

Trusted Computing-Based Security Architecture For 4G Mobile Networks

Yu Zheng, Dake He, Weichi Yu and Xiaohu Tang

School of Info. Science & Tech., Southwest Jiaotong University, Chengdu, Sichuan, China

zhyu_swjtu@163.com or cdzhengyu@yahoo.com.cn

Abstract

In this paper security requirements and security architecture for 4G systems are presented with the consideration of Trusted Computing (TC) for mobile equipment (ME). The security framework based on Trusted Mobile Platform (TMP) and PKI is proposed to provide a considerable robust platform for user's access to sensitive service and data in the scenario of 4G systems. Over this framework, with the combination of password and biometric identification (BI) as well as public key-based identification, an efficient hybrid authentication and key agreement (HAKA) scheme is presented to resist the possible attacks, particularly the attacks on/from ME. Compared with 3G architecture and other security schemes for 4G mobile networks, our architecture and corresponding HAKA is more secure, scalable and convenient to support globe mobility and capable of being employed to handle the complicated security issues in 4G mobile networks.

1. Introduction

The coming 4G wireless systems focus on seamlessly integrating the existing wireless technologies [1, 2], which raises further security vulnerabilities in turn [3]. On one hand, heterogeneous wireless networks have their own security domains and provide diverse security mechanisms and architectures. On the other hand, with the increasing functionality, the mobile equipments (ME) are becoming ever more powerful to open up a broader range of applications, and allow users to access secure service and sensitive data at any time and any place [4].

Conventionally, more attentions are paid on the side of access networks and air interface during the development of security scheme for current 2G/2.5G/3G systems [5]. However, the MEs still remain open to possible attacks and have to face more and more risks of virus, backdoor and losing devices carrying sensitive data etc [6, 7]. Though SIM (Subscriber Identity Model) or USIM (Universal Subscriber Identity Module) are employed in the wireless cellular networks to authenticate users, they can not ensure the computing platform on the ME is

trustworthy either. Moreover, the password-based identification is not secure enough to control user's access to ME/USIM and vulnerable to birthday attack or brute-attack.

Current 3G architecture can not be employed in 4G systems for its "weak points" [8], such as the unprotected link among wired parties, poor scalability of symmetric key-based authentication scheme and sometimes exposure of user's permanent identity over air interface etc. Some security schemes have been proposed in [8-10] for 4G mobile networks. However, none of them takes the security of ME into account, which will raise lots of security vulnerabilities and can not satisfy the security requirements of 4G systems discussed in section 2 in this paper.

This paper aims to take user and ME as two security factors into account during the analysis of security requirements and security architecture as well as security framework for 4G networks. With the combination of TMP and PKI the security framework and corresponding HAKA scheme are proposed to provide a considerable robust platform for mobile users and enhance the security of 4G systems.

2. Security requirements of 4G networks

According to the four kinds of security threats on 4G wireless networks, which are associated with attack on the ME/USIM, radio interface, radio network operator and IP bone networks separately, we list corresponding security requirements briefly as the follows.

(1) Security requirements on ME/USIM:

- It shall protect the integrity of the hardware, software and OS in mobile platform.
- It shall control access to data in ME/USIM.
- It shall to protect the confidentiality and integrity of data stored in the ME/USIM or transported on the interface between ME and USIM.
- It shall retain user's identity as privacy to ME.
- It shall prevent the stolen/compromised ME/USIM from being abused and/or used as an attack tool.

(2) Security requirements on radio interface and network operator:

- Entity authentication: mutual authentication between user and network shall be implemented to ensure secure service access and provision.

- Ensure confidentiality of data including user traffic and signaling data on wired or wireless interface.
 - Ensure integrity and origin authentication of user traffic, signaling data and control data.
 - Security of user identity: It shall protect user identity confidentiality, user location confidentiality and user untraceability.
 - Lawful interception: It shall be possible for law enforcement agencies to monitor and intercept every call in accordance with national laws.
- (3) Security visibility, configurability and scalability:
- The security features of the visited network should be transparent to user.
 - The user can negotiate acceptable security lever with the visited network when user roams outside HE (home environment).
 - The security mechanism shall be scalable to support increase of user and/or network elements.

3. Overview Of Trusted Mobile Platform

In 2004, Trusted Computing Group (TCG) [11] develops TMP hardware architecture, software architecture and protocol specifications [12-14], which defines comprehensive end-to-end security architecture and focuses on mobile platform identity and integrity to prove trusted computing (TC) for ME. The generic two processors hardware architecture for TMP is depicted in Fig.1. The darkened components make up the trust boundary including 1) the application processor 2) Trusted Platform Module (TPM) 3) USIM 4) Core Root of Trust for Measurement (CRTM) 5) internal flash, 6) memory controllers and 7) DMA controller. Where CRTM is stored in the ROM memory and performs the initial trust measurements for the remainder of platform on power up. While, TPM [15] is a very important tamper-resistant component in TMP who is responsible for recording the integrity measurements of TMP and works closely with the CRTM to perform trusted boot. TPM also provides security functionality, such as platform attestation, protected storage, and sealing, to measure and validate the hardware and/or software configurations of the platform. For more detail about TMP, refer to [12-15].

Some key features of TMP are listed as the follows, which are beneficial to enhance the security of ME and 4G networks. Firstly, integrity measurement can provide trusted boot of ME and detect virus or attacker's malicious tamper on operating system and/or application software when ME powers on. Secondly,

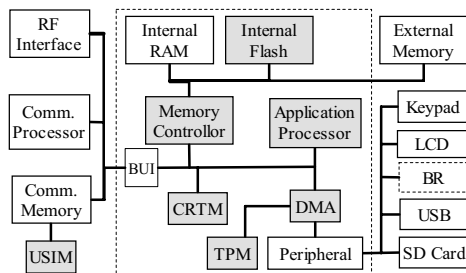


Figure 1. Generic hardware architecture for trusted mobile platform

access networks (AN) can verify the validity of current state of mobile platform via TMP's remote attestation before negotiates sensitive information with ME. Thirdly, process separation supported by hardware can resist unauthorized access to the sensitive data from process in ME, during ME's operation. Finally, protected storage can be utilized to safeguard TPM's private key and other sensitive information such as password and biometric template.

Three trusted levels (class 1, 2 and 3) are defined for TMP in [13]. It is strongly recommended that password should be used in combination with BI to authenticate user in security class 3. A TC-based biometric authentication system is proposed in [16] and introduced by [13] as a solution example to identify user. However, the solution is only an offline local authentication scheme on the premise of that TPM and user belong to the same certificate authority (CA). Moreover, the heavy computing loads for signature in this solution would also increase transaction time and hinder its enforcement in ME. What's more, the BI was not associated with password, which can not satisfy the security requirements of TMP class 3.

4. 4G Security Architecture & Framework

4.1 Scenario of 4G security architecture

As shown in fig.2, in terms of the security requirements the scenario of security architecture for 4G wireless networks including the following four security features (A, B, C, D) on different stratum is proposed as follows.

- A: Network access security: the set of security features that provide users with secure access to 4G services and against attacks on the (radio) access link.
- B: Network area security: the set of security features that enable nodes in the provider domain to securely exchange data, and protect against attacks on the wired network and network entities.
- C: User area security: the set of security features that enable secure access to ME/USIM and provide security environment in ME/USIM.
- D: Application security: the set of security features that enable applications in the user and in the provider domain to securely exchange messages.

4.2 Theory of public key broadcast protocol

Generally, in order to achieve mutual authentication in public key-based authentication scheme, communication participants should verify the validity of other side's public-key certificate before their negotiation. However, it is very difficult for ME to verify the validity of base station (BS)'s public-key

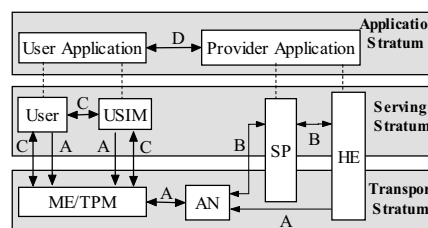


Figure 2. Scenario of security architecture for 4G systems

certificate since ME and BS usually belongs to different CA. Thus ME is vulnerable to be cheated by fake/forged BS. In the scenario of 4G systems, we present PKBP as follows to reduce complexity for certificates validation in ME and resist attack launched by fake/forged BS.

Every BS co-broadcasts its own public key (PK_B), identity (ID_B), modulus (N_B) and IPv6 address (IP_B) and those parameters of its neighbors via public broadcasting channel. E.g., as shown in Fig.3, BS2 broadcasts its public parameters (PK_{B2} , ID_{B2} , N_{B2} , IP_{B2}) together with BS1's (PK_{B1} , ID_{B1} , N_{B1} , IP_{B1}) and BS3's (PK_{B3} , ID_{B3} , N_{B3} , IP_{B3}) separately. Just like BS2, BS1 broadcasts its own parameters and that of BS2 and BS3, and so on. Thus, a seamless coverage will be formed on the premise of 4G network's seamless coverage. In fact, the number of fake/forged BS established by attacker is much smaller than genuine BS in 4G networks in view of the expensive cost for BS. I.e. even if attacker publishes its parameters via fake/forged BS, the number of parameters broadcasted by genuine BSs is greater than that issued by forged/fake one.

As shown in Fig.4, a small FIFO (First In First Out) buffer should be hold in ME, the main role of which is to store received public-key parameters and corresponding signal power (SP). As a result, the number of (PK_{B1} , ID_{B1} , N_{B1} , IP_{B1}) in the FIFO is much more than ($PK_{B'}$, $ID_{B'}$, $N_{B'}$, $IP_{B'}$) issued by forged BS. Then according to SP_{B1} , which is greater than SP_{B2} and SP_{B3} , MS will access BS1 despite of the most powerful signal $SP_{B'}$. In this way, according to the number of received public-key parameters and corresponding signal power, ME can resist attack launched by fake/forged BS.

4.3 Security framework based on TMP & PKI

As shown in Fig.5, according to TMP specifications, a trusted ME (TME) that comprises of a trusted biometric reader (BR) and TPM etc. to support TMP security class 3 is introduced to our security framework. Where TPM as the heart of TME is banded with and fixed in the motherland. On the other side, AN, HE, service provider (SP) and TME manufacturer (MF) hold a public-key certificate issued by their own trusted authority respectively which should be connected via PKI in the scenario of 4G networks.

The following notations will be used in the description of our scheme: ID_X , SK_X , PK_X , $Cert_X$ and Sig_X denote entity X 's identity, private key, public key, digital certificate and digital signature separately. $H(x)$ is a secure hash function and $E(k, x)$ represents encrypting content x with key k .

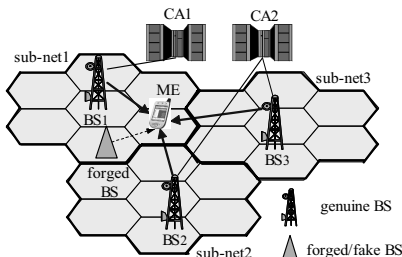


Figure 3. An example of PKBP over PKI

User remembers his password (PW) and holds a USIM card that is capable of checking the integrity and validity of the mobile platform and stores some authenticating parameters including user's biometric template (F_U , usually is user's fingerprint), SK_{User} , $Cert_{User}$, $Cert_{HE}$, x , y and z . The x , y and z are computed by user's HE as the follows before HE issues the USIM card to the user. Where n is a secure module of RSA signature algorithm.

$$\begin{aligned} x &= H(F_U || PW), \\ y &= x \oplus H(PW), \\ z &= S \oplus H(F_U \oplus PW), \\ S &= H(ID_{User} || PW || F_U)^{SK_{HE}} \bmod n. \end{aligned}$$

TPM stores SK_{TPM} , symmetric key (K_{BT}) shared between BR, $Cert_{TPM}$ as well as integrity metrics of other components in the TMP. Meanwhile, HE saves user's (ID_{User} , S , $Cert_{User}$) securely in its database.

In order to access 4G networks securely, firstly, user must insert his USIM card into ME and check the validity of TMP with the help of USIM and AN. If the state of TMP is reported trustworthy via trusted model indicator (TMI), user inputs his password and puts his finger on the BR, and will be identified by TME and USIM. Finally, authentication between user and AN will be enforced with the help of USIM and TPM.

4.4 TMP-Based Hybrid AKA Scheme

According to 4G "all-IP" vision, we perceive authentication as a service performed at the higher protocol layers irrespective of the underlying network technology. Two phases of our HAKA by means of user's permanent identity (ID_{User}) are depicted as follows. (1) In phase 1 local mutual authentication among user/USIM/TPM will be achieved and pre-authentication between user and AN will be enforced. (2) In phase 2 remote mutual identification among user/AN/HE will be implemented as well as key agreement between AN and user.

4.4.1 Authentication among User/USIM/TPM

M1. USIM \rightarrow TPM: r_1, ID_{USIM}, D_1 .

M2. TPM \rightarrow BR: r_2, ID_{TPM}, D_2 .

M3. BR \rightarrow TPM: MAC_{BR} .

$$MAC_{BR} = E(K_{BT}, r_2 || ID_{TPM} || D_3). \quad (1)$$

M4. TPM \rightarrow USIM: $r_3, Cert_{TPM}, Sig_{TPM}$.

$$Sig_{TPM} = E[SK_{TPM}, r_1 || r_3 || ID_{USIM} || D_4]. \quad (2)$$

M5. USIM \rightarrow AN: $r_1, r_3, C_1, Sig_{TPM}, Sig_{User}, Cert_{TPM}$.

$$C_1 = E(PK_{AN}, ID_{User} || IDC_{User} || r_4 || TS), \quad (3)$$

$$Sig_{User} = E(SK_{User}, IDC_{User} || ID_{TPM} || r_1 || r_3 || TS). \quad (4)$$

M6. AN \rightarrow USIM: D_5, MAC_{AN} .

$$MAC_{AN} = E(r_4, r_3 || ID_{User} || ID_{TPM} || D_5). \quad (5)$$

M7. USIM \rightarrow TPM: C_2, C_3 . BR \rightarrow TPM: C_4 .

$$C_2 = E(PK_{TPM}, r_5 || y || ID_{USIM}), \quad (6)$$

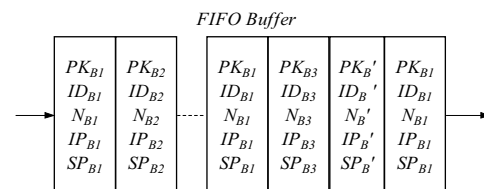


Figure 4. Assert valid BS in FIFO on ME

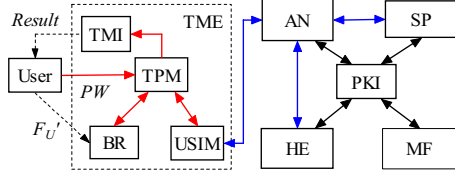


Figure 5. Security framework based on TPM and PKI

$$K_{ST} = H[(r_5 \oplus r_3) \| x \| ID_{TPM}], \quad (7)$$

$$C_3 = E(K_{ST}, r_5 \| ID_{TPM} \| F_U \| CS). \quad (8)$$

$$C_4 = E[K_{BT}, ID_{BR} \| ID_{TPM} \| r_2 \| F_U']. \quad (9)$$

M8. TPM \rightarrow USIM: C_5 .

$$C_5 = E(K_{ST}, ID_{USIM} \| r_5 \| H(F_U \oplus PW) \| D_6). \quad (10)$$

Description of phase 1:

M1. USIM generates a nonce r_1 and sends an integrity-checking request D_1 with (r_1, ID_{USIM}) as M1 to TPM.

M2. On receipt of M1, TPM issues a nonce r_2 and sends an integrity-checking request D_2 with (r_2, ID_{TPM}) to the BR.

M3. On receipt of M2, BR encrypts its integrity metric D_3 with (r_2, ID_{TPM}) in use of K_{BT} and responds MAC_{BR} to TPM.

M4. With original integrity metrics of BR and that of other components pre-stored in its tamper-resistant memory, TPM checks received MAC_{BR} is valid and the integrity of other components of TPM needed to perform the authentication operation are correct. Then TPM generates a nonce r_3 and signs its own integrity metric D_4 with (r_1, r_3, ID_{USIM}) . Then TPM delivers r_3 , $Cert_{TPM}$ and Sig_{TPM} to USIM.

M5. On receipt M4, USIM issues a nonce r_4 and calculates (C_1, Sig_{User}) as equation (3, 4). The AN's public-key parameters can be gained with the help of PKBP. Then USIM sends them with (r_1, r_3) to AN to verify Sig_{TPM} . Where $ID_{C_{User}}$ is a unique identity of user's certificate and TS is a timestamp.

M6. After decrypting C_1 , AN checks TS is acceptable and turns to PKI to gain valid $Cert_{User}$ according to (ID_{User}, IDC_{User}) . After verifying the validity of $(Cert_{TPM}, Sig_{TPM}, Sig_{User})$, AN pre-authenticates user. Then AN buffers $(ID_{User}, Cert_{User}, Cert_{TPM}, r_4)$ temporarily and responds USIM the checking result D_5 on TPM followed by MAC_{AN} .

M7. If received MAC_{AN} is correct and $(Sig_{TPM}, Cert_{TPM})$ are both valid according to D_5 , both TPM and AN are identified by USIM. As shown in Fig.6, USIM generates a nonce r_5 and sends (C_2, C_3) computed as equations (6, 8) to TPM. Optionally, biometric

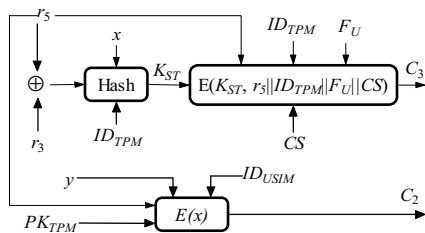


Figure 6. Data encapsulation algorithm in USIM

comparison software (CS) is also encrypted in C_3 and sent from USIM to TPM. After USIM shows the current state of platform is trustworthy via TMI, user inputs his password to TPM through Trusted I/O [14] and puts his finger on BR. The captured live fingerprint (F_U') is encrypted in C_4 with K_{BT} and sent to TPM.

M8. As shown in Fig.7, with the PW inputted by user and (r_5, y) decrypted from received C_2 , TPM firstly calculates

$$x = y \oplus H(PW) \quad (11)$$

and computes K_{ST} as equation (7). Then TPM decrypts C_3 with K_{ST} and gains (r_5, ID_{TPM}, F_U, CS) . If the (r_5, ID_{TPM}) contained in C_3 are both correct, TPM checks whether equation (12) holds.

$$H(F_U \| PW) = x \quad (12)$$

If equation (12) holds, USIM is identified by TPM. Then TPM decrypts C_4 sent by BR and checks (ID_{BR}, ID_{TPM}, r_2) are all correct. TPM makes a comparison between the F_U and F_U' in use of CS to see to what degree they are matched. If the match is achieved successfully, the user is authenticated by TPM. Then TPM computes $H(F_U \oplus PW)$ and transfers C_5 computed as equation (10) to USIM. Where D_6 is the authentication result on user. If (ID_{USIM}, r_5) contained in C_5 are both correct and user is valid according to D_6 , both user and TPM are identified by USIM.

4.4.2 Mutual authentication among user/AN/HE

M9. USIM \rightarrow AN: C_6 .

$$S = z \oplus H(F_U \oplus PW), \quad (13)$$

$$C_6 = E(r_4, ID_{HE} \| ID_{User} \| C_7), \quad (14)$$

$$C_7 = E(PK_{HE}, ID_{AN} \| ID_{User} \| TS \| Sig_{User}), \quad (15)$$

$$Sig_{User} = E[SK_{User}, ID_{User} \| H((ID_{AN} \| TS) \oplus S)]. \quad (16)$$

M10. AN \rightarrow HE: $C_7, C_8, Sig_{AN}, Cert_{AN}$.

$$C_8 = E(PK_{HE}, ID_{AN} \| ID_{User} \| r_6), \quad (17)$$

$$Sig_{AN} = E[SK_{AN}, ID_{HE} \| H(C_7)]. \quad (18)$$

M11. HE \rightarrow AN: C_9, C_{10} .

$$C_9 = E(PK_{AN}, ID_{AN} \| r_6 \| D_7), \quad (19)$$

$$C_{10} = E[H((ID_{AN} \| TS) \oplus S), ID_{AN} \| r_6]. \quad (20)$$

M12. AN \rightarrow USIM: C_{10}, C_{11} .

$$K_{AU} = H(ID_{User} \| r_4 \| r_6), \quad (21)$$

$$C_{11} = E(K_{AU}, ID_{AN} \| r_6 \| TID_{User} \| Lt), \quad (22)$$

M13. USIM \rightarrow AN: MAC_{USIM} .

$$MAC_{USIM} = MAC(K_{AU}, TID_{User} \| r_6). \quad (23)$$

Description of Phase 2 is just like that of phase 1. Where TID_{User} is a new temporary identity for user and K_{AU} is a session key shared between user and AN. Lt includes lifetime of (TID_{User}, K_{AU}) .

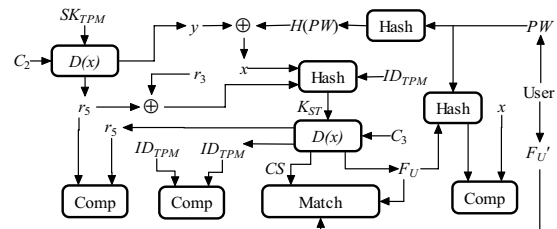


Figure 7. Date un-package and identification algorithm in TPM

5. Performance analysis

As shown in table 1, our security architecture and HAKA based on the combination of public key (PK), password (PW) and BI, is compared with symmetric key (SK)-based 3G AKA protocol and public key-based SSL AKA in [8].

TABLE I. COMPARISON BETWEEN OUR SCHEME AND OTHERS

Security goals and feature		3G AKA	AKA In [8]	Our AKA
Cryptography mechanism		SK	PK	PK, PW, BI
Mutual authentication	Between user and AN	Yes	Yes	Yes
	Between user and ME	No	No	Yes
	Between user and USIM	No	No	Yes
	Between ME and USIM	No	No	Yes
	Between AN and HE	No	No	Yes
Between user and HE		No	No	Yes
Security of key agreement		No	Yes	Yes
Protection on wired links		No	No	Yes
User's privacy over air interface		No	Yes	Yes
User's Privacy in ME		No	No	Yes
Non-repudiation		No	Yes	Yes
Resistant on replay attack		Yes	Yes	Yes
Against man-in-middle attack		Yes	Yes	Yes
Against malicious AN's attack		No	No	Yes
Against ME's attack or abuse		No	No	Yes
Support temporary user identity		Yes	Yes	Yes
Scalability and flexibility		Poor	Good	Good
Support trusted computing		No	No	Yes
Security level		Low	Middle	High

As shown in table 2, we investigate the computational loads of our AKA scheme in the viewpoint of ME including operations in BR, USIM and TPM. The computational loads of phase 1 and phase 2 in our scheme are compared with that of TC-based scheme in [16] and that of SSL AKA in [8] respectively. The numbers of public-key encryption, public-key decryption, symmetric-key encryption/decryption, signature, signature verification, and hash operations are given from the first row to the last row respectively in table 2.

TABLE II. COMPUTATIONAL LOADS OF OUR PROTOCOL IN ME

	PKE	PKD	EK	Sig	Ver	Hash
Phase 1 with ID_{User}	2	1	8	2	0	5
Scheme in [16]	2	2	4	5	5	0
Phase 2	1	0	4	1	0	2
SSL AKA in [8]	1	0	0	1	1	3

6. Conclusion

In this paper security architecture based on TMP and PKI are presented for 4G systems to provide a considerable robust platform for user's access to sensitive service and data. Meanwhile, a hybrid AKA scheme is proposed to offer enhanced end-to-end security and TC for ME. Mutual authentication among user/USIM/TPM as well as mutual authentication among user/AN/HE have been achieved in our scheme's phase 1 and phase 2 separately. According to

the comparing results shown in table 1 and 2, our scheme with slighter computational payloads in phase 1 than the TC-base local authentication protocol in [16] as well as slighter computational loads in phase 2 than SSL AKA in [8] separately, can offer advanced security than 3G AKA and SSL AKA in [8], and satisfy the security requirements of TMP class 3. So it is more suitable for ME and capable of being employed to handle the security issues in 4G networks.

Acknowledgment

This work was partially supported by the National Lab. for Modern Comm. Foundation of China under Grant No.51436050404QT2202.

References

- [1] Kim Jin Young, Kim Eun Cheol. Wired and wiresee intergration for the 4G mobile comm. systems. In proc. International Conf. on Advanced Comm. Tech., Phoenix Park, Kero, pp.51-54, 2004, Feb.9-11.
- [2] Gazis V., Housos N. and Alonistioti A. "Generic systems architecture for 4G mobile comm.," In proc. Intenational conf. on Vehicular Tech., Orlando, USA, pp.1512-1516, 2003.
- [3] Suk Y.H., Kai H.Y. "Challenges in the migration to 4G mobile systems". IEEE Magazine of Comm.,Vol.41, pp.54-59, 2003.
- [4] Kim J. Y., Kim E. C.. "Smart terminal tech. for the 4G mobile comm. systems," In proc. International Conf. on Advanced Comm. Tech., Phoenix Park, Kero, pp.51-54. 2004, Feb.9-11.
- [5] 3GPP TS 33.102: Security Architecture.
- [6] How secure are current mobile operating systems. <http://sec.isi.salford.ac.uk/cms2004/Program/CMS2004final/p2a2.pdf>
- [7] An Investigation into Access Control for Mobile Devices. <http://www.infoseca.co.za/proceedings2004/035.pdf>
- [8] Georgios Kambourakis, Angelos Rouskas. "Performance Evaluation of Public Key-Based Authentication in Future Mobile Communication Systems," EURASIP Journal on Wireless Comm. and Networking. Vol.1, pp. 184-197, 2004.
- [9] Al-Muhtadi J., Mickunas D.and Campbell, R. "A lightweight reconfigurable security mechanism for 3G-4G mobile devices," IEEE journal of Wireless Comm.,Vol. 9, pp.60-65, 2002.
- [10] Dell'Uomo L., Scarrone E. "An all-IP solution for QoS mobility management and AAA in the 4G mobile networks," In proceedings International Symposium on Wireless Personal Multimedia Communications, Hawaii, USA, pp.591-595, 2002.
- [11] TCG. <https://www.trustedcomputinggroup.org/>
- [12] Trusted Mobile Platform Hardware Architecture Description. http://www.trusted-mobile.org/TMP_HWAD_rev1_00.pdf.
- [13] Trusted Mobile Platform Software Architecture Description. http://www.trusted-mobile.org/TMP_SWAD_rev1_00.pdf.
- [14] Trusted Mobile Platform Protocol Specification Document. http://www.trusted-mobile.org/TMP_Protocol_rev1_00.pdf.
- [15] TPM Main Part 2 TPM Structures. https://www.trustedcomputinggroup.org/downloads/tpmwg-mainrev62_Part2_TPM_Structures.pdf.
- [16] B. Balacheff, D. Chan, L. Chen., "Securing smartcard intelligent adjuncts using trusted computing platform technology," In Proc: Conf. of IEIF Fourth Smart Card Research and Advanced App., pp.177-195, Bristol, UK, 2000.