A Hardware-Assisted Protection and Restoration Scheme of Lost Smart Phones

Ki YounKim
Computer System Lab
SungKyunKwan University
Suwon, South Korea
kiyoun0414.kim@samsung.com

Euiseong Seo
College of ICE
SungKyunKwan University
Suwon, South Korea
euiseong@gmail.com

Abstract*— Since smart phones are expensive and carrying sensitive personal information including e-mail messages, memos, photos and so on, mobile phone manufacturers are providing services that can protect personal information and help restoration of lost or stolen smart phones. Currently, most of the protection and restoration schemes, which are being used in the commodity smart phones, are software-based. However, such software-based schemes are not effective as they can be easily incapacitated through device initialization, network disconnection, system software modification and so on. This paper categorizes the incapacitation threat methods of the protection and restoration schemes into four, and analyzes how the current software-based schemes cannot function correctly in each threat model. In order to counter these four exploitation models, this paper also proposes a hardware-assisted solution. The proposed scheme is built upon on an additional internal SIM (Subscriber Identifier Module) card and small capacity sub-battery. Finally, this paper assesses the effectiveness of the proposed scheme against the four cases.

***Keywords*— smart phones, security, information protection, privacy, wireless network, SIM**

I. INTRODUCTION

With the increase in the use and prices of mobile phones, the number of theft and loss cases has increased as well. In addition, the loss due to smart phone loss/theft in the US was estimated to be approximately 30 billion dollars in 2012.

According to the research conducted by a network provider, the return rate of the lost smart phones was approximately 50%. In 96% of the cases, the finders accessed data on the phones. That is, half of the smart phone finders chose to return the phones to the owners; however, 96% of them attempted to view information on the smart phones. In particular, 83% of the finders tried to access the files seemingly containing company information, 60% tried to view the information related to social media and emails, and 43% tried to access bank information [2].As this result suggests, loss of a smart phone may lead to a serious information leakage.

As lost mobile phone cases have increased, the mobile phone manufacturers and service providers have attempted to provide information protection schemes to prevent information leakage from lost smart phones and help restoration of them. Most of such schemes are implemented in the software layer. The protection and restoration scheme is activated through wireless network when the owners notify the smart phone of their loss. Then the activated protection software locks the phones or erases the information.

Although the software-based protection schemes can be easily applied to the existing smart phones and requires marginal cost for the application, they can easily become incapable. For example, the device can be forcibly initialized to reset the protection and restoration software. All wireless and Wi-Fi connections can be disconnected to block the loss notification. In some cases, the battery can be detached to hinder the lost phones from entering into the locked state.

This paper proposes a novel hardware-assisted information protection and device restoration scheme that can provide proper service under all four exploit scenarios with the aid of the additional internal SIM card and small capacity non-removable battery..

II. RELATED WORK

A. Related Work

The two largest mobile phone manufacturers, Samsung and Apple, provide services called “Find My Mobile” and “Find My iPhone”, respectively. Both services come with an application software-based remote-control function. These are limited, however, as they require in-advance service registrations and are controlled by application software.

We analyzed the limitations and found there are three primary weaknesses.

First, both services are controlled by an application. There is no service available if the application has not been installed. If the application was deleted or if the user failed to reinstall the application when the smart phone was updated, the services were also unavailable. Most of the abusers who acquired lost or stolen smart phones installed a new version of the binary and sold them in the illegal market.

Second, both services require registration prior to use. The Samsung service provides a lost phone location service in Home Sync, however, as the user manual states, that service is only available when the mobile phone and the Home Sync terminal have been synchronized [5].

Finally, the power is forced off. Locating a lost smart phone is difficult if the battery is removed without any other actions. Moreover, if a new mobile phone binary is installed, the lost phone becomes a used phone, not a lost phone.

Korea’s SKT, a mobile phone service provider, offers a service that locates mobile phones in a more aggressive manner than the mobile phone manufacturers. Its strengths and weakness are as follows.

First, when a smart phone is lost and the customer center is notified, the lost phone is set to the initial screen on which instructions for a lost phone and a 'Call the owner' button display. The emergency call setting that can call the lost phone center and the lock status are updated. However, this service is available only when the lost phone is connected to the network at the time of the report.

Second, when the smart phone finder turns the power off and back on and removes the USIM, the smart phone remains locked. This service, though, is only available when the lost phone has been reported to the customer center and set to the lock status.

Third, the service can delete information such as texts, addresses, and call history in the lost phone. This SKT service can delete all the information in the internal/external memory and initialize the phone settings, preventing personal information misuse. However, if the lost phone finder removes the battery, the initialization setting service of "Find the phone" becomes unavailable.

The above is our analysis of the strengths and weaknesses of the currently commercialized services, products, and patents. We found the common weaknesses are the initialization of the phones, connection to the network, and power cut off. Therefore, the purpose of this study is to propose a solution to address these weaknesses. Our solution will be discussed in detail in the body of this study.

B. *Background Work*

We selected a physical object – the internal SIM card – to overcome the weaknesses of the available services and studies previously discussed. In accordance with TS 31.102, we will now provide a brief description of a SIM card.

A SIM card is a type of ICC card. A mobile phone can be installed with a single SIM card for general usage or up to three SIM cards in the commercial market. All SIM cards are inserted in the outer space of the mobile phone. A SIM card is a physical communication medium used to initialize the mobile phone and to link with the service provider's network. The structure of a SIM card is tree-shaped containing an MF (Master File), DF (Directory File), and EF (Element File). The MF is the root of the tree. As shown in Fig. 1, the DF and EF remain below the MF. The DF, as defined in TS 31.102, is a directory file consisting of GSM and Telecom. There are multiple EFs under these two directory files. A mobile phone links to the network and saves personal information using these two directory files. In addition to the directory files defined in the specification, the network providers create or define new directory files or EFs as required.

The fields in a SIM card define the access conditions. With the conditions of READ, UPDATE, DEACTIVATE, and ACTIVATE, there are five access conditions: ALW (Always), PIN1 (Personal Identification Number 1), PIN2 (Personal Identification Number 2), NEV (Never), and ADM (administrative). For example, if a mobile phone is set to PIN in READ, the user can READ the corresponding field in the SIM card only when a PIN is entered. When it is in ADM, no one can access the field except the administrator. Therefore, the administrator, i.e., the SIM card provider, assigns a confidential ADM code to each SIM card [3].

III. Our approach

A. *Hardware Components*

We adopted an additional internal SIM card and internal small-capacity battery to overcome the aforementioned limitations of the conventional software-based schemes.

1) Internal SIM card

There are three reasons why we selected an additional SIM card as the medium for remote control of smart phones.

First, a SIM card is more robust to taming than the software component. In accordance with the mechanism explained in TS33.102 and TS31.102, the data stored in a SIM card is strongly encrypted, and the procedure for the authentication and participation for a wireless network is strictly defined to use the SIM card data when the device is powered on. Furthermore, a phone is required to evaluate the access condition and verify it in order to access the EF if the access condition is set to PIN or PIN2.

Second, a SIM card has a memory and CPU and is capable of executing a simple program. Thus, if an event occurs, the SIM card can make a decision to proceed or interrupt services following the predefined procedures. If a mobile phone is considered as lost or out of owner's control, the external SIM card can be blocked and the smart phone is enforced to connect to the network for the protection and restoration service by the internal SIM card.

Third, a SIM card requires marginal power consumption in comparison to the other components. In addition, it stays in the sleep state when it is not necessary. Therefore, the impact to the battery lifetime by the external SIM card will be negligible.

Fourth, SIM card has own protect solutions. When SIM filed is accessed, SIM card check the access condition.

The internal SIM card includes DF REMOTE and EF CRL fields, in addition to the basic SIM file tree structure as shown in Fig. 1. Access condition of EF CRL is PIN2. So, a phone is required to evaluate the access condition and verify it in order to access the EF CRL if the access condition is set to PIN2.EF CRL stores the IMEI, the unique identification number for the mobile phone, MSISDN, the phone number for the mobile phone, and the lock level. The host smart phone must be able to separate its internal SIM card from the external SIM card. Therefore, both internal and external SIM cards are assigned their own "GPIO" values, which define event process channels between the host device and SIM cards. When the lost mode is activated, the internal SIM has been designed to set the "lock level" bit appropriately in the EF field. The lock level is either the Protection Mode or Lock Mode. Both internal and external SIM cards are distinguishable by the 1 bit field of RFU in the EF ICCID field, which is the SIM identifier to the network provider.

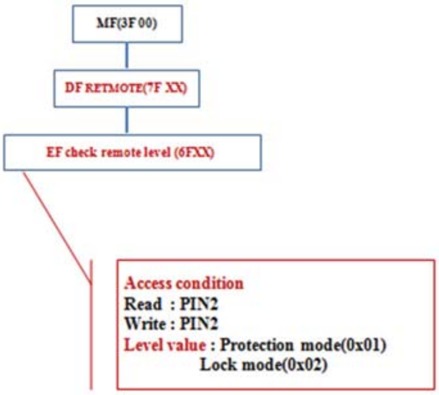

Fig. 1. Internal SIM card structure

2) Non-removable small-capacity battery

If the main battery is removed, the protection and restoration services will not function. Therefore, we include a small-capacity internal battery in the scheme for the case that the external battery is removed. The non-removable internal battery is supposed to supply power for only about ten to fifteen minutes, allowing the terminal to react to abrupt detachment of the main battery.

The utility value of the built-in battery will be explained. The "GalaxyS5" has a capacity of 2800mAh. We were calculated with size ratio and capability. For Galaxy S5, it may be the Internet 11 hours of continuous use, 13 hours continuous video view; it is 20 hours of continuous use 3G call. According to this, it may be useful to 30 minutes continuous time to time for the remote control, if 1/40 of the size of the current, it is possible to receive the remote control service.

IHS is a market research organization was analyzed by $ 5.5 per piece price of the battery of Galaxy S5. When the size ratio of the internal battery is thus calculated as 1/40, the remote control can receive a price

B. *Operation Strategies for Threat Types*

1) Preserved connection

The operation of a remote-controlled system with an internal SIM card can be remotely controlled. When the user reports the missing smart phone to the network provider, the provider sends an STK message SMS PP download [3][4]. This message is not noticeable to the user. However, a large size message can be sent to the SIM card directly from the network provider.

The network service provider sends messages to both the external and internal SIM cards. The message deactivates the external SIM card. Then, the internal SIM card is activated and the lock level of the internal SIM card is set to the Lock Mode. The lock level is always checked whenever the smart phone is powered on or off. If the value is set to the Lock Mode, the device enters into the lock state that can only be deactivated with the reconfirmation message from the network provider.

In case that the Lock Mode is set, the internal SIM card and the network are linked in the emergency mode. The linked network can continue to update the location of the device.

When the device is in the Lock Mode, any outside events and interrupts are ignored to prevent a finder of the device to access the stored data or to abuse the device. In addition, the internal SIM card can be programmed to provide alarm services such as displaying messages, playing ring tones and so on to help the finder returning the phone to the owner.

2) Disconnection from the network provider

The device is normally in the Protection Mode. In this mode, the internal SIM card continues to check the status of the device and changes the lock level in the EF CRL field to the Lock Mode or enables the conventional software lock screen, which requires the predefined PIN2 code to use the device, when it determines that the personal information or integrity of the device is in jeopardy.

For example, user set the Protection mode with setting menu. At that time, user has to insert the PIN2 number for accessing the EF CRL filed. If the device is disconnected from the wireless network and the user tries to use the smart phone, it will request the user to input the PIN2 code. If the user failed to enter the correct PIN2 code, the device will enter into the Lock Mode and wait for the release message from the network provider.

Finally, if the user tries to initialize the device or enforces the debug (or development) mode via a USB link as shown in Fig. 2, the device will block such operations until it verifies that the internal SIM is in safe condition. In other words, the initialization or transition to the debug mode is only available while the device is being connected to the wireless network and the SIM card is able to verify the soundness of the device state.

3) Graceful power down

A malicious finder may try to change the device state to the debug mode after turning off the device and connecting it to a host PC via a USB link.

The lock level is set to Lock Mode when the device is unsure that the device is not lost or stolen while the power is down. The required power to make the transition to the Lock Mode is supplied by the internal battery even when the main battery is not available. In the Lock Mode, all USB connections are blocked.

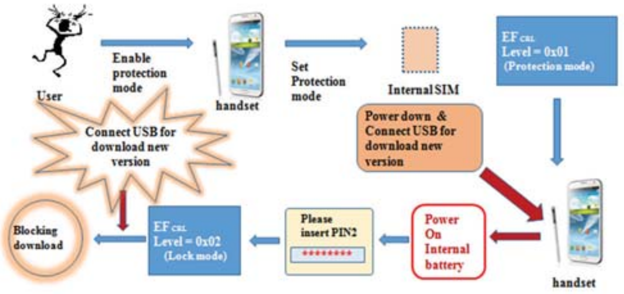
User
Enable protection mode
handset
Set Protection mode
Internal SIM
EF CRL Level = 0x01 (Protection mode)
Connect USB for download new version
Power down & Connect USB for download new version
handset
Blocking download
EF CRL Level = 0x02 (Lock mode)
Please insert PIN2
****
Power On Internal battery

Fig. 2. Power down and USB connect

4) Abrupt battery detachment

When the power is forcibly down and the lock level is the Protection Mode, the lock level changes to the Lock Mode. This lock will be released when the device is turned on again and verifies that it is not lost or stolen by consulting with the network provider via wireless network.

If the device wakes up and finds out that it is lost, the device uses the internal battery as its power source to transfer the location information of the device to the network provider and to deliver alarm messages to the finder.

IV. Conclusion

The current software-based protection and restoration schemes for lost smart phones can be easily neutralized by malicious but simple maneuvers. In order to protect the lost phones against such threats, this paper proposed a novel hardware-assisted scheme that is built on the internal subsidiary SIM card and battery. This paper categorized the possible threats to the lost smart phones into four, and showed that the proposed scheme is resistant to all four exploitations..

References

[1] R. Yu, “Lost cell phones added up fast in 2011,” USA Today, March 23, 2012.

[2] Symantec Co., “Introducing the Symantec Honey Stick Project,” The Official Symantec Blog, March 9, 2012.

[3] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application," The 3rd Generation Partnership Project (3GPP), 2013.

[4] 3GPP TS 31.111: "USIM Application Toolkit (USAT),” The 3rd Generation Partnership Project (3GPP), 2013.

[5] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[6] 3GPP TS 33.102:” 3G security; Security architecture”

[7] Apple’s icloud manual http://support.apple.com/kb/PH2580