Remotely Wiping Sensitive Data on Stolen Smartphone

Orkan Bakis & Matthew Austin

Fontbonne University

Abstract

A smartphone is personal computer which has a mobile operating system. Today’s biggest smartphone companies are Apple and Samsung. Smartphones use cellular network for voice, SMS, and Internet communication, it also supports WiFi. The world's first smartphone was created in 1995, and since then it took over the world. This device allows us to store personal data such as, photos, messages, contacts, credit card information, passwords, etc. It is important to keep this data private, and in order to protect the private data major companies such as Apple and Samsung implemented remote deletion techniques into their devices. These techniques rely on the connection via Wi-Fi or cellular network connection (SMS). However, if the phone is lost or stolen, the owner of the phone may not be able to use this technique due to loss of connection. In this paper, we will explain how the user can remotely delete his data on his smartphone even if there is no connection. We will also cover some of the cases, which hackers use these techniques to steal personal and business data.

1. Introduction

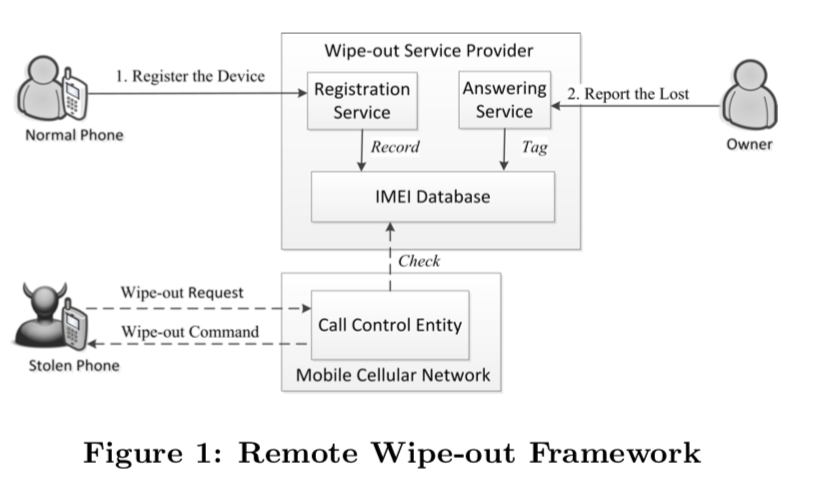
We use smartphones for communication, storing personal data, such as pictures, contacts, credit card information, emails, etc. Smartphones have become a huge part of our lives, it is even used in the military for the soldiers to access classified documents. This makes keeping these data secure is very important. According to the researches, a lot of the crimes have declined since the 1990’s, however the theft of mobile devices became an increasingly serious problem. This issue forced the experts to come up with techniques to make sure the users can remotely access their devices and delete their personal data if the device is lost or stolen. One of the first solutions was if there was an excessive failed attempt to access to the device, it would automatically delete the data. However, this doesn’t happen remotely. Remote wipe technique allows user to remotely access their device and erase their personal data through the Internet. For example, iPhone users can use iCloud.com to remotely access their device and take multiple actions such as playing a sound from the phone, this may help find the lost device if it is close by, lock their device (this may disable whoever has access to phone to not be able to reach the data), and erase all of the data. The biggest issue with this technique is that if the device is stolen and the thief took the sim card out and turned off the Wifi, the owner off the phone cannot do anything due to lack of connection.

This paper explains a technique which allows users to access their device even if it has no connection to the Internet. When the device is lacking a SIM card, it cannot make any calls except 911. This technique is similar to that, as the smartphone detects when it’s missing a SIM card, and automatically initiates an emergency call to the wipe-out service provider. After the emergency call, the provider will send back a wipe-out command after it confirms that the device is lost or stolen. The key of this process is that the criminal who is in possession of the device will not have knowledge of this happening, which would disable him to take action against the wipe-out mechanism. This mechanism makes sure the only the real owner of the device can activate this wipe-out action remotely, and it also makes sure that criminal cannot recover the deleted data.

* 1. *Related Work*

There are some related projects similar to this wipe-out system, to protect the data on stolen smartphones. CleanOS is an Android-based scheme, which identifies, and tracks the data in the memory, and encrypts the data with a key and puts the key in the cloud when the data is not in active use. However, this mechanism(CleanOS) requires connection to the cloud at all times. This makes this scheme not trusting by smartphone owners.

1. Wipe-Out System Design



The owner’s interaction steps are followed as:

* The owner must register to the remote wipe-out service from the service provider before the device is lost or stolen. After the registration, the service provider saves the IMEI number of the device in the database and marks it state “normal”.
* After the device is lost or stolen, the owner asks the service provider to erase the data and to tag the device as “stolen” in the database.

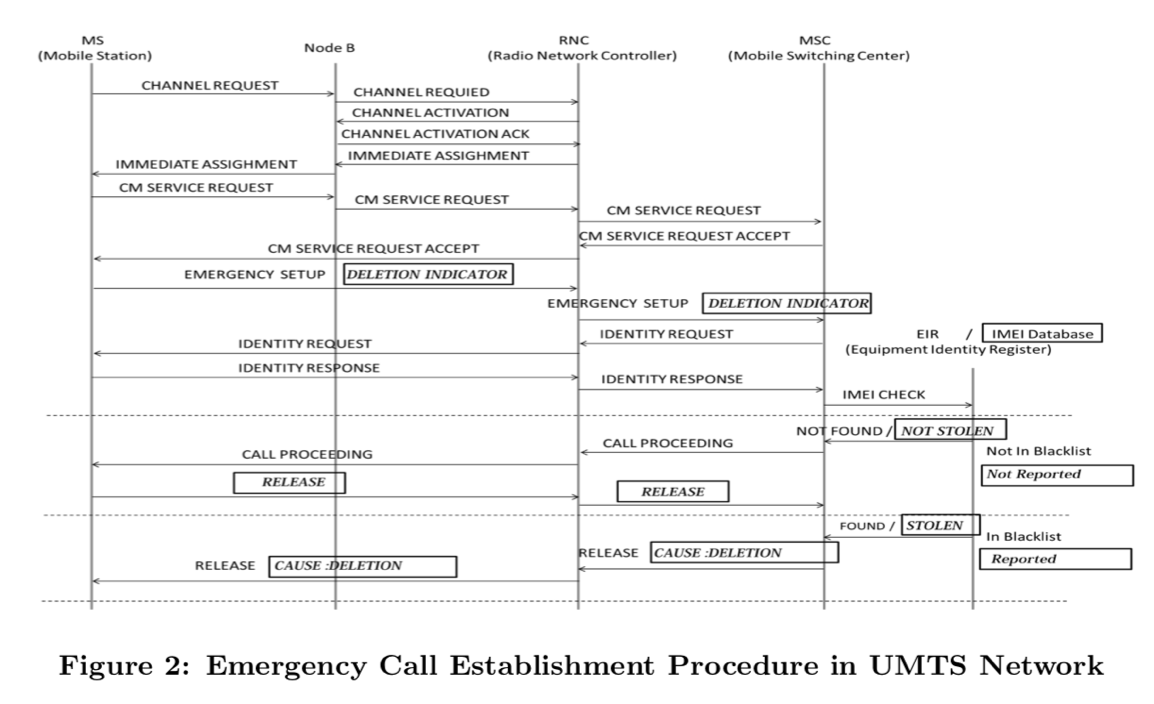
This mechanism requires users to install a backstage application on their phone. This backstage application is programmed to make the emergency call to the wipe-out service provider. It is a huge advantage to have this application as a backstage application because as mentioned before the criminal will have no idea the wipe-out is happening. The steps of the process of receiving a wipe-out request and checking the database is:

* The backstage application makes the emergency call and the IMEI of the phone is used as the equipment identification.
* After the request, the state of the phone is checked in the database.
* After checking the state, if its tagged as stolen the wipe-out operation takes place.

If there is a normal emergency call made on the phone, or the SIM card has been inserted into the device, the backstage application terminates.

1. Emergency Call

Emergency call procedure is shown in the figure below.



1. Hacking by Remote Wipe Cases
2. *Apple*

The traditional methods of remote wipe all prove to be a disadvantage to the very user it is meant to protect. Through various articles such as “How Apple let a hacker remote wipe an iPhone, iPad and, MacBook”, the results show that current mechanism are outdated. The author of the article Emil, states how someone hacked into his iCloud account and reset his password by exploiting Wi-Fi/Internet Connection. The notification of the password reset was sent to the trash by the hacker, thus Emil was unaware of their actions. With access to their iCloud and saved password via Keychain, the hacker was able to access their primary and secondary emails as well as their social media to prevent Emil from having any chance of regaining access. Of course, once the hacker extracted all the data that they needed, they remote wiped Emil’s iPhone, iPad, and MacBook.

1. *Samsung*

In another article called “Any Samsung smartphone can be factory reset remotely with this hack”, the author Vijay, explains how a hacker exploits a phones SIM/Network Connection to remote wipe a user’s phone against their will (Vijay). The hacker begins by rebooting the stolen iPhone, connecting it to Wifi and connecting it to a computer. The hacker then downloads a program on the phone that allows fake phone calls to be made. Once the call comes in the call inhibits the user and service provider from sending the kill command to the phone, thus causing the phone to become useless to the hacker. The hacker bypasses, this thus allowing them to reboot the phone and use it as a new normal Samsung phone. These examples show how the traditional methods that require Internet and Network Connection to prevent hackers are in fact being used to help them control or wipe the phone.

1. Conclusion

With the new method created by Xingjie Yu, the user can still have control of the phone and remote wipe, thus protecting their data by establishing an emergency call in UMTS network (Emergency Call). This procedure starts when the “CM service request message specifies the requested CM (Connection Management) service type as an emergency call and the equipment identification as the IMEI (International Mobile Equipment Identity) (Yu).” This request message is sent to the service provider once the SIM card is removed or the user request deletion via Service Provider, since emergency calls can be sent in any condition that International Mobile Equipment Identity has to see the requesting service type as an emergency. The IMEI knows that the request is an emergency call because “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 (Yu).” To customize the emergency call system the author attaches a deletion indicator to the “emergency setup” message. This is done by assigning a special emergency service category value (SESCV), that information’s the emergency service of data erasure. This SESCV is assigned by a bit and “each bit of this field stands for one emergency case, including police, ambulance, fire brigade, etc. and the Mobile station may set one or more bits to 1 to specify an emergency service category (Yu).” To differentiate a regular emergency call from the new data erasure call, the value is set to “10000000”. Thus, once a person iPhone is stolen and the their or hacker is able to disconnect the phone from Internet and Network Connection, “the MSC sends a “release” message with the cause “Deletion” to the MS as a wipe-out command (Yu).”

**References**

Yu, Xingjie, et al. “Remotely Wiping Sensitive Data on Stolen Smartphones.”*Proceedings of the*

*9th ACM Symposium on Information, Computer and Communications Security - ASIA CCS '14*, 2014, doi:10.1145/2590296.2590318.

Protalinski, Emil. “How Apple Let a Hacker Remotely Wipe an IPhone, IPad, MacBook.”*ZDNet*,

ZDNet, 4 Dec. 2015, .

Vijay. “Any Samsung Smartphone Can Be Factory Reset Remotely with This Hack.”*TechWorm*, 13