Security for Android Mobile Phones using Biometric Authentication against Factory Reset

Suchita Rane[1], Dr. Narendra Shekokar[2]

[1]Student, Computer Engineering Department, D. J. Sanghavi College of Engineering, Mumbai, India

[2]Professor, Computer Engineering Department, D. J. Sanghavi College of Engineering, Mumbai, India

Abstract: ***Android Mobile devices are secured using various mechanisms like pattern, pin, and password. Biometric Authentication is an upcoming technology accepted by various android mobile manufactures for better security and with change in technology, time this mechanisms are vulnerable to various attacks like factory reset. Factory Reset will erase all the settings in the device and makes device vulnerable for hackers to misuse it. This paper proposes a mechanism to overcome against hard reset as well as factory reset through settings by allowing person to perform factory reset operation only after passing biometric authentication and using correct back-up code. Mobile device can be more secured by using biometric authentication with other factors like security question, alternate email-id, and authentication code generation algorithm.***

Keywords: Biometric, Factory Reset, Security, Mobile devices

1. Introduction

Mobile phones vary from simple to smart phones, from cheap to the most expensive phones. Mobile devices are not only used for communication but also for storing sensitive data and credential information like username password, bank details, personal details and such information can be misused when mobile device gets stolen or lost [6]. With increase in mobile theft, security plays an important role. When proper security is provided to the device sensitive data can be deleted remotely after device gets stolen or make device useless for thief which will discourage mobile theft.

Biometric Authentication is a technology adapted by many mobile manufactures for mobile security [1], [4]. Biometric authentication means authenticating a person based on their biological characteristics such as fingerprint, face, iris, voice, and retina. Biometric fingerprint recognition is used in majority of the smart phone's. The advantage of fingerprint biometric authentication over other biometric authentication is the uniqueness, high performance. All the people in the world have their own unique fingerprint, two persons cannot have same fingerprint not even the twins. A standalone biometric security is unreliable because of device vulnerabilities.

In Android mobile devices like HTC One Max, Samsung Galaxy Note [5] user can start device using back-up password or by fingerprint biometric authentication. Once the device is stolen there is no security to prevent against factory reset since system does not ask user to provide any authentication before resetting the device. So such devices are vulnerable for hard reset as well for data wipe software's from memory card.

Factory Reset is one the mechanism by which device can be hacked even though it consist biometric authentication. Factory Reset [7], [8] is a way to erase all device settings as well as user data, applications, storage. This will return the device in state when it was shipped from the manufacturer. Factory reset has positive as well as negative usage. The positive usage is to wipe out user data before selling device, to fix any software issue, to remove virus that is difficult to remove, to clear memory space. The negative usage is to start a stolen mobile device. When the device gets factory reset all security is wipe out and all sensitive data is vulnerable to the hacker.

In this paper we are proposing a mechanism to secure the device against factory reset and mechanism to make mobile security more reliable.

This paper is designed as follows: Section 2 describes the work done in biometric field related to mobile devices. Section 3 describes the proposed system. Section 4 concludes paper.

2. Related Work

Kataria, Adhyaru, Sharma, Zaveri [1] have briefly explained biometric authentication process and different types of authentication techniques including its strength and limitations. Fingerprint authentication have high uniqueness, permanence, performance and medium universality, measurability, acceptability, circumvention which states that it is best among other biometric authentication like hand geometry, iris, retina, face, ear, voice, signature etc.

Ritu, Sonam, Vinita, Vishakha [2] have proposed an algorithm to generate pseudo random numbers. The algorithm has large cycle and values are uniformly distributed. The algorithm takes a seed value (X_0) as input further using formula given below it is used to generate a set of random numbers. The formula used is as follow:

$$X_{n+1} = X_n^{\log(\sin(X_n))} \quad (1)$$

This formula can be used in various applications to generate random numbers, computer programming, simulation, sampling, decision making, and cryptography.

Donny, Liza, Lei [3] has proposed a system to discourage mobile theft and prevent theft of sensitive information. The mobile phone having biometric authentication will only charge when it gets connected to phone charger which consist biometric authentication that act as a dongle. Such system will discourage mobile theft since the thief has to steal both phone and charger without charger the phone will be useless. When phone gets stolen due of biometric authentication the owner of phone get time to erase the sensitive data remotely. Vendors should provide a unique mechanism to delete data remotely since apps which are used to delete data remotely may sometimes be vulnerable to viruses [9].

The drawback in this system is the cost of biometric scanner based charger, further user have to carry the charger everywhere since the device can only charge with that particular charger. Such charging mechanism will discourage the wireless charging technology used in mobile phones and the build-in-lithium battery cannot be removed. Biometric reader in phone when connected to computer with USB cord act as authorization point, the power button is enable only to lock and unlock the device, which reduce the use of power button feature to perform other operations. The system is still vulnerable to factory Reset since there must be other provision to perform hard reset and hacker can also introduce data wipe software through memory card slot.

3. Proposed System

3.1 System Overview

To overcome the vulnerability of factory reset we are proposing a mechanism using biometric authentication with factors like back-up code, alternate email-id, and security question to secure the system. Device start by fingerprint biometric authentication and only one fingerprint will be register. The device consist no memory card slot since no proper external storage encryption is provided in android devices allowing no provision to introduce the data wipe software in mobile device [10]. Our proposed system consists of three phases. The first phase is about storing the biometric fingerprint for the first time and updating the factors. Second phase is about mechanism to protect from Factory reset. Third phase is generation of authentication code algorithm.

Table 1: Factors used to secure Mobile device.

Sr .no	*Factors*
1.	Fingerprint
2.	Back-up code
3.	Alternate Email-id
4.	Security question

3.2 Phase one: Registration and Updating of Factors.

User should register fingerprint 10 times in system for system accuracy for first time in shop when device is purchased. Further the user enters a back-up code which will be alpha numeric and case sensitive of length 6. The first 4 input is user defined whereas last 2 inputs are system generated. The back-up code have strong strength since it is combination of lower case, upper case and numeric value and since it is a combination of user and system generated code it will be difficult to guess. The user needs to enter an alternate email-id. Further the user enters answer for a user selected security question. Last the user enter numeric key which will be used for authentication code algorithm for first time.

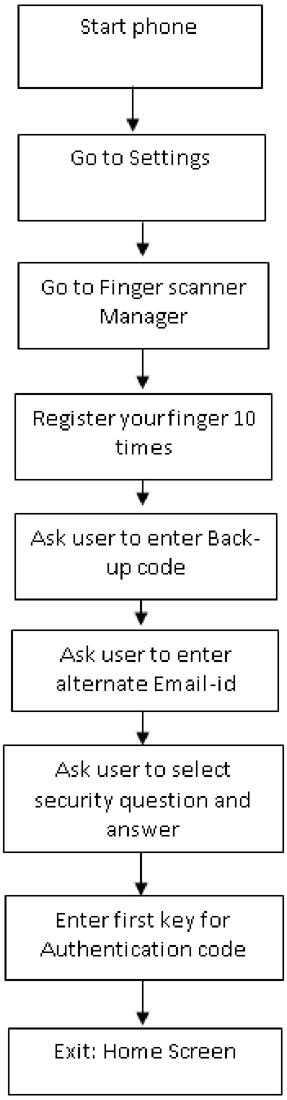
Start phone
Go to Settings
Go to Finger scanner Manager
Register your finger 10 times
Ask user to enter Back-up code
Ask user to enter alternate Email-id
Ask user to select security question and answer
Enter first key for Authentication code
Exit: Home Screen

Figure 1: Registration of Factors

To update any of the listed factors the user has to start device by passing fingerprint biometric authentication [11] and select finger print manager in settings. User select any one of choice like to update fingerprint, update back-up code, update alternate email-id, update security question.

For updating fingerprint the user should provide correct back-up code which allows deleting the existing fingerprint. To register for new fingerprint user should provide generated authentication code which is obtain by using multi window feature of mobile device. Generate authentication code option is selected from settings to generate authentication code, user have to make use of key which user enters while registration for first time (in case of first time update) or while obtaining the generated authenticated code during previous update (in case of nth time update) and provide in other window. When correct authentication code is provided system allow user to register for new fingerprint 10 times. This mechanism will help in case of artificial fingerprint is obtain, it will be difficult to guess the key use to generate the authentication code and the hacker won't be able to update existing fingerprint which will discourage use of multiple sections in device having biometric authentication.

Updating the back-up code require correct current back-up code and answer for security question. Appropriate existing email-id and answer to security question will allow to updated email-id. To update security question, correct answer for existing security question and back-up code should be provided by user to the system.

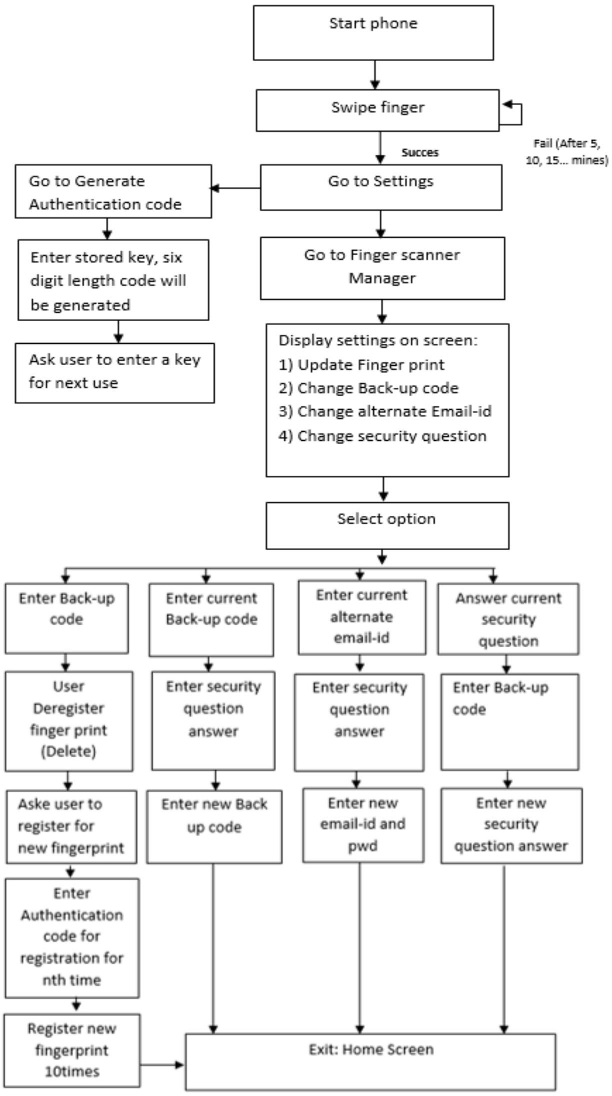
Start phone
Swipe finger
Succes
Fail (After 5, 10, 15… mines)
Go to Generate Authentication code
Go to Settings
Enter stored key, six digit length code will be generated
Go to Finger scanner Manager
Ask user to enter a key for next use
Display settings on screen:
1) Update Finger print
2) Change Back-up code
3) Change alternate Email-id
4) Change security question
Select option
Enter Back-up code
Enter current Back-up code
Enter current alternate email-id
Answer current security question
User Deregister finger print (Delete)
Enter security question answer
Enter security question answer
Enter Back-up code
Aske user to register for new fingerprint
Enter new Back up code
Enter new email-id and pwd
Enter new security question answer
Enter Authentication code for registration for nth time
Register new fingerprint 10times
Exit: Home Screen

Figure 2: Updating of Factors

3.3 Phase two: Securing against Factory Reset

Factory Reset is perform through settings and hard reset. For factory reset through settings, user have to pass the biometric fingerprint authentication allowing access to settings and selecting back up and reset option in which factory reset is selected. User need to turn on the Wi-Fi/data plan and location service to proceed further and enter correct back-up code which will reset mobile device after 5 hrs when the number of attempt exceed 3, in 4th attempt the front and back camera will capture the image, GPS co-ordinate and send to the alternate email-id [12]. In 5th attempt phone will get switch off, to switch on the phone user needs to visit phone gallery.

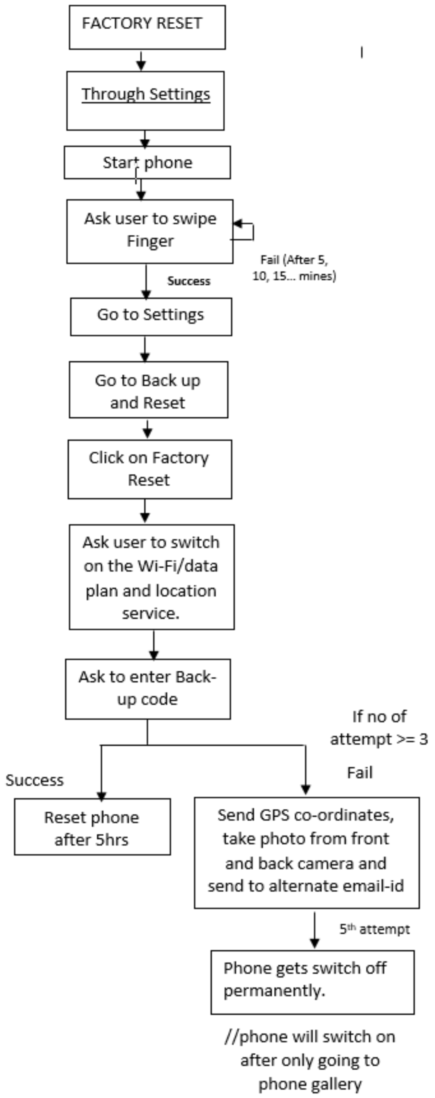
FACTORY RESET
Through Settings
Start phone
Ask user to swipe Finger
Fail (After 5, 10, 15… mines)
Success
Go to Settings
Go to Back up and Reset
Click on Factory Reset
Ask user to switch on the Wi-Fi/data plan and location service.
Ask to enter Back-up code
If no of attempt >= 3
Success
Fail
Reset phone after 5hrs
Send GPS co-ordinates, take photo from front and back camera and send to alternate email-id
5th attempt
Phone gets switch off permanently.
//phone will switch on after only going to phone gallery

Figure 3: Mechanism to Secure against Factory Reset through Settings.

During hard reset, the user requires to switch off the phone, press and hold home and volume up button for few seconds further pressing power button until phone vibrates, the android logo appears and options are displayed and with help of volume down button factory reset option is selected. The user will require turning on Wi-Fi/data plan and location service and passing biometric fingerprint authentication and further enter correct back-up code within 3 attempts allowing phone to reset after 5hrs. At same time front and back camera will capture the image, GPS co-ordinate and send to the alternate email-id till 4 attempts of biometric fingerprint authentication, in the 5th attempt phone get switch off, phone will switch on only when user visit gallery.

Thus we conclude, factory reset in either of case is only possible when user pass biometric authentication and knows the back-up code, thief cannot reset the device because of lack of fingerprint and back-up code. Also we get the position of stolen cell phone and picture of thief.

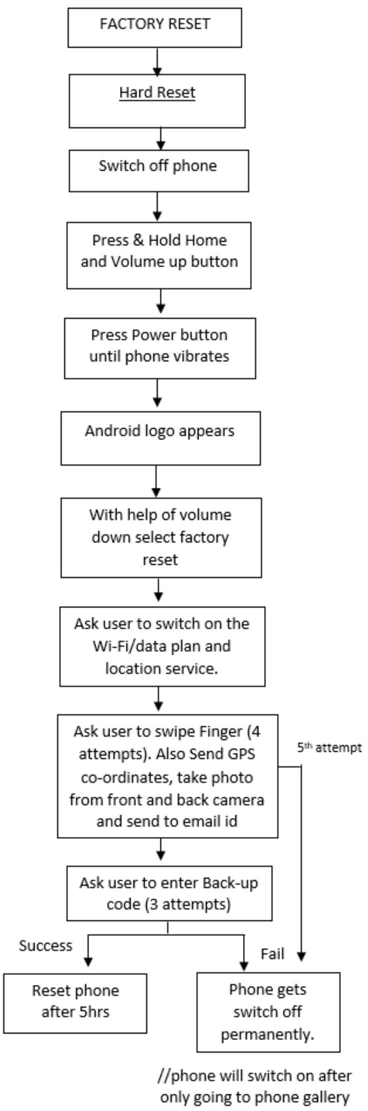
FACTORY RESET
Hard Reset
Switch off phone
Press & Hold Home and Volume up button
Press Power button until phone vibrates
Android logo appears
With help of volume down select factory reset
Ask user to switch on the Wi-Fi/data plan and location service.
Ask user to swipe Finger (4 attempts). Also Send GPS co-ordinates, take photo from front and back camera and send to email id
5th attempt
Ask user to enter Back-up code (3 attempts)
Success
Fail
Reset phone after 5hrs
Phone gets switch off permanently.
//phone will switch on after only going to phone gallery

Figure 4: Mechanism to Secure against Hard Reset

3.4 Phase three: Generation of Authentication code

During the registration of new Fingerprint in figure 2 the user requires to provide authentication code, a random number of length six [13].

Algorithm works in two Stages. Stage 2 will generate require authentication code and switch to stage 1 where user is allowed to register new fingerprint when counters and authentication code matches.

At stage 1 initially counter from both phase are compared, counter of stage 1 c1=1 and counter of stage 2 c2 becomes 1 only after generation of authentication code ac_g allowing authentication code to generate only from stage 2 and not from any other means of mathematical calculation. When entered authentication code ac_u matches to generated code ac_g user is allow registering a new fingerprint.

Steps of Algorithm in stage 1:

```
1. Set counter c1=1
2. Enter generate authentication code $ac_u$
3. Compare if counter c1= c2 go to step 4 else print invalid
   authentication code
4. Compare if $ac_u$= $ac_g$ allow user to register new fingerprint
   and go to step 5 else print invalid authentication code
5. Ask user to enter key for next use and go to step 1
```

In stage 2 user enter a key i.e. key (value 1 to 179 since sine is only positive in this range as per our formula need) of length 3 which user entered in previous session of generation of authentication code. System compares both the input and stored key. When there is match user is authenticated as genuine user else no authentication code will be generated for stage 1. In algorithm some part of code is generate using a formula [2]. Time plays an important part in generating authentication code as code will change for each minute and second. Authentication code will be length of 6 and each time variable length code will be generate because of step 6-10 in following algorithm. The code will be valid for one min and allow user to switch between windows and enter code at stage 1 window.

Steps in Algorithm in stage 2:

```
1. Set counter c2= 0
2. Enter key u
3. Compare store key s with u, if success go to step 4
   else got to step 2
4. Calculate $X_{n+1} = X_n^{\log(\sin(X_n))}$ [2]
5. Extract the fraction part from output of Xn+1
6. At time t(min, sec)
   $\frac{\min + \sec + \sum u}{(2 + lengthofu)} = Y$
7. If Y > 6 then keep on dividing Y with 2 till Y =< 6
   Then checks if Y is integer if yes go to step 10 else
   go to step 8
   Else if Y =< 6 go to step 9
8. (a.b), represent a=whole number, b= fraction part.
   Perform $p= a^b$; is p's first digit< 6 then extract 1st
   digit(Y) else set Y=6 go to step 10
9. Checks if Y is whole number if it's a whole number
   go to step 10 else go to step 8
10. Extract Y number of digits from fraction output of
    $X_{n+1}$ i.e. authentication code $ac_g$
11. Increment the counter c2
12. Make $ac_g$ valid for one minute
13. If within one minute $ac_g$ is used go to step 1
    Else Destroy $ac_g$ value
```

4. Conclusion

In this paper, a strong authentication mechanism after mobile theft and before performing Factory Reset is proposed which will secure the sensitive data on the device. Factors like back-up code which perform work of dual authentication in every step in proposed mechanism, security question which act as security for back up code, and alternate email-id where thief images will be send, provide strong security to system and give better security as compared to existing security in android devices. The proposed authentication code algorithm allowing user to register new fingerprint will help to discourage the use of different sections in mobile device which require biometric authentication and make device useless and discourage mobile theft since hacker cannot use artificial fingerprint for daily use of device.

References

[1] Kataria, Adhyaru, Sharma, Zaveri, "A survey of automated biometric authentication techniques" In Proceedings of the IEEE Nirma University International Conference on Engineering (NUiCONE), pp. 1-6, 2013.
[2] Ritu, Sonam, Vinita, Vishakha, "VRS algorithm A Novel Approach to Generate Pseudo Random Numbers" In Proceedings of the IEEE International Advance Computing Conference (IACC), pp. 7-10, 2014.
[3] Donny, Liza, Lei, "Preventing Cell Phone Intrusion and Theft using Biometrics" In Proceedings of the IEEE Security and Privacy Workshops (SPW), pp. 173-180, 2013.
[4] Charles Severance. "Anil Jain: 25 Years of Biometric Recognition" IEEE Journal Computer, pp. 8-10, 2015.
[5] Weizhi Meng, Wong, Furnell, Jianying, "Surveying the Development of Biometric User Authentication on Mobile Phones" Communications Surveys & Tutorials, IEEE, pp. 1268 – 1293, 2014.
[6] Zhiling, Yufei, "Understanding User's Behaviors in Coping with Security Threat of Mobile Devices Loss and Theft" In Proceedings of the IEEE 45th Hawaii International Conference on System Sciences (HICSS), pp. 1393 – 1402, 2012.
[7] R. Schwamm, N. C. Rowe, "Effects of the factory reset on mobile devices," in The Journal of Digital Forensics, Security and Law (JDFSL), VOL 9, NO 2, pp. 205-220, 2014.
[8] L. Simon, R. Anderson, "Security analysis of android factory resets" n 3rd Mobile Security Technologies Workshop (MoST) IEEE Computer Society Security and Privacy Workshops, 2015.
[9] Laurent, Ross, "Security Analysis of Consumer-Grade Anti-Theft Solutions Provided by Android Mobile Anti-Virus Apps" Mobile Security Technologies (MoST) IEEE Computer Society Security and Privacy Workshops, 2015.
[10] Nseir, Hirzallah, Aqel, "Issues with Various Security Threats on Mobile Phones" In Proceedings of the IEEE Information and Communication Technology (PICICT), pp. 37 – 42, 2013.
[11] Yamazaki, Dongju Li, Isshiki, Kunieda, "SIFT-based algorithm for fingerprint authentication on smartphone" In Proceedings of the IEEE Information and Communication Technology for Embedded Systems (IC-ICTES), pp. 1 – 5, 2015.
[12] Khan, Qureshi, Qadeer, "Anti-theft application for android based devices", In Proceedings of the IEEE Advance Computing Conference (IACC), pp.365 – 369, 2014.
[13] Ankur, Divyanjali, Bhardwaj, "A dissection of pseudorandom number generators", In Proceedings of the IEEE 2nd International Conference on Signal Processing and Integrated Networks (SPIN), pp. 318 – 323, 2015.