PROCEEDINGS OF SCIENCE

Research on Safety Mobile Terminal and Judging Credibility Method Based on Call Tracking

Jun Xu [1]

Safety Training Department, North China Institute of Science and Technology
Langfang, 065201, China
E-mail: jtcembx@sina.com

Through the user's behavior with call tracking, we propose a self-destruction mechanism of mobile equipment based on the chip materials. The system uses the self-destruction chip to destroy the untrusted mobile terminal remotely with a trusted computing algorithm. This method has a certain application prospect in the the special environment with high security requirements. The experimental results show that the time cost of the large data detection algorithm is very small and the call tracking can be used to decide whether the mobile is fraud or not.

CENet2017
22-23 July 2017
Shanghai, China

[1]This work was supported in part by the Foundation Items: The National Natural Science Foundation of China（No.: 61472137）, the Fundamental Research Funds for the Central Universities (No.: 3142015022) ,the Key Research Program of Qinhai Prvince（No.: 2016-SF-130 and Hebei Engineering Technology Research Center for IOT Data acquisition & Processing and The National Natural Science Foundation of China (No.: 61304024).

PoS(CENet2017)041

1.Introduction

Although all kinds of network security of mobile communication systems have been considered in the establishment of the network, there are always a variety of problems.

Trusted Computing Platform Alliance proposed the idea of the trusted computing to protect the security of computing terminals in 1999. Trusted Computing Group officially released the new TPM2.0 in 2013 [1-3]. The study on the strong safety environment of the operating system is many research achievements and theoretical articles[4-8] . But they have some shortcomings such as failing to solve the mobile access control terminal. According to the report of the IEEE Spectrum, the magazine of ADVANCED MATERIALS, the researchers of Saudi King Abdullah University of science and technology said that the self-destruction mechanism depending on the expandable polymer layer can be used as the new chip material. The self-destruction chip using the new material will be the ultimate way to solve the equipment security problem because the self-destruction can be triggered in the terminal side or by network. To use the self-destruction chip, we should decide whether the mobile terminal is safe or not. The online business tracked by call trace will be described in other papers.

2.Trusted Mobile Terminal Architecture Based on the Self-Destruction Model

In Figure 1, the based band processor-ARM11 is responsible for baseband and high-level protocol stack processing. ARM9 is the application processor which runs the main application layer software. Bio_Featrue_Mo module for fingerprint or iris biometric identification is responsible for verifying the identity of the user information. The self-contruction module for the self-destructive detection controls ARM9, ARM11 and the memory for self-destruction.

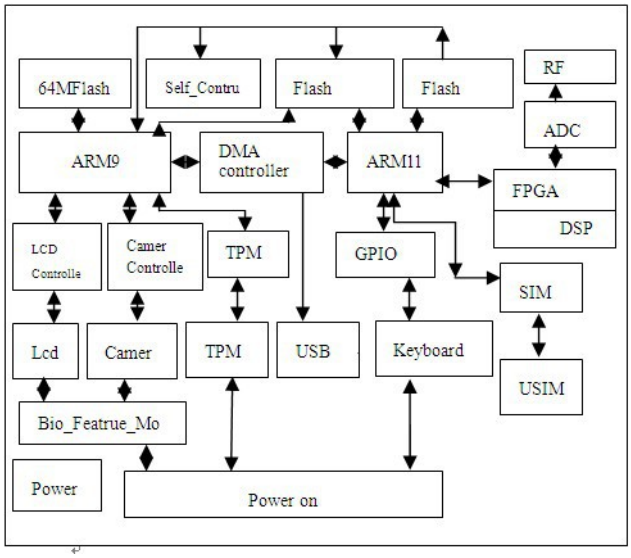

Figure 1: Security Architecture of Trusted Mobile Terminal

TrustZone divides hardware and software resources into two execution environments: the security environment and the general environment. Each execution environment has its own system software and application software with its own memory area and peripheral equipment.

3.Call Tracking

This paper describes the implementation of the UE call tracking illustrated in Fig.2. UE trace is unknown to the NodeB and UE. In the RANAP signaling process, when the UE is a

completed access to CN after the initial direct transmission (INITIAL UE MESSAGE process is completed), CN can start the RNC side of the tracking process with the RANAP signaling CN INVOKE TRACE. RNC processes RANAP signaling module first after receiving the message. It is immediately ready for the tracking process of the UE, and will notify the relevant processing module as soon as possible to handle the event of other signalings so as to track the processing of UE. At the same time, it sends the MM_CNInvokeTrace_ind to RNC detection module, notifying RNC detection module to receive and process data. After receiving the MM_CNInvokeTrace_ind message, RNC detection module needs to reply to the message MM_CNInvokeTrace_Cfm and be ready to receive and process the data.

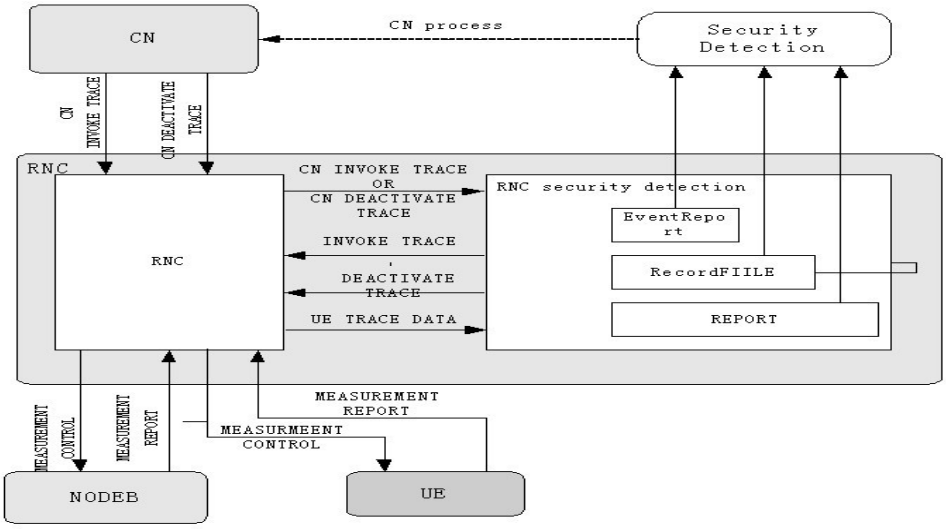

Figure 2: UE Tracking

If the same UE is simultaneously initiated by IMSI and IMEI tracking, the RNC receives CN DEACTIVATE TRACE to determine which tracking process should be stopped without affecting the other process. When the UE connection with the CN is released, for example, the CN initiates the Iu connection release or the UE is relocated to other RNCs that caused the release, the tracking process is immediately aborted by Iu. After the UE relocation is successful, the CN side can restart the request on the new RNC side as needed. CN's INVOKE TRACE message includes the following items:

Trace Type: data for 8bits, illustrating the tracking of the project.

8	7	6	5	4	3	2	1
Priority Indication	For future expansion (Set to 0)	BSS Record Type		MSC Record Type		Invoking Event	

Table 1: Trace Type

Invoking Event: for MSC, when the event in the project is agreed upon, it is necessary to start the trace. The events of NAS for RNC layer are not visible.

Bits		Invoking Events
2	1	
0	0	MOC, MTC, SMS MO, SMS MT, SS, Location Updates, IMSI attach, IMSI detach
0	1	MOC, MTC, SMS_MO, SMS_MT, SS only
1	0	Location updates, IMSI attach IMSI detach only
1	1	Operator definable

Table 2: The Definition of Invoking Event

MSC Record Type: agrees to generate the type of tracking record CN, different types of records in the tracking record.

BSS Record Type: relative to the 3G mobile communications, can be seen as the definition

of the type of RNS records, different types of records in the tracking agreement.

Priority Indication. 0 represents no priority, 1 represents high priority.

The security detection can be triggered in the RNC detection module when the RNC is launched in the UE tracking process. RNC detection module tracking object can be a UE that has established RRC connection with RNC, or a UE that has not yet established a RRC connection.

When the RNC detection module is required to initiate a UE trace, the message MM_ActUETrace_req with the UE logo (IMEI, IMSI, TMSI, P-TIMSI or UE Id) is sent out to activate the UE tracking process. The message with the UE logo is set in advance according to the need, for example, prior to know IMSI or TMSI of UE. When receiving the activation instructions from the RNC detection module, MM_ActUETrace _rsp first responds to messages, confirms the receipt of instructions, and then searchs the connected UE list. If it finds the specified UE of the activation message in the connected UE list, it immediately starts tracking processing in each sub module. If the tracking object is not in the connected UE list, it is required to check the accessing UE. Once the UE is found, the tracking object immediately begins tracking.

The RNC detection module initiating the UE tracking can always stop tracking the UE by the message MM_DeActUserTrace_req. Once the high-level signal receives the message, it immediately stops tracking the UE processing and responds to the message MM_DeActUserTrace_rsp.

RNC detection module to initiate the tracking of the message MM_ActUETrace_req should include:

1) operation identifier assigned by the RNC detection module: Since the RNC detection module can initiate multiple tracking, the message must be marked with a different tracking process so that RNC detection module and high-level signaling can distinguish themselves from different tracking operations.

2) Track type:The type of identifier to be tracked by UE specifies which of the UE's identifier is IMEI, IMSI or TMSI.

3) UE logo to be tracked: To meet different needs, UE logo can be set as IMSI, TMSI, PTMSI, IMEI.

The response message received by the RNC detection module should include the content as follows: operation identifier, time stamp, UE logo to be tracked, the identity of the cell that UE is tracking and status of the tracked UE. The current state of the UE is tracked (referring to the RRC connection state: IDLE, CELL_DCH, CELL_PCH, CELL_FACH, URA_PCH, GSM Connected Mode, GPRS Packet Transfer Mode).

4.Self-Deconstruction Decision Algorithm

In TD-SCDMA, Paging Type 1:UE and RAN have no RRC connection (in Idle mode) or use PCCH channel paging in the CELL_PCH or URA_PCH state. Type1 paging messages can be targeted at multiple UE.Paging Type2:UE and RAN have RRC connections, and in the CELL_DCH or CELL_FACH state, AM RLC mode paging is used in the DCCH channel A. Type 2 paging message is directed at a single UE, also known as UE paging.To use the paging type 1 or the paging type 2 is determined by RNC.

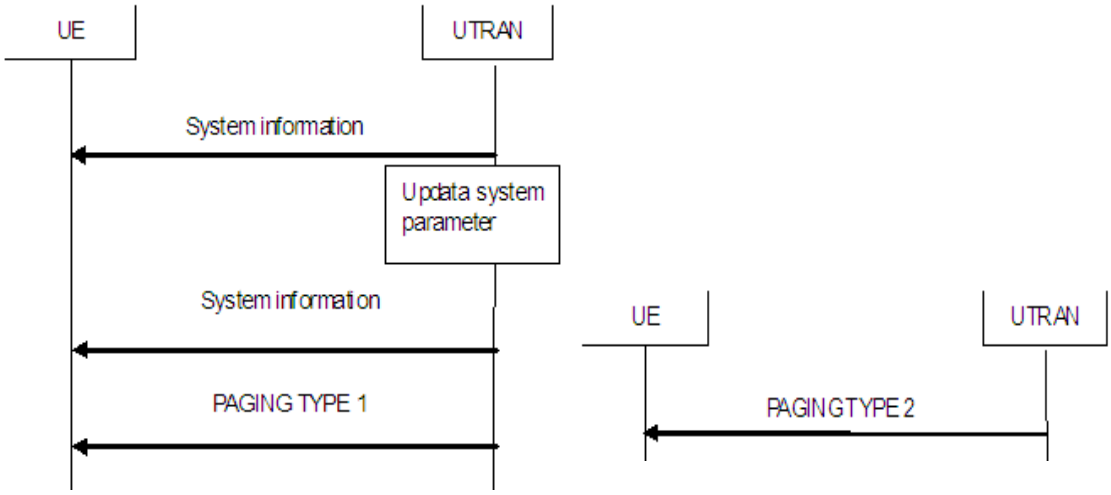

Figure 3: the Signalling Flow of the System

The algorithm of security detection is described as follows:

1）the user sets security level SEC collection and criticality safety level SECSelfDestruct under normal operating system environment;

2 ） sets security threats S_unSec under the normal operating system environment according to the mobile terminal operation safety detection;

3）executes a virus detection program to get virus security threats set Viruses_Sec in the general operating system environment down with;

4 ） if S_unSec - Viruses_Sec is in SECSelfDestruct, it will request the user to input fingerprint in the general operating system environment. If the fingerprint verification is passed, then turn to 10.

5 ） if the fingerprint verification is not passed, operating system environment sends the self-destruct request to network for security purpose and the self-destruction information is transfered to the network through the reserved field of RRC Connection Request.

6) the network starts the tracking process, depending on the type of CALL TRACE described in table 2 to get services such as MOC, MTC, SMS MO, SMS MT, SS, the Location Updates, IMSI attach, IMSI detach.

7) the network decides whether the mobile terminal has been attacked. Transfer the decision through the reserved field of rrcConnectionSetup message.

8 ） the mobile terminal needs the caller to verify the fingerprint. If the verification is passed, then turn to 10.

9）terminal receiving the network requirements for self-destruction operate as Fig. 1.

10）the common operating system environment of operation is to continue.

5. Experiment Result and Conclusion

Paper [9] used the call tracking to transmit fingerprint information by the reserved bytes of the message in the protocol. Paper [10] used the call tracking for network system testing.

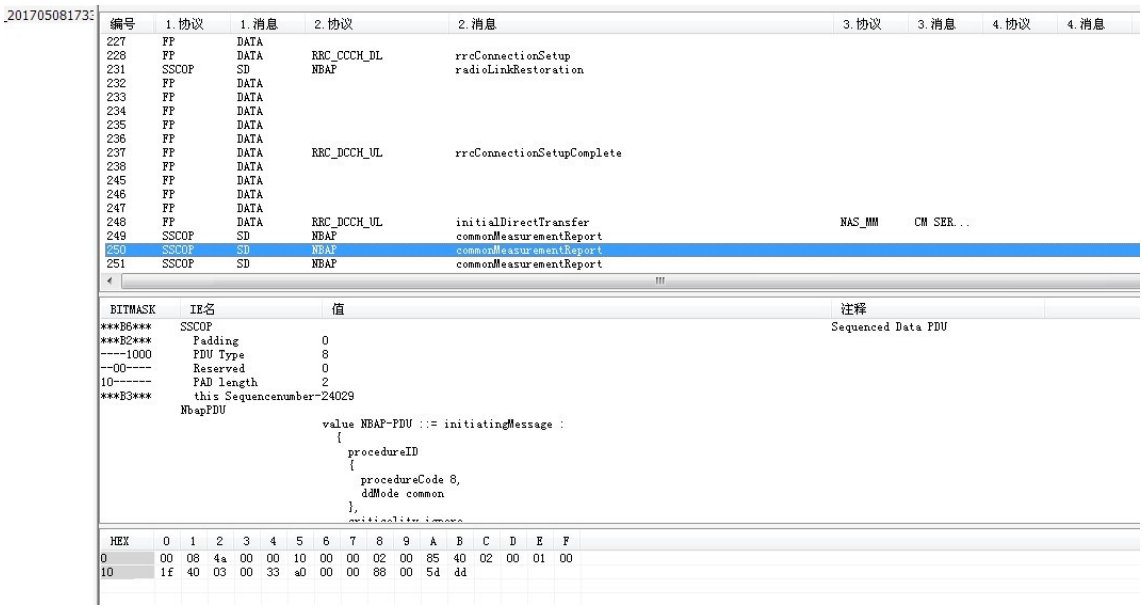

Figure 4: RRC CONNECTION SETUP COMPLETE in the Network

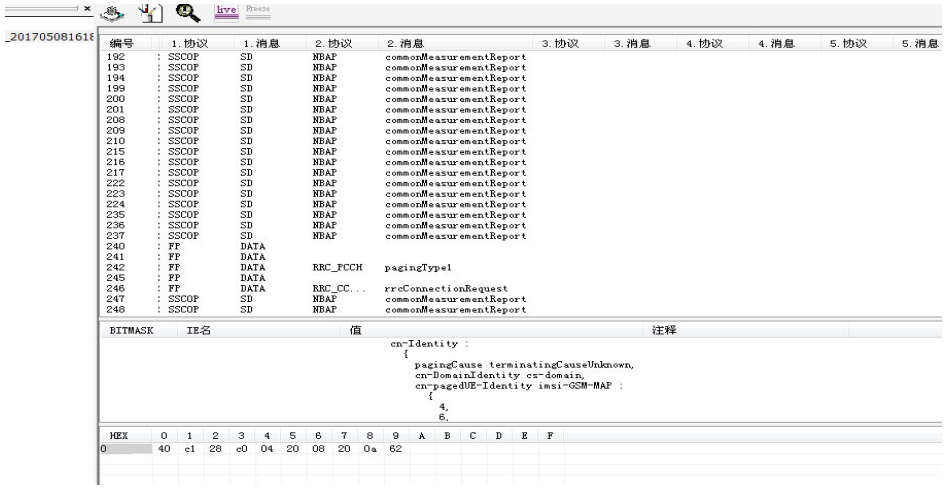

Figure 5: PagingType1 in the Network

Fig 4 shows the signaling of UE for RRC CONNECTION SETUP COMPLETE, which will transfer detection result to UE.

Procedure	RRC Connection	CM SERVICE REQUEST	AUTHENTICATION REQUEST
Time cost of standard protocol（ms）	3.527	1.248	2.305
Time cost of new protocol（ms）	3.535	2.583	3.736

Table 3: Time Cost of the System

Procedure	MOC, SMS MO, Location Updates, IMSI attach, IMSI detach	MOC, SMS MO
the probability of fraud user	0.8	0.3

Table 4:the Probability of Using a Business on Network in a Certain Period of Time

Fig. 5 shows the network paging the objective mobile terminal with IMSI. The RNC initiates the paging message PagingType1 (PCCH) / PagingType2 (FACH) to theUE in air interface. When the value of paging cause is terminating conversational call/terminating streaming call/terminating interactive call/terminating background call/terminating low priority

signalling, UEID of the paging UE is recorded and subsequent RRC Request messages is monitored on the RACH channel of the same cell. Table 3 shows that time cost of the new protol increased is very small. Table 4 shows the probability of using a business on the network in a certain period of time. It will combine with offline behavior to determine whether it is fraudulent or not.

In this paper, the system of tracking the mobile terminal business prevent users from denying the business of user behavior analysis. In the discovery of anomalies, the user needs to verify the fingerprint, and on the network side to initiate a request to destroy the mobile terminal. This method has a certain application prospect in the special environment with high security requirements.

References

[1] Trusted Mobile Platform Hardware Architecture Description. http://www.trusted-mobile.org/TMP_HWAD_rev1_00.pdf

[2] Trusted Mobile Platform Software Architecture Description. http://www.trusted-mobile.org/TMP_SWAD_rev1_00.pdf

[3] Trusted Mobile Platform Protocol Specification Document. http://www.trusted-mobile.org/TMP_Protocol_rev1_00.pdf

[4] Samuel AB, Don F, Virginie G, Franz H, Janne H, Milas F. *The trusted execution environment: Delivering enhanced security at a lower cost to the mobile market*. White Paper, GlobalPlatform, 2011.

[5] Jang J, Kong S, Kim M, Kim D, Kang BB. *SeCReT: Secure channel between rich execution environment and trusted execution environment.* In: Proc. of the 2015 Network and Distributed System Security Symp. (NDSS 2015). Internet Society, 2015. [doi: 10.14722/ndss.2015.23189]

[6] Li WH, Li HB, Chen HB, Xia YB. AdAttester: *Secure online mobile advertisement attestation using TrustZone.* In: Proc. of the 13th Annual Int'l Conf. on Mobile Systems, Applications, and Services (MobiSys 2015). ACM Press, 2015. 75–88. [doi: 10.1145/ 2742647.2742676]

[7] Yang B, Yang K, Qin Y, Zhang ZF, Feng DG. DAA-TZ: *An efficient DAA scheme for mobile devices using ARM TrustZone.* In: Proc. of the 8th Int'l Conf. on Trust and Trustworthy Computing (TRUST 2015). LNCS 9229, Springer Int'l Publishing, 2015. 209–227. [doi: 10.1007/978-3-319-22846-4_13]

[8] Zhang Yingjun,Feng Dengguo,Qin Yu,Yang Bo.. *A Trustzone-Based Trusted Code Execution with Strong Security Requirements.* Journal of Computer Research and Development,2015,52(10):2224-2238.

[9] Xu Jun. *Trusted computing mobile terminal application research based on biometric trusted access protocol*.Chinese Journal of Network and Information Security.2017,2(2): 66-76[DOI: 10.11959/j.issn.2096-109x.2017.00143]

[10] Feng Wei-guang.*The Analysis and design of an automatic call tracing system based on TD-SCDMA*.[D]Beijing:Beijing University of Post and Telecommunications,2011