Remotely Wiping Sensitive Data on Stolen Smartphones

Xingjie Yu[†,‡,♮] Zhan Wang[†,‡,*] Kun Sun[♯]
Wen Tao Zhu[‡,†] Neng Gao[‡,†] Jiwu Jing[†,‡]

† State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, CHINA
‡ Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, CHINA
♮ University of Chinese Academy of Sciences, CHINA
♯ Center for Secure Information System, George Mason University, USA
Email: xjyu@is.ac.cn, zwang@is.ac.cn, ksun3@gmu.edu, wtzhu@ieee.org, gaoneng@is.ac.cn, jing@is.ac.cn

ABSTRACT

Smartphones are playing an increasingly important role in personal life and carrying massive private data. Unfortunately, once the smartphones are stolen, all the sensitive information, such as contacts, messages, photos, credit card information and passwords, may fall into the hands of malicious people. In order to protect the private data, remote deletion mechanism is required to allow owners to wipe the sensitive data on the stolen phone remotely. Existing remote deletion techniques rely on the availability of either WiFi for Internet connection or SIM card for cellular network connection; however, these requirements may not be satisfied when the phones are stolen by some sophisticated adversaries. In this paper, we propose a new remote deletion mechanism that allows the phone owner to delete the private data remotely even if the WiFi is disabled and the SIM card is unplugged. The basic idea is to use emergency call mechanisms to establish a communication connection with a service provider to verify the state of the phone and perform remote deletion. We present a case study of our mechanism with the Universal Mobile Telecommunications System (UMTS) network.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Security

*This author is the corresponding author.

ASIA CCS'14, June 4–6, 2014, Kyoto, Japan.

http://dx.doi.org/10.1145/2590296.2590318.

Keywords

Mobile Device Security, Remote Deletion, Emergency Call

1. INTRODUCTION

Smartphones are playing an increasingly important role in our daily life to access personal and corporate email, prepare tax returns, and review customer documents, etc [6]. US military also announced that it will equip soldiers with Android devices for accessing classified documents [10]. Smart phones provide massive non-volatile memory to store private and sensitive data such as SMS (Short Message Service) messages, photos, credit card information and social security numbers, user names and passwords [15]. The popularity of mobile devices raises serious and yet unsolved concerns, particularly with respect to data security on stolen or lost devices. From the mid-1990s many crimes have declined significantly, but the theft of mobile phones has become an increasingly serious problem - 49% New Yorkers have experienced mobile loss/theft [11]. Once a smartphone is lost, its sensitive data may be compromised through directly breaking into the phone system or connecting the phone to a PC as an external USB storage.

A number of smartphone wipe-out mechanisms have been developed to delete the sensitive data from lost smartphones. One solution is to automatically delete the sensitive data after a number of failed authentication attempts [12]. However, it may cause accidental data deletion when the owner forgets the password or someone plays with another's phone. Moreover, an adversary still may access the sensitive data by connecting the smartphone to a PC. Remote wipe-out mechanisms allow owners to remotely delete the sensitive data by sending a wipe-out command to the lost devices through the Internet or SMS. For example, iCloud remote wipe-out system [4] can initiate the deletion of all user data by sending "kill" messages to lost mobile devices through the Internet. All existing solutions have to rely on the Internet or cellular network to send specific commands to the smartphone.

Unfortunately, sophisticated adversaries can defeat all existing remote wipe-out mechanisms by removing the SIM (Subscriber Identity Module) card and turning off the WiFi. Once a smartphone is stolen, since the adversary can physically access the device, he/she can remove the SIM card

to disrupt normal communication through cellular network and disable or jam all the WiFi connections to the Internet. Thus, without receiving a wipe-out command, the smartphone has no chances to be remotely wiped out.

In this paper, we develop a remote wipe-out mechanism that allow owners to remotely wipe out a smartphone even if WiFi is unavailable and the SIM card has been unplugged. The basic idea is allow the smartphone use emergency call channel of the cellular network to receive remote commands. When the SIM card is unplugged, no normal calls can be made since the service carrier requires the SIM card for authentication and billing. However, the smartphone still can make emergency calls such as 911 in the US. In our solution, when the smartphone detects the removal of the SIM card, it will initiate a stealthy emergency call to the wipe-out service provider, who will send back a wipe-out command after confirming that the phone has been lost or stolen. The adversary will be blind to the undergoing emergency call. To the best of our knowledge, our solution is the first to enable remote data erasure without relying on the availability of SIM card or the WiFi connection. Our system guarantees that only the real owner can activate the remote wipe-out service through user authentication. Moreover, we can prevent the service provider from accidentally deleting user's data. We choose strong data deletion mechanisms to prevent adversaries from recovering the deleted data after the remote wipe-out process. The whole wipe-out process is unobservable to the adversary.

To demonstrate the feasibility, we provide an example of such a remote wipe-out service in the Universal Mobile Telecommunications System (UMTS) cellular network. Our system only requires a small extension to the current emergency call mechanism, and there is no change on current network structure.

In summary, we make the following contributions:

- We propose a remote wipe-out framework that enables the owner to remotely wipe the data on a smartphone even if the adversary removes the SIM card and disables the WiFi connection.
- We evaluate the feasibility of our design by providing a prototype in the UMTS network.

The next section discusses related work. Section 3 describes the threat model and assumptions. In Section 4, we describe the design of our remote wipe-out mechanism. In Section 5, we take UMTS network environment as a study case. Section 6 discusses the integration of our proposed mechanism with current existing remote data erasure mechanisms. Section 7 concludes this paper.

2. RELATED WORK

To protect sensitive data on stolen smartphones, several anti-theft schemes have been proposed. Tang et al. [14] presented an Android-based scheme called CleanOS, which identifies and tracks sensitive data in RAM and on stable storage, encrypts them with a key, and evicts that key to the cloud when the data is not in active use on the device. However, CleanOS requires network connectivity with the cloud all the time. In addition, Ion et al. [7] found that most users do not trust the cloud provider. As a home-based scheme, Avinash et al. [12] proposed a PIN-based extended security mechanism for iOS devices that can be wiped out automatically after a certain number of attempt failures. Unfortunately, this may cause accidental deletion.

Kuppusamy et al. [9] proposed a model to control a stolen smartphone remotely via SMS. However, it is subject to the removal of the SIM card. Another remote control system, proposed by Joe et al. [8], communicates with remote devices through the Internet. However, none of these solutions can communicate with a smartphone with neither the SIM card nor the WiFi connection.

To improve the privacy and security of lost and stolen smartphones, various anti-theft applications exist and help increase post-theft data control, such as Find My iPhone of iCloud [4], Avast Free Mobile Security [5], Norton Mobile Security [13]. All these apps support remotely wiping the data on an on-line stolen or lost smartphone. However, they all rely on the Internet connection based on the WiFi or the data service from cellular network. Some apps also allow the user to wipe confidential files by sending a special SMS, such as Avast Free Mobile Security [5] and Norton Mobile Security [13]. All SMS-based solutions only work on a smartphone with the SIM card plugged; however, since most devices or data thieves tend to immediately disable the WiFi and remove the SIM card, these solutions cannot guarantee to wipe out the sensitive data remotely.

3. THREAT MODEL AND ASSUMPTIONS

In our threat model, we allow the adversary to remove the SIM card from a stolen smartphone and turn off the WiFi. We assume that the adversary is interested in obtaining its locally stored data, but has not extract the storage chips or transferred the user data before removing the SIM card. We do not consider the sophisticated adversaries who keep a stolen smartphone switched off or position the phone in an electromagnetic shielding environment or keep the battery unplugged all the time. For example, if the attacker performs the attack inside a cage or underground chamber without any signal from the cellular network, our wipe-out mechanism cannot work correctly.

IMSI (International Mobile Subscriber Identity) is used to identify and authenticate a subscriber and is a unique identification associated with all cellular networks. For a GSM (Global System for Mobile Communication) phone, this number is provisioned in the SIM card. The R-UIM (Removable User Identity Module) card used by the CDMA2000 (Code Division Multiple Access 2000) phone is analogous to the SIM card for a GSM phone. In this paper, we use the SIM card to represent all similar components which have the same functionality in different networks.

We perform remote control through emergency call channel. However, not all the cellular networks support using the IMEI (International Mobile Equipment Identity) instead of the IMSI as identification in the emergency call establishment. We assume that the operator accepts the emergency call that uses the IMEI as the identification.

Although the IMEI is usually a unique number to identify mobile phones, sophisticated attackers may be able to tamper with this number. However, this number is still used to uniquely identify a stolen smartphone in most countries. For example, Australia first implemented IMEI blocking across all GSM networks, in 2003 [1]. We assume that the IMEI is unique for a stolen smartphone.

Some smartphones use an internal SIM card instead of a removable SIM card. In addition, some mobile phones

have an IMSI written by special software module. For those devices, the adversary cannot remove the SIM card easily, so we can remotely wipe the device through the SMS or the Internet-based solutions as [13, 5, 4] do.

4. WIPE-OUT SYSTEM DESIGN

4.1 Overview

To provide sensitive data protection for a stolen smartphone without the SIM card and the WiFi connection, we put forward a remote wipe-out mechanism, as shown in Figure 1. Our proposed mechanism allows users to remote control their stolen phones through the emergency call channel, which in our opinion is the only communication channel between such a smartphone and the outside.

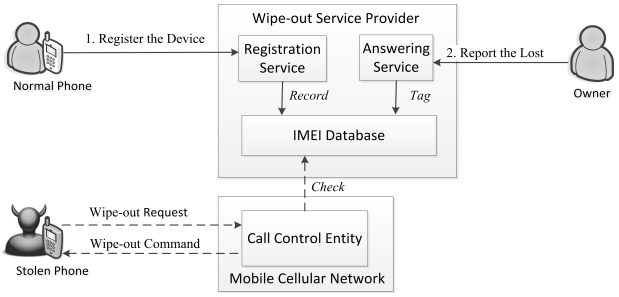

Figure 1: Remote Wipe-out Framework

To remotely wipe sensitive data on a stolen smartphone, the owner interacts with the service provider as follows:

1 The owner subscribes to the remote wipe-out service from the service provider and registers his/her phone before it is stolen. After a successful registration, the service provider records the IMEI number of the phone in the IMEI database and marks its state as normal.

2 The owner reports the loss and asks for erasing the data on the device, as soon as he realizes the lost of the smartphone. After authenticating the user, the service provider tags the associated item of the reported phone as stolen in the IMEI database.

To enable the remote wipe-out service, a backstage application is required to be installed on the phone. Once the SIM card is removed from a smartphone, it may imply that the phone is stolen. In this circumstance, the backstage application starts to ask for data erasure through making a customized emergency call automatically and stealthily. The backstage application will be triggered to make a customized emergency call by either of the following two events: the SIM card is removed from a switched-on smartphone or the smartphone is powered on with the SIM card unplugged. Stealthy operation means that the procedure runs in the backstage: the screen neither lights up nor shows any related information, and any other relevant reminder program could not be activated, for the purpose of preventing the adversary from being conscious of the running procedure.

Once the call control entity of the network receives a wipe-out request from the smartphone, it will check the state of this phone in the IMEI database of the service provider. Here we detail this procedure:

1 The smartphone attaches a deletion indicator to an emergency call, and makes this customized emergency call attempt on the mobile cellular network. The IMEI is used as the equipment identification.

2 The call control entity checks the state of the smartphone in the IMEI database of the service provider, after receiving the request for setting up a customized emergency call.

3 If the smartphone is tagged as stolen in the database, the call control entity sends the wipe-out command to the smartphone. Otherwise, the call control entity responds with a call accepted message which is the same as the access permission for a normal legal emergency call.

The smartphone performs stealthy data erasure after receiving the wipe-out command. If the smartphone receives the call accepted message (case 3), it ends the ongoing emergency call. The customized emergency call can be dialed only once, which consumes little power. But in this case, if the adversary removes the SIM card before the owner realizes and reports the theft, the stolen phone will have no chance to receive the wipe-out command, as the service provider/owner has already missed the only call. To provide higher security, the smartphone can make customized emergency calls periodically until the reception of the wipe-out command. The higher frequency of making such emergency calls, the higher possibility of wiping the data before the adversary peeks at or transfers the user data. However, high frequency results in high power consumption and heavy burden on network as well.

In case there is a normal emergency call dialed on the screen, the backstage application stops making customized emergency call attempts and the ongoing customized emergency call is cancelled instantly. Moreover, the backstage application keeps monitoring the state change of the SIM card. If a SIM card is plugged in after the backstage application has detected the absence of the SIM card, the device stops making the customized emergency call and the data on the device can be remotely wiped out through other current existing mechanisms.

4.2 Device Registration

To remotely wipe sensitive data on a stolen phone without the SIM card and the WiFi connection, a user needs to subscribe to the remote wipe-out service before the smartphone gets lost. The owner registers the service with identification information (e.g., ID card information) that can uniquely identify himself to the service provider and installs our application on the smartphone. The application may be downloaded from a specified web site or obtained through any other way following the specification of the service provider. The identity information can be submitted online or through any other specified way. The service provider records the IMEI number of the registered smartphone and marks its state as normal in the IMEI database.

4.3 Report of Lost Smartphone

If the smartphone is stolen, the owner could request for remotely wiping out the device through a service call or web interface, or even the SMS. The specific way to report the theft is dependent on the specification of the service provider. But the service provider must authenticate the

user before recording the report and perform follow-up procedure, in case that the data erasure is initiated by malicious people. So the user needs to provide identity information for authentication. When the user reports the theft and the identity is verified successfully, the service provider updates the record of the stolen device in the IMEI database by tagging its state as stolen.

4.4 Remote Wipe-Out

When the SIM card is removed from a smartphone, any service that uses the IMSI as the subscriber identification cannot be requested by this phone, such as the basic call service and SMS. However, a smartphone without the SIM card still could camp on an available network to make an emergency call, using IMEI as equipment identification. So we use the emergency channel to remotely control a stolen smartphone.

4.4.1 Deletion Indicator

Once the smartphone detects the absence of the SIM card, it asks for data erasure through making a customized emergency call with a deletion indicator attached. It will receive a wipe-out command after the call control entity of the network confirms that the phone has been stolen. The deletion indicator is attached to an emergency call on the premise that the signaling procedure of the customized emergency call is consistent with the normal emergency call originated by a smartphone as defined in standard protocols. So the network carriers can support our mechanism without any change to the current network structure. The deletion indicator is attached based on minimal modification of the implementation of current protocols. For example, the deletion indicator could be attached by using reserved bits in certain data fields to assign customized values.

4.4.2 Phone State Confirmation

Our mechanism guarantees that the data on the phone will be erased only if the device is indeed stolen. If the call control entity receives a request for setting up a customized emergency call, it checks the state of the smartphone by querying the IMEI number and its state in the IMEI database of the service provider.

The usage of the IMEI database is similar to the blacklist of IMEI numbers which is used during the normal call establishment procedures. The blacklist is an IMEI database deployed in the mobile cellular network. This list records the IMEI numbers of the phones reported stolen or whose operation will adversely affect the network. During any procedure of establishing a call, the call control entity could check the IMEI of the phone in the blacklist and determine whether the device needs to be blocked. Similarly, for a customized emergency call, the call control entity checks the IMEI number in the IMEI database of the service provider confirming the state of the phone, and then decides whether the device needs to be wiped out.

4.4.3 Wipe-out Command

If the returned state is stolen in the IMEI database, the call control entity sends a wipe-out command to the device. The wipe-out command could be formatted through assigning a specific value for a special data field of the call reject message defined in the current call control protocol. Upon receiving the wipe-out command, the smartphone initiates the data erasure.

On the other hand, if the state of the phone is normal, the network will send a call accepted message to the smartphone consistent with the access permission for a legal ongoing emergency call originated by a smartphone without the SIM card. This design aims at keeping the consistency with current protocol. The smartphone hangs up the customized emergency call releasing all occupied resources after receiving this message.

4.5 Security Analysis

Since the service provider verifies the reporter's identity when a smartphone is reported stolen, we can prevent a malicious attacker from misusing our system to falsely wipe another user's smartphone. When a user registers the remote wipe-out service, he submits certain identification information that can uniquely identify himself to the service provider. Furthermore, the service provider may enhance the authentication process by challenging the reporter who wants to activate the wipe-out service with certain specific questions, such as providing one phone number with the most frequent communication.

We can also prevent the service provider or the network carrier from accidentally or maliciously wiping out a smartphone. The user specifies the PIN code for further authentication when installing the wipe-out application on his phone. The user only needs to disclose the PIN code to the service provider when he wants to activate the wipe-out service. The service provider should send the PIN code to the call control entity, if the state of the queried IMEI is stolen. The smartphone should verify the PIN code when receiving a wipe-out command from the call control entity. The PIN code will be deleted during the wipe-out procedure. Users should choose different PIN codes for different mobile devices due to the disclosure of one PIN code to the operator when one device is stolen.

Most anti-theft mobile apps provide two options for users to remotely wipe out a mobile device, *factory reset* and *security deletion*. We test five popular data recovery apps to recover the data deleted by resetting. Though those apps cannot recovery all data, they may recover some data in user partitions. Since resetting can be easily defeated by adversaries, we demand secure deletion instead. Our framework is flexible to accommodate various secure deletion solutions. To ensure a completed deletion, secure deletion should not be interrupted by adversaries, except for power off or being out of battery. Even in this case, an unfinished secure deletion procedure will automatically resume at the next boot until all sensitive data are totally wiped out. Since the execution of secure deletion is transparent to the user, the adversary will not be alerted.

5. CASE STUDY

5.1 UMTS Network

UMTS is a third generation mobile cellular system standard. Smartphone is known as MS (Mobile Station) in UMTS. The MSC (Mobile Switching Center) is the primary call control entity in UMTS network, responsible for setting up and releasing the end-to-end connection, handling mobility and hand-over requirements during the call.

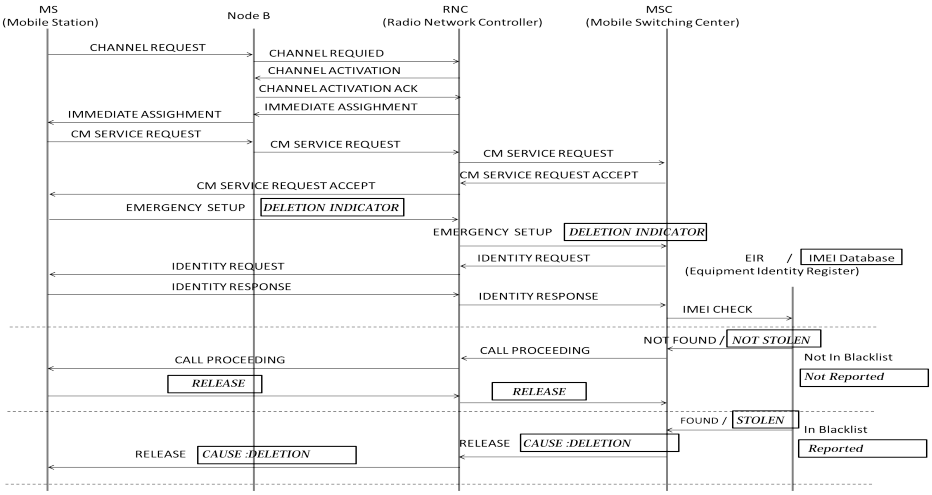

Figure 2: Emergency Call Establishment Procedure in UMTS Network

The core network of UMTS can be accessed through either UTRAN (Universal Terrestrial Radio Access Network) or GERAN (GSM EDGE Radio Access Network). Here we describe the radio access network of UMTS using Radio Network Controllers (RNC) and Node B in UTRAN, which could be substituted by Base Station Control (BSC) and Base Transceiver Station (BTS) in the GERAN.

Equipment Identity Register (EIR) deployed in the UMTS network contains the blacklist of the IMEI numbers associated with banned devices. For a normal call, the MSC could check the IMEI number of the MS in the EIR to decide whether the call needs to be terminated. If the IMEI of the MS is in the blacklist, the MSC will release all active connections for this call.

5.2 Emergency Call

The procedure of establishing an emergency call in UMTS network is shown in Figure 2, and the bordered words indicate our customizations. The "CM service request" message specifies the requested CM (Connection Management) service type as an emergency call and the equipment identification as the IMEI. If the network supports using IMEI as identification, the request will be accepted and the mobile station will send an "emergency setup" message to the MSC asking for the establishment of a call control connection for the emergency call.

5.3 Deletion Indicator

As stipulated in UMTS specification, the information element "emergency category" of the "emergency setup" message indicates the emergency service requested by the MS [3]. Each emergency number stored on the MS is associated with a specific emergency service. The call control entity routes the emergency call to a related emergency center, according to the emergency service category. To customize an emergency call for our remote wipe-out service, we attach a deletion indicator to the "emergency setup" message by assigning a special emergency service category value, indicating the emergency service for data erasure.

The emergency category field is defined in UMTS specification [3], each bit of this field stands for one emergency case, including police, ambulance, fire brigade etc. Specially, bit 8 is reserved and set to 0. Mobile station may set one or more bits to 1 to specify an emergency service category.

8	7	6	5	4	3	2	1
	Service Category IEI						
Length of Service Category							
0	Normal Emergency Service Category Value						
1	Customized Emergency Service Category Value						

Table 1: Emergency Category

To distinguish data erasure from any other emergency service, we set the reserved bit of emergency service category value to 1 as shown in Table 1 and specify this value as "10000000" indicating emergency service for data erasure. This value can be specified to any other value with the bit 8 set to 1.

5.4 Wipe-out Command

For a normal emergency call attempt, the MSC sends a "release" message to the MS with a specific cause value if the IMEI of the MS is in the blacklist. The cause information element in the "release" message is used to indicate the reason for the abortion. We customize a cause "Deletion" through assigning a special cause value.

Upon receipt of the customized "emergency setup" message, the MSC initiates the identification procedure asking for equipment identity, and then it queries the responded IMEI and its state in the IMEI database of the service provider. If the state of the phone is stolen, the MSC sends a "release" message with the cause "Deletion" to the MS as a wipe-out command. We define the cause "Deletion" as 01100111 which is distinguished from all existing cause values, so as to avoid accidental deletion from misunderstanding of a "release" message.

6. DISCUSSION

We design a remote deletion mechanism for smartphones, which will be enabled even though the SIM cards are unplugged and the WiFi is disconnected. However, an adversary may keep the smartphone in different conditions.

Communication Channel	SIM Card Plugged	WiFi Availability
SMS Channel/Internet	√	√
SMS Channel/Internet	√	×
Internet	×	√
Emergency Call Channel	×	×

Table 2: Remote Deletion Mechanism

To provide a full-fledged remote wipe-out mechanism, we suggest implementing several developed remote data erasure methods together with our framework as shown in Table 2. For a stolen smartphone with the original SIM card plugged or replaced by another SIM card, the owner can send a specific wipe-out SMS message to the device. Moreover, if the data service from cellular network or the WiFi connection is available, the owner can remotely wipe out an online device through the Internet. In addition, our proposed mechanism enables remote data erasure on a stolen smartphone when the SIM card is removed and the WiFi connection is not available.

The implementation of our prototype on Android platform is our future work. To support our wipe-out mechanism, we need to make some modifications on current procedure of making an emergency call, involving both the application processor and the modem, so that our remote wipe-out application could make the customized emergency calls and perform the stealthy dialing automatically. Although our mechanism needs the support from cellular network carriers, the carriers only need to make some extensions on their software modules rather than changing their infrastructures. Some carriers in US have already promised that they would support a free and secure anti-theft application for Android devices if and when a manufacturer provides an appropriate solution [2].

7. CONCLUSION

Smartphones are increasingly used for processing and carrying sensitive data, meanwhile become the main targets for thieves, which poses serious security risk on personal data. We propose a novel remote data destruction mechanism for a stolen smartphone when whose SIM card is unplugged and the WiFi is disabled. The network operators can integrate our proposed mechanism to provide remote wipe-put service for the user without any modification on current network structure. Once a smartphone is stolen, its owner can report the theft and ask for wipe-out. If the SIM card is removed by the adversary, the stolen smartphone starts to request user permission for wipe-out through making customized emergency call. We utilize the only communication channel for remote control in such connection constrained environment. We present the remote wipe-out mechanism here to encourage further investigation of implementing remote data deletion on a stolen smartphone.

8. ACKNOWLEDGMENTS

Xingjie Yu, Zhan Wang and Jiwu Jing were partially supported by the National 973 Program of China under Grant 2014CB340603. Wen Tao Zhu and Neng Gao were partially supported by the National 973 Program of China under Grant 2013CB338001. The authors were partially supported by the Strategy Pilot Project of Chinese Academy of Sciences under Grant XDA06010702 and the National Natural Science Foundation of China under Grant 61272479. Dr. Kun Sun's work was supported by U.S. Army Research Office under Grant W911NF-12-1-0060.

9. REFERENCES

[1] AMTA. FAQs on mobile security. `http://www.amta.org.au/pages/amta/FAQs.on.mobile.security`.

[2] Brian X. Chen. New York Asks Cellphone Carriers to Explain Why They Rejected Antitheft Switch. `http://www.nytimes.com/2013/12/11/technology/new-york-asks-cellphone-carriers-to-explain-why-they-rejected-antitheft-switch.html`.

[3] ETSI. TS24.008 Mobile Radio Interface Layer 3 Specification. `www.etsi.org/deliver/etsi_ts/124000_124099/124008/08.06.00_60/ts_124008v080600p.pdf`.

[4] Apple Inc. Find my iPhone, iPad, iPod touch, or Mac. `www.apple.com/support/icloud/find-my-device/`.

[5] AVAST Inc. Avast Free Mobile Security. `http://www.avast.com/en-us/free-mobile-security`.

[6] McAfee Inc. The lost smartphone problem. `http://www.mcafee.com/us/resources/reports/rp-ponemon-lost-smartphone-problem.pdf`.

[7] Iulia Ion, Niharika Sachdeva, Ponnurangam Kumaraguru, and Srdjan Čapkun. Home is safer than the cloud! : privacy concerns for consumer cloud storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, page 13. ACM, 2011.

[8] Inwhee Joe and Yoonsang Lee. Design of remote control system for data protection and backup in mobile devices. In *Interaction Sciences (ICIS), 2011 4th International Conference on*, pages 189–193. IEEE, 2011.

[9] Senthilraja .R G. Aghila Kuppusamy. A model for remote access and protection of smartphones using short message service. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.1, February 2012.*

[10] M Milian. Military to get secure Android phones. `http://edition.cnn.com/2012/02/03/tech/mobile/government-android-phones/`.

[11] Lookout Mobile Security. Lost and Found: The challenges of finding your lost or stolen phone. `https://blog.lookout.com/blog/2011/07/12/lost-and-found-the-challenges-of-finding-your-lost-or-stolen-phone/`.

[12] Avinash Srinivasan and Jie Wu. SafeCode–Safeguarding Security and Privacy of User Data on Stolen iOS Devices. In *Cyberspace Safety and Security*, pages 11–20. Springer, 2012.

[13] Symantec Inc. Norton Mobile Security. `https://antitheft.norton.com/`.

[14] Yang Tang, Phillip Ames, Sravan Bhamidipati, Ashish Bijlani, Roxana Geambasu, and Nikhil Sarda. CleanOS: Limiting mobile data exposure with idle eviction. In *Proceedings of the USENIX Conference on Operating Systems Design and Implementation, Berkeley, CA, USA*, 2012.

[15] Joe Wilcox. Two stories of smartphones stolen. `http://www.oddlytogether.com/post/485601927/two-stories-of-smartphones-stolen`.