International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1, October, 2019

CEIR based Smartphones Anti-stolen System: SASSCEIR

Arun Kumar Bediya, Rajendra Kumar

Abstract: ***Mobile stolen has become a big problem all over the world. International Mobile Equipment Identity (IMEI) is a unique number which used to identify mobile device throughout the world. An IMEI is to be made non editable number which cannot be reprogrammed. Central Equipment Identity Register (CEIR) is systems that registers the stolen/theft mobiles and update all TSP's local EIR with blacklisted IMEI. Many countries have enabled CEIR system to terminate mobile stolen problem. Despite of many features CEIR is not able to stop working of smartphone on Wi-Fi networks. Current CEIR system block the mobile devices by placing stolen devices in blacklist hence telecom services get disabled for blacklisted mobiles. This paper represents capacity of CEIR deployment in telecommunication network system and demonstrates the existing problem in CEIR. This paper also focuses on our proposed solution SASSCEIR, for complete blocking of smartphones.SASSCEIR will help to alleviate the stealing of smartphones by making them completely futileto use. We have performed test cases to analyze SASSCEIR concept by developing android based apps prototype of SASSCEIR and mobile side TESTSASSCEIR app to communicate with SASSCEIR app.***

Keywords: Smartphones Anti Stolen, SASSCEIR, Mobile Theft

I. INTRODUCTION: NEED OF SMARTPHONES ANTI-STOLEN SYSTEM

Smartphones have become the necessity of human life now a day because it provides the simplest way of communication. Smartphones are enabled with internet accessing facility that powered the mobile device to the next level email, voice messages, videos, picture and shopping are made easy via using various applications installed in smartphones. Smartphones turned human life easier in various prospects. Today's smartphones stores consumer information like credit cards details, connectivity with banks, ATM and many private data of consumer etc.

It is very difficult to recover mobile if mobile is stolen or misplaced. The number associated with the mobile is connected to various applications such as banks, credit cards and many financial components. Though the same mobile number i.e. Mobile station international subscriber directory number (MSISDN) can be recovered from telecom service provider (TSP) but recovery of same mobile device is very rare and arduous.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Arun Kumar Bediya*, Center for Development of Telematics, New Delhi- India, arunbediya@gmail.com
Dr. Rajendra Kumar, Department of Computer Science, Jamia Millia Islamia, New Delhi-India, verma_rajk@yahoo.com

Stolen or lost mobiles can also be used in illegal activities i.e. terrorists attack, kidnapping, blackmailing, identity frauds etc. It is necessary to have a system which can block all services to lost/stolen mobile so that it cannot be used for any malicious activities. Availability of system like this will also de-motivate theft activity. Many countries like Australia, France, Philippines, Poland, Turkey , Pakistan and UK has enabled mobile anti stolen system to block stolen/lost of mobile devices[1].

An IMEI that is an identity code associated with all the GSM handsets. Each Telecom service provider (TSP) maintain a local Equipment Identity Register (EIR) of their own subscribers, EIR is a system which maintain a database that comprise of all the IMEI/ESN numbers of the mobile devices of all their subscribers that are allowed to work and all the subscriber that are marked banned due to reported as stolen/lost i.e. blacklisted. TSP checks its local EIR whenever a mobile switched-on and in each 4 hours. Unfortunately all the TSPs maintain their own blacklist but it is not shared and synchronized among the all TSPs and this is the reason that lost/stolen mobile device works perfectly in different TSP.

At the point when the handset is connect to a specific system, MSC ask for IMEI of that handset and after that it is sent to EIR for further approval process. If IMEI is not found in local EIR blacklist i.e. the mobile devices are not blacklisted then only the device will be able to use telecom services.

Dong Hui, Huan Lei discussed importance of EIR system based mobile security methods to control on smuggling and theft [2]. Gao Yongqing , Zhou Chunlai, Shang Dan presented mobile anti theft method based on locking SIM card that can protect user information and prevent mobile to use by other persons [3]. Graham Farrell proposed method and seeking for government action for making law, regulation and codes of conduct for stolen/lost mobile to avoid crime related to mobile misuse and enable tracking of stolen mobile [4]. To implement CEIR in India the responsibility of TSP's will play most important role. TSP's responses on CEIR are positive in terms of blocking of mobile phones but additional load on their network and TSP's are deliberate to their customer base [5].

The rest of this paper is organized as follows. In Section II, we give a brief overview of the standard CEIR system architecture and basic elements of CEIR. Section III describes the limitations of existing CEIR and problem which still exists in CEIR system. In Section IV, Introduction of the proposed solution of the provable

concept of Smartphones Anti-Stolen System based on Central Equipment Identity Register (SASSCEIR) and its implementation authenticate mobile device. In Section V testbed of SASSCEIR and experiment with SASSCEIR, results are demonstrated and the paper is concluded with a summary in Section VI.

II. CEIR MOBILE ANTI-STOLEN SYSTEM

The current model is just handling the IMEI numbers in the EIR database of particular cellular network to which the subscriber is latched. If the mobile subscriber lost mobile device, its service provider i.e. TSP blocks the IMEI of that device in its own network to make device futile and can't be abused by the criminal. But criminal is able to change the SIM card with SIM card of other TSP which has not blocked this device, consequently giving the criminal an approved access to the network. These issues were persistently occurring before and telecom regulatory authority watched these restrictions with the current model and looking to another solution i.e. central equipment identity register (CEIR) system[1].

CEIR is meant to block stolen reported and lost mobile devices in all over the country. Fig. 1 represents the basic architecture of CEIR system. It also explains how TSP's communicates with CEIR system to authenticate IMEI before providing any telecom service. TSP will deactivate all services on blacklisted mobiles as it is illegal to provide telecom network services to blacklisted mobile.

A. Lost/Stolen Registration: This facility can be available at LEA/TSP/Police i.e. a legal organizational authority. Mobile device owner has report lost/stolen at LEA/TSP with all proofs of ownership like invoice, last bill etc. LEA/TSP register using registration module, the IMEI of the device will be registered in CEIR system which store IMEI in CEIR database.

B. CEIR Database: CEIR database keep all registered IMEI of lost/stolen devices and further blacklist can be generated. Database is updated each time when a new lost/stolen is registered.

C. TSP: TSP operators plays a vital role in CEIR system, when mobile devices switched on TSP get request from the mobile to provide network, TSP afterword check authenticity of requested mobile IMEI in its local EIR. Local EIR contains the blacklist of IMEI provided by CEIR to the TSP. When TSP confirmed authenticity of IMEI it start providing telecom services to requested mobile otherwise TSP block all kind of services for the mobile.

D. Blacklist: Blacklist is the list of IMEI which are reported lost/stolen. Blacklist is generated by CEIR and periodically update to all TSP'[1, 6].

E. Greylist: Greylist is the list of IMEI which are under observation and keep continue to use telecom services.

F. Whitelist: Whitelist is the list of IMEI which are legal to access the telecom network services.

Once mobile device IMEI is registered with CEIR database, system update corresponding list black/grey and if IMEI is updated in blacklist, CEIR send blacklist to all TSP's and TSP's updated its local EIR blacklist, therefore each TSP block all services to that mobile device i.e. the lost/stolen mobile cannot be use by anyone for calls, messaging etc.crime can be control related to mobile fraudulent like stolen, misuse of mobile phones in financials, terrorist etc. [7]. Cloned mobile receive less signals that alleviate TSP's reputation therefore CEIR is beneficial for TSP's perspective as well [8].

Limitation of CEIR

CEIR is capable to successfully block lost/stolen mobile devices as blacklisted mobile not aspire to use telecom services on the mobile. Lost/stolen mobile is still able to works in WiFi networks to use internet services via mobile applications such Whatsapp, Facebook, Google, Instagram and many more. Mobiles that are blacklisted by CEIR are still works for E-commerce, bill payment, banking and many other applications because mobile application does not required telecom services as it is not directly connected to TSP's networks. Thief can also make voice call using many android apps like Whatsapp, Skype, Imo, Google duo, hangout etc. These apps allow user to make calls and messaging and therefore mobile becomes completely useful even though mobile is blacklisted by all TSP's.

fig.1 CEIR Limitation: Blacklisted mobiles in WiFi

Fig. 1 describes how a lost/stolen mobile can work without using TSP's services. This can be done in easy steps. 1. Connect mobile device with WiFi router. 2. WiFi router connect device with Internet. 3. Install android/ios apps in mobile device. 4. Apps are now can be connect to internet. 5. Now thief can perform any operation of mobile i.e. browsing, chats, calls etc.

III. SECURITY ASSESSMENT

If we consider that mobile stolen report is registered and it is blacklisted by CEIR to all TSP's, thus SIM get blocked and no telecom service will be enabled.

To achieve the similar hypothesis we removed the SIM card from testing mobile device. Now we can consider it as the practical scenario of mobile lost/stolen. We connect the test mobile device with private Wi-Fi network and performed some test case on many major e-commerce mobile apps installed in the to elucidate the concernment of the existing problem. Some of them are listed below:

1. Amazon pay: Mobile recharge, bill payment and make order using wallet balance available in the Amazon account.
2. Flipkart: Mobile recharge, bill payment and make order using wallet balance available in the Flipkart account.
3. Paytm: We perform the Paytm balance transfer, mobile recharges and various bill payments on the same mobile device using wallet balance available on the Paytm account.
4. Myntra: Make buy order using Myntra credits available in account, cancelled existing orders of the account.
5. Freecharge: Mobile recharge, bill payment using wallet balance.

Mobile wallet applications are easy to use, and in future of all banking and transactions would be performed using them, but mobile apps are not secure enough to handle security issues similar to the test cases performed in our experiment. Financial transaction performed using mobile apps must be safe and secure[9]. Other money transfer mobile apps based on Unified Payments Interface (UPI) like BHIM, GoogelPay, PhonePay etc. that transfer money bank-to-bank checks the SIM (Subscriber Identity Module) card availability in the mobile thus money transfer from mobile without SIM from UPI apps is not possible.

There are many anti theft and device tracking model available and proposed[10][11][12][13][14] but complete solution is still not available. Mobile theft still make mobile usable and therefore the purpose are not delivered even after registration and blacklisting mobile IMEI in TSP's with CEIR. Thus it is clear that CEIR is not sufficient to establish the purpose i.e. making mobile devices unserviceable after lost/stolen. It is needed to strengthen the CEIR by facilitating more functionality or providing some other solution that can handle these issues. We are proposing solution which overcomes to determine such problems.

IV. PROPOSED SOLUTION: SASSCEIR

Complete blocking of mobile can be considered if subscriber report theft/stolen mobile device and handset become futile i.e. mobile cannot be use for any kind of work. It is found that if mobile device reported stolen and registered in CEIRits all kinds of telecom services will be stopped but still it can perform various tasks using Wi-Fi network and mobile apps discussed in section III. Smartphones Anti-Stolen System based on Central Equipment Identity Register (SASSCEIR) is a java based application which maintains the blacklist of IMEI generated by CEIR i.e. all new IMEI added in CEIR blacklist it must be updated in SASSCEIR blacklist. SASSCEIR blacklist can be updated using SOAP web service periodically. Thus CEIR is the backbone system for SASSCEIR. This application can be used by mobile manufacturer or mobile app developerso that stolen of mobiles devices can be avoided. To utilize SASSCEIR, Mobile manufacturer have to make an inbuilt function to check the validity of mobile by sending its IMEI to SASSCEIR. SASSCEIR check receiving IMEI validity from blacklist and return the authenticity result for IMEI to mobile inbuilt function, so as mobile function can decide that mobile should work properly or notify user that mobile is not authentic or blacklisted. Similarly mobile apps can also check authenticity of mobile by sending IMEI.

There are two prerequisites for SASSCEIR to function appropriately to block mobile completely.

1. Legitimate mobile manufacturer to check IMEI authenticity from SASSCEIR in a similar fashion that TPS's authenticates the IMEI of mobile device with CEIR.

2. Periodic update of blacklist from CEIR is mandatory to perform SASSCEIR appropriately i.e. blacklist at both sides must be synchronized.

Mobile inbuilt function connects SASSCEIR via web service to check IMEI authenticity. If above two requirement is considered SASSCEIR will proficiently block mobile to access internet facility and stolen of mobile will not be useful for anyone thus stolen practices can be ended completely.

fig.2 SASSCEIR achitecture - proposed solution

Fig.2 demonstrates the functions of SASSCEIR. Following are steps to perceive SASSCEIR work flow. 1. Connect mobile device with Wi-Fi router. 2. Wi-Fi router connect device with Internet. 3. Mobile call to SASSCEIR with IMEI. 4. Open mobile apps. 5. If mobile is authentic i.e. not found in blacklist of SASSCEIR, mobile will work as properly and apps are now can connect to internet. 6. Now only valid mobile devices apps can works properly.

```
/* Algorithm for mobile side functionality */
/* Mobile inbuilt function to checks IMEI
authenticity */

fetch device imei;
If(checkImeiAuth(imei));
{
        work properly();
}
else
{
alert("This device is not authentic");
exit(); //mobile should not connect to
internet.
}
```

```
/* Algorithm for SASSCEIR side functionality */
/*      SASSCEIR function */

// receiveimei from the callee mobile
function checkImeiAuth(Argument IMEI)
{
        define authflag = true;
        search IMEI in database;
        If(found );
            set authflag false;
        else
            return  authflag;
}
```

It is presumed that blacklist is provided to SASSCEIR from CEIR. For testing two android based apps is developed. 1. SASSCEIR (prototype version). 2. TestSASSCEIR app that performs some functions and uses internet services like Whatsapp, to hypothesis the practical scenario. TestSASSCEIR app included a function that check IMEI authenticity of mobile in which it runs before performing any task. Whilelaunching TestSASSCEIR app firstly it checks the authenticity of IMEI of mobile device by sending IMEI to SASSCEIR application. Once SASSCEIR receive IMEI for authentication it examines received IMEI in blacklist, if received IMEI is found in blacklist, SASSCEIR set AuthFlag as 'false' which means the sender IMEI is blacklisted i.e. it is reported stolen and TSP services are stopped on this device.On the other hand if received IMEI is not found in SASSCEIR blacklist it send AuthFlag as'true' which means the sender IMEI is not blacklisted and all services should be run on this device.

TESTCASE 1: Open the TestSASSCEIR app in mobile that is already blacklisted. So it will receive authflag as 'false' from SASSCEIR hence TestSASSCEIR gives an alert message "This device is not authentic" and TestSASSCEIR will be closed automatically.

TESTCASE 2: Open the TestSASSCEIR app in mobile that is not blacklisted. TestSASSCEIR app will work perfectly without any alert message. This is because TestSSACEIR received authflagas 'true' i.e. mobile is not blacklisted.

Experiments outcome showsSASSCEIR is able to block internet services for a stolen/lost reported smartphone i.e. smartphone will be authenticate IMEI to avoid its misuse for criminal activities as well as for general functionality mentioned in section III. We scrutinized 100 smartphones and installed TestSASSCEIR app and performed above test cases by adding and removing their IMEI in testing blacklist. As a result we found that presented concept of SASSCEIR application works as per expectations and it is able to help lost/stolen smartphones to make completely futile, it will also make stolen/theft of mobile devices uninteresting to thieves.

VI. CONCLUSION AND FUTURE WORK

This paper presented SASSCEIR functionality, its development and test cases with results. SASSCEIR is able to block mobile device completely after reporting lost/stolen in CEIR. This can also lead to discourage for thefts/criminals and cyber crime and it may declined.

A law needs to be passed by authorities for mobile manufacturer to check IMEI authenticity before performing any tasks as similar TSP's authenticates IMEI of each mobile.Both CEIR and SASSCEIR can also helps to track the mobile in real time once reported stolen by smartphones users and it may lead to recover the lost/stolen smartphones. Cloning/duplicating of IMEI is also a serious predicament in terms of blocking of mobile devices as multiple devices can be cloned with same IMEI.

Finally we conclude that both CEIR and SASSCEIR are able to completely block the stolen/lost mobile phone and insure it that mobile will be non-usable once it is reported stolen in CEIR. For future work we can enableSASSCEIR to identify the cloned/duplicates IMEI and block the cloned device that is reported stolen.

REFERENCES

1. TRAI, *TRAI Consultation Paper on Issues relating to blocking of IMEI for lost /stolen mobile handsets*. Telecom Regulatory Authority of India: New Delhi, 2010. p. 1-14.
2. Hui, D. and H. Lei. *EIR Based Mobile Communication Network Security Technology*. in *2011 Third International Conference on Multimedia Information Networking and Security*. 2011. IEEE.
3. Gao, Y., C. Zhou, and D. Shang. *A smart phone anti-theft solution based on locking card of mobile phone*. in *2011 International Conference on Computational and Information Sciences*. 2011. IEEE.
4. Farrell, G., *Preventing phone theft and robbery: the need for government action and international coordination.* Crime science, 2015. **4**(1): p. 4.
5. TRAI. *TELECOM REGULATORY AUTHORITY OF INDIA - Highlights of Telecom Subscriptionm Data as on 31st January, 2015,"*. 2015 [cited DATA 18 / 2015].
6. Whitehead, S., et al., *In safe hands: a review of mobile phone anti-theft designs.* European Journal on Criminal Policy and Research, 2008. **14**(1): p. 39-60.
7. Mailley, J., *The prevention of mobile phone theft: a case study of crime as pollution; rational choices and consumer demand*. 2011, © JC Mailley.
8. Loureiro, A.J.F., D. Gallegos, and G. Caldwell, *Substandard cell phones: Impact on network quality and a new method to identify an unlicensed IMEI in the network.* IEEE Communications Magazine, 2014. **52**(3): p. 90-96.

9. Darvish, H. and M. Husain. *Security analysis of mobile money applications on android*. in *2018 IEEE International Conference on Big Data (Big Data)*. 2018. IEEE.
10. Kwon, Y., et al. *An Enhanced Java-Based Mobile Device Theft Response System*. in *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. 2015. IEEE.
11. Yoon, S., Y. Jeon, and J. Kim. *Mobile security technology for smart devices*. in *2015 International Conference on Information and Communication Technology Convergence (ICTC)*. 2015. IEEE.
12. Dar, M.A. and J. Parvez. *A live-tracking framework for Smartphones*. in *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*. 2015. IEEE.
13. Ba, Z., S. Piao, and K. Ren. *Defending against Speaker Fingerprinting Based Device Tracking for Smartphones*. in *2017 IEEE Symposium on Privacy-Aware Computing (PAC)*. 2017. IEEE.
14. Martinez, J.J.L. and N. Widjaya, *Architecture for Lost Mobile Tracker Application*. International Journal of e-Education, e-Business, e-Management and e-Learning, 2012. **2**(3): p. 197.

AUTHOR PROFILE

Ar**un Kumar Bediya received** B.E degree in computer science and Engineering from SGSITS, in 2005 and completed M.Tech. (Computer science) from MANIT, Bhopal in 2008. He joined Center for Development of Telematics (C-DOT), New Delhi in 2008 and working as senior research engineer. He is also pursuing PhD from JMI, New Delhi. He has a wide research experience in the field of computer science. He has published various research papers in the conferences of international/national repute.

Dr. Rajendra Kumar is presently working as Assistant Professor in the Department ofComputer Science, Faculty of Natural Sciences, Jamia Millia Islamia (Central University), New Delhi-110025, INDIA. He has an excellent academic background with a very sound academic and research experience. He has published various research papers in the conferences of international/national repute. His research interest includes: cyber security, Cloud Security and Privacy, Big DataAnalytics, Data Mining, IoT, Software Security, Requirements Engineering, Security Policies and Standards, Software Engineering, Access control and Identity Management, Vulnerability Assessment etc.