gateway (SAG) which was used to receive and send secure SMS messages, a trusted third-party, Certification Authority (CA), which provided a public-key certification service and a Mobile Operator which provided the communication infrastructure for the SMS.

III. DESCRIPTION OF SYSTEM

Mobile phones have been the focus of cybercriminals for a while now. Some problems lie even deeper in your phone.The target of the attack is the SIM card (Subscriber Identification Module) which is present in all mobile phones. This smart card is responsible for the unique identification number known as the IMSI (International Mobile Subscriber Identity) and also for handling the encryption when communicating with the telephone network..An attacker can send a cleverly crafted silent binary SMS update message over-the-air (OTA) to the mobile phone, even without knowing the private signing key. The device will reject the unsigned message, but it will also answer with an error code signed with the 56-bit DES private key. This allows the attacker to crack the private key through a brute-force attack. Once the key is known, an attacker can go ahead and sign malicious software updates, which are essentially mini Java applets, and send them through OTA updates to the mobile phone. Since the signature matches, the applets will run on the device. Such malicious applets can silently send premium text messages which will generate profit for the attacker or reveal the geo-location of the device.

This alone would be bad enough, but unfortunately some SIM card providers have additional vulnerabilities in their Java implementation, which results in malicious Java applets being able to break out of the sandbox. Hence the applet can read out information from other applets or even extract the master key which is used to derive the encryption keys for voice and data communication. With more and more functions, like mobile payment systems, now relying on the SIM card it makes this vulnerability all the more worrying as it has the potential for a lot of abuse.There are millions of devices worldwide are susceptible to this attack. Telecommunication providers have been informed and some have already started to filter such OTA messages from the network. Users can check with their provider to see if their SIM card is vulnerable to this attack and, if necessary, upgrade to a newer card which is not vulnerable.

Back-end System

The back-end system can be anything from a customer care operator to a billing system, acontent provider or a subscriber web interface. The provisioning system has to be connectedto the mobile network. Service requests contain the service requested (activate, deactivate,Load, modify…), the subscriber targeted and the data to perform the service. The back-endsystem then sends out service requests to the OTA gateway.

OTA Gateway

The OTA Gateway receives Service-Requests through a Gateway API that will indicate theactual card to

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

modify/update/activate. In fact, inside the OTA Gateway there is a carddatabase that indicates for each card, the card manufacturer vendor, the card's identification number, the IMSI and the MSISDN.The second step is to format the service request into a message that can be understood bythe recipient card.

To achieve this, the OTA Gateway has a set of libraries that contain theformats to use for each brand of smart cards. The OTA Gateway then formats the messagedifferently depending on the recipient card.The third step consists in sending a formatted message to the SMSC using the right set ofparameters .

Then the OTA Gateway issues as many SMS as required fulfilling the Service-Request.In this step the OTA Gateway is also responsible for the integrity and security of the process.

SMSC
Services center for short messages (SMS) exchanged between the management system ofthese messages (OTA Gateway) and the cellular network. A message can be sent to or froma Mobile Phone. If the Mobile Phone is powered off or has left the coverage area, themessage is stored and offered back to the subscriber when the mobile is powered on or hasre-entered the coverage area of the network.

SMS Channel
The communication between the SIM card and the OTA Gateway can be done by SMSexchange and in this case named the SMS channel.

Mobile Equipment
Regarding OTA services, the mobile equipment has to be SIM Toolkit compliant.

SIM card
A SIM card, also known as a Subscriber Identity Module, Fig.2 shown below is a subscriber identity module application on a smartcard that stores data for GSM/CDMA Cellular telephone subscribers. Such data includes user identity, network authorization data, and personal security keys, contact lists and stored text messages.

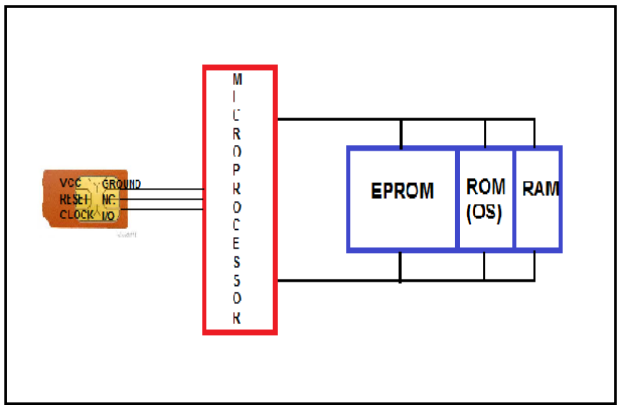

Figure 3: SIM Card Architecture

Function of the SIM card
The SIM card performs the following valuable functions:

1. Identification of a subscriber: The IMSI programmed on the SIM card, is the identity of a subscriber. Each IMSI is mapped to a mobile number and provisioned on the HLR to allow a subscriber to be identified.

2. Authentication of a subscriber: This is a process, where, using the authentication algorithm (COMP128V3 for 2/2.5 G GSM, CAVE for CDMA and Mileage for 3G) on the SIM card, a unique response is provided by each subscriber based on IMSI, Ki (stored on SIM) and RAND (provided by network). By matching this response with values computed on the network a legal subscriber is logged on to the network and he or she can now make use the services of the mobile service provider
.

3. Storage: To store phone numbers and SMS.

4. Applications: The SIM Tool Kit or GSM standard allows creating applications on the SIM to provide basic information on demand and other applications for m-commerce, chatting, cell broadcast, phonebook backup, location based services etc.

Tool Used
Android Development Tools (ADT) is a plugin for the Eclipse IDE that is designed to give you a powerful, integrated environment in which to build Android applications. ADT extends the capabilities of Eclipse to let you quickly set up new Android projects, create an application UI, add packages based on the Android Framework API, debug your applications using the Android SDK tools, and even export signed (or unsigned) .apk files in order to distribute your application.

Developing in Eclipse with ADT is highly recommended and is the fastest way to get started. With the guided project setup it provides, as well as tools integration, custom XML editors, and debug output pane, ADT gives you an incredible boost in developing Android applications.

IV. RESULTS OF SYSTEM

SIM Application Toolkit (commonly referred to as STK) is a standard of the GSM system which enables the Subscriber Identity Module (SIM) to initiate actions which can be used for various value-added services.Figure.3 shows how the STK display looks like.SIM Application Toolkit consists of a set of commands programmed into the SIM that determine how the SIM to interact directly with the outside world and start commands from the handset and network independent.

STK uses the OTA technology which allows the SIM to build an interactive exchange between network applications and end users and access, or access control to network. SIM also provides a command such as displaying a menu on the handset and / or ask for user input.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Figure 4: Steps of System a) When Hit on STK,This Menu Shown, b) Different Options, c) Sends Automatically SMS by Hitting

SIM application Toolkit or STK facilitates the design of VAS applications which run on SIM. STK also allows VAS applications in the SIM to communicate with the external world via messages and commands which are specified by the standardized STK shown in Fig.4. So STK having two functionalities:-

- Designing VAS applications
- Providing mechanism for SMS to run those applications i.e. "trigger" a certain VAS application by receiving a specific SMS or STK commands.

Once this VAS is start running in the SIM, the SIM will be able to send STK commands to the mobile equipment, which is shown in Fig.6, these commands are also standardized in SIM Toolkit specifications. Some user - recognizable examples of these commands is to display some text on the screen or playing a tone to declare some event that requires the attention of the subscriber.

There are other STK commands that interact with the network like sending SMS to the network or setup a call. It's very small software but very helpful to control SMS.No messages can be sent without our confirmation. We can also make same software's for exchanging media, Bluetooth sharing, nfc, calls, mmsetc so that all these can also be controlled.

Figure 5: Confirmation Action For SMS

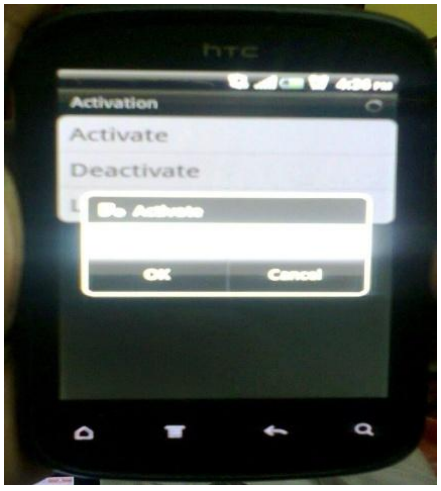

Figure 6: Confirmation Action Forcall

In proposed application, it asks for activation of application. As it is activated, it only provides the send SMS button. It does not provide any back or cancel button for stopping the sending of SMS. When any message is automatically sending in the response of any attacker SMS it will generate a pop up window for the confirmation if we really want to allow our phone to send SMS.

Without permission it cannot send single SMS through our phone. It will also help to stop sending message if by mistaken SMS button is pressed by us. Overall it is good software to control our SMS permissions.

DOI 10.17148/IJARCCE.2016.5623

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

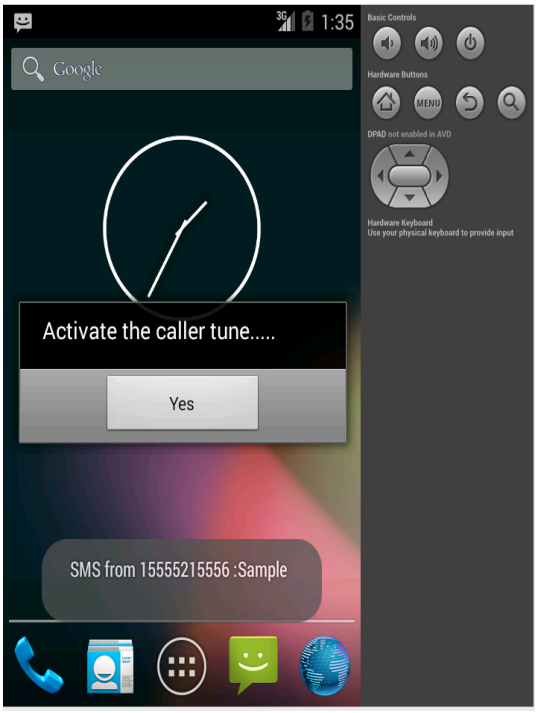

Figure 7: Example of Proposed Application

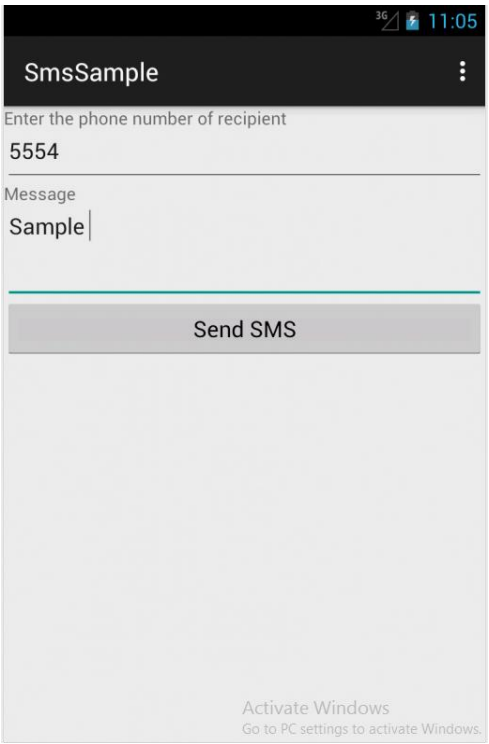

Figure 8: Sample of SMS Sending from the Application

CONCLUSION

It is an Android based software once is installed in phone, then it will run in background continuously and tracking every message which are coming from network. When any message is automatically sending in the response of any attacker SMS it will generate a pop up window for the confirmation if we really want to allow our phone to send SMS. Without permission it cannot send single SMS through our phone. It will also help to stop sending message if by mistaken SMS button is pressed by us. Overall it is good software to control our SMS permissions. Installation of this software will be helpful to stop STK events to be fired without prior to your knowledge (Only feasible for android & Smart Phones).

REFERENCES

[1] SMS Forum, Short Message Peer-to-Peer Protocol Specification version 5.0,http://www.SMSforum.net.
[2] The Monthly Statistics in Communication Industry, http://www.mii.gov.cn/art/2006/12/22 /art_27_27537.htm.
[3] T. Walter, et al., Secure mobile business applications framework, architecture andimplementation, Information Security Technical Report, 9, Issue 4, December2004, pp. 6–21.
[4] S.P. Shieh, F.S. Ho, Y.L. Huang, An efficient authentication protocol for mobilenetworks, Journal of Information Science and Engineering 15 (1999) 505520.
[5] M. Hassinen, SafeSMS—end-to-end encryption for SMS messages, Proceedings ofthe 8th International Conference on Telecommunications, 2, June 15–17, 2005,pp. 359–365.
[6] M. Hassinen, K. Hypponen, Strong mobile authentication, 2nd InternationalSymposium on Wireless Communication Systems, Sept. 5–7 2005, pp. 96–100
[7] Almeida, T. A., Gómez Hidalgo, J. M., &Yamakami, A. (2011). InProceedings of the11th ACM Symposium on document engineering DOCENG'11 (pp. 259-262).Mountain View, CA, USA: ACM.
[8] Beaufort, R., Roekhaut, S., Cougnon, L. A., &Fairon, C. (2010). A hybrid rule/modelbased finite-state framework for normalizing SMS messages. InProceedings ofthe 48th annual meeting of the association for computational linguistics ACL '10(pp. 770–779). Stroudsburg, PA, USA: Association for Computational Linguistics
[9] https://www.defcon.org/-Bogdan-Alecu-Attacking-SIM-Toolkit-with-SMS