In this modern day and age, cellular devices are seamlessly integrated into everyone’s daily lives. Most people would easily say that their livelihood, private information, and precious memories reside on their cell phone. It would completely devastate someone if suddenly they realize their phone was stolen and everything was deleted or they wake up to someone demanding a ransom for the non-deletion of the contents on their phone. In the article “Remotely Wiping Sensitive Data on Stolen Smartphones” the authors describe and evaluate how a hacker is able to deleting everything on a persons phone via remote wipe and ways protect a person can protect themselves from it.

In order for a hacker to delete private data, they take advantage of the very mechanism that was created to protect them. This mechanism is called the remote deletion mechanism, which allows users to wipe their sensitive data if their phone is stolen. Traditional remote deletion methods rely on the access to WiFi (Internet Connection) or the SIM card (Network Connection). Unfortunately, hackers are able to use a new remote wipe mechanism that doesn’t require internet or network connection, but the usage of the emergency call mechanism that establishes a “communication connection with a service provider to verify the state of the phone and perform remote deletion (Yu).”

As stated before, smart phones play a major role in people's daily lives as it hold personal information such as emails, and corporate and documents. With so much power in a small device it’s become common for them to be stolen, in New York almost fifty-percent of its citizens stated that they have been a victim of mobile loss and/or theft. Thus once the device is stolen, hacker is able to steal and/or delete the phones contents by breaking into the phone directly or connecting it to a computer via USB. The phone has many other mechanisms to combat theft which include automatic deletion of sensitive data after multiple failed authentication attempts, such as typing in the wrong pin too many times. This mechanism can also be a disadvantage to the user due to the chance of their data being accidentally deleted because they either forgot their password or someone played on their phone. In order to remote wipe-out command is sent to the phone, an example of this is iCloud sending a kill message to cell phones through internet connection. A theft or hacker can easily bypass or prevent the kill command by removing the SIM or disconnecting the device from WiFi, thus prevent the user to remote wipe by choice.

To prevent a situation where a stolen iphone is disconnected from WiFi or has the SIM card removed preventing user remote wipe, the authors developed a remote wipe mechanism that allows remote wipe without Wifi or SIM by allowing the smartphone to use the emergency call channel of the cellular network to receive the remote kill command once the SIM card is removed or is disconnected from WiFi. Once the data is deleted from the phone, the thief or hacker has no way of recovering it. There are other similar mechanisms that allows the user to still have control once their phone is stolen. The mechanism is called CleanOS, “that 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.” the major drawback of this method is that it requires network connectivity with the Cloud all the time. There are many other mechanisms such as PIN authentication failure and “Find My iPhone” that have major limitations that prevent the user from still having control.

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 (Protalinski). The author of the article Emil, states how someone hacked into his iCloud account and reset his password by exploiting WiFi/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. 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 users 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.

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 informations 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).”

Works Cited

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

Aug. 2016,.