Mobile Platform and Secure Access Approach of UMTS Terminal Based on Trusted Computing

Yingyou Wen
College of Information Science and Engineering, Northeastern University, Shenyang, China
Email: wenyy@neusoft.com

Xuena Peng, Shuyi Chen, Hong Zhao
College of Information Science and Engineering, Northeastern University, Shenyang, China
Email: {pengxn, chensy, zhaoh}@neusoft.com

Abstract—On the basis of comprehensive study of trusted computing technology and the threats to 3G network, the architecture of trusted mobile platform based on mobile trusted module is proposed, and a DAA-based key management and a trusted computing based access mechanism for 3G network are designed. Furthermore, a predicate logic based formal analysis method is also proposed. With DAA mechanism, user privacy is protected and the bottleneck problem of centralized CA is avoided. The proposed MTM-based trusted access mechanism focuses on not only the authentication of mobile user, but also the healthy status of the mobile user. Therefore, the UMTS network can forbid the unsafe mobile terminals from accessing it, which guarantees the security of the network from the source. The validity of platform and trusted UMTS access scheme is verified with the proposed formal analysis method.

Index Terms—trusted computing; TNC; MTM; UMTS; direct anonymous attestation

I. INTRODUCTION

The security of 3G system has become a key problem during its developing and become one of the most important research areas. Nowadays, the researches of 3G security mainly focus on two aspects. One is the adoption of traditional security products into 3G system, so that the core network could be protected [1, 2]. The other is the identity authentication and the key exchange in Radio Access Network (RAN) [3, 4]. However, these researches cannot solve the 3G security problem thoroughly. On one hand, traditional network security products can only protect core network from attacks which launched from the Internet, but not that from smart mobile terminals. On the other hand, identity authentication and key exchange based access control only focuses on the verification of SIM card, but without any consideration of the healthy status of mobile devices. It is often the unsafe mobile terminals which bring security threats to the whole network, so the authentication based access control could not be the silver bullet either. All these vulnerabilities will bring more threats to whole network operation and those business applications provided on top layer.

II. TRUSTED COMPUTING AND MOBILE TRUSTED MODULE

A. Trusted Computing

Anderson J.P. first proposed the concept of the credibility of the system so far trusted computing considers credibility as an evaluable and verifiable performance metric, which can be used to solve the information security problem from a new angle [5]. Its main purpose is to enhance the security of the terminal architecture at source, by which terminal devices can acquire immunity to malicious code such as viruses, Trojans and other attacks, thus provide a reliable and credible network environment [6]. As 3G network has a rigorous identity management, authentication and billing mechanism, and easy to execute management of mobile devices, Therefore, this paper proposed an architecture of trusted mobile platform based on Mobile Trusted Module, and a Trusted Network Connect (TNC) scheme is given, by which the mobile terminals’ authenticity and integrity will be detected and unsafe terminal access will be automatic refused.

Figure 1 Architecture of trusted network connection.
research has gone through the course of more than 30 years [7, 8]. TCG (Trusted Computing Group) as an important representative body, has set up various working groups responsible for developing and publishing trusted computing architecture, trusted computing modules, Trusted Network Connect and credibility of the mobile platform specifications [9]. A typical application of utilizing trusted computing technology to protect network is Trusted Network Connect (TNC) [11]. Its main purpose is to provide network access control through the use of trusted computing technology. TNC architecture based on the TPM (Trusted Platform Module) is shown in Fig.1.

TNC is divided into three tiers, namely client-side AR, PDP strategic services and PEP access control. It also defines interface specification between different entities. Clients with the TPM provide hardware-based host authentication and host integrity verification. TNC allows only trusted terminal to access the network through the platform authentication, access restrictions, evaluation, isolation and remediation technology, and then prevent unsafe endpoints linked to the network and protect the entire network security.

B. Mobile Trusted Module

The wide use and increasing capabilities of mobile devices introduce security risks to the mobile phone users as well as mobile operators. Applying TPM directly to the mobile platform facing some problems.

First, mobile platform is subject to the limited computing capability, storage and energy capacity of mobile devices, so the consideration in designment of both security chip and security policy will be different with those in PC.

Secondly, the application environment of mobile platform is very complex, users, operators, content providers and device manufacturers have different requirements, all of which should be considered during the designment of trusted mobile platform. The Trusted Computing Group (TCG) specification [12] aims to address this problem and Mobile Phone Work Group (MPWG) in TCG specically deals with trusted computing in mobile environment. [13].

MPWG has described a set of selected mobile phone uses cases, and announced Mobile Trusted Module specification (MTM), which provides protection for mobile terminals instead of TPM. Major components of a trusted mobile platform based on MTM include:

a) Reference Integrity Metric (RIM). RIM is a value used to validate the result of a measurement taken before software or hardware is loaded or initialized (for execution). Typically a digest of a compiled software and configuration data which can affect the engine trust state.

b) Engine. Engine is a dedicated processor or runtime environment which is able to access trusted resources for the implementation of reliable service or ordinary service. TIM (Target Integrity Metric) is Integrity Metric of a target object or component as measured by the measurement agent of that object. Typically a digest of a software image and/or configuration data. trusted services execute reliable measurement and reliable verification, verify whether the integrity is damaged by comparison of TIM and RIM.

c) Engine authorization (RIM Auth). It is the entity that issued the certificate RIM_Certs.

d) MTM include trusted storage root, Root of Trust for Measurement and Root-of-Trust-For-Reporting, verify the integrity of RIM and RIM Auth and record the RTM/RTV measurement results.

III. SAFETY BOOTING OF TRUSTED MOBILE PLATFORM BASED ON MTM

A. Architecture of Trusted Mobile Platform

Processor of Trusted Mobile Platform include baseband processor and application processor, the two processors can be separated. We adopt dual-processor architecture in our solution. According to MTM specification of TCG and referring to the architecture of the mobile platform proposed by MPWG, revised trusted mobile platform architecture is proposed as shown in Fig.2.

The whole system consists of the following security components and constitutes a credible border.

a) Application processor. Application processor control system execution at boot time and later, isolates the trusted applications and their data with entrusted application.

b) MTM: MTM provides a protected execution environment with a variety of security features, including key algorithms, authentication, and trusted storage. MTM can provide more flexible use of the security and services to meet multi-owner requirements of the mobile platform. Equipment suppliers can ensure that the mobile platform is in a trusted state through the built-in MRTM, and provide trust assurance for the upper applications. The upper applications, such as mobile operators, application achieve reliable service through additional MRTM and MLTM.

c) RTV/RTM: RTM (Root of Trusted for Measurement) measure the integrity of subsequent components. TV is responsible for
the comparison of on-site measurement and reference value in RIM to determine whether the integrity of the measurement object is damaged. MTM visit RTV / RTM through the DMA.

d) DMA: In system with a High security level, DMA is controlled by a trusted core to ensure trusted application or operating system to access physical memory.

B. Safety Booting of Trusted Mobile Platform

Safety booting process is a basis to ensure that mobile platform is trusted. After safety booting, a trusted program execution environment can be established, ensure that the system in a trusted state both at startup and runtime, and provide protection for program. Safety booting process is transfer of trusted measurement and trusted verification along the chain of trust, also a delivery process of execution control.

RTM measure the integrity of follow-up components in trust chain, RTV is responsible for the comparison of on-site measurement and reference value in RIM to determine whether the integrity of the measurement object is damaged. If verification is passed, it will pass execution control to components in next level. Booting is implemented step by step and the integrity of the entire platform is assured.

Safety booting process in MTM related specification is implemented by using a measurement and verification agent to measure and verify follow-up components. After completion of the measurement and verification, control of measurement and verification is passed to the measurement and verification agency in the next component. However, as the agency is not entirely credible, so that trust measurement and certification approach will bring loss of trust, loss of trust will be enlarged with the increase of trust chain length and leading to degrade of credibility of whole platform.

The function of MTM is to generate and manage the keys, Module (MTM) is embedded in the mobile terminals [14]. UMTC access solution, which can secure the 3G network design an integrity measurement and authentication-based UMTS access solution, which can secure the 3G network [14].

Safety booting process in MTM related specification is implemented by using a measurement and verification agent to measure and verify follow-up components. After completion of the measurement and verification, control of measurement and verification is passed to the measurement and verification agency in the next component. However, as the agency is not entirely credible, so that trust measurement and certification approach will bring loss of trust, loss of trust will be enlarged with the increase of trust chain length and leading to degrade of credibility of whole platform.

Assuming that a RIM certificate needed in the safety booting process has been generated, a safety booting process of mobile platform based on direct measurement is described using TCG specified original language as follows:

Stage 1: MTM \(\rightarrow\) TPM \_Init, TPM \_startup

MTM setup after TPM_Init and TPM_Startup has been called; all values of PCRs are initiated as 0;

Stage 2: MTM \(\rightarrow\) TPM \_VerifyRIMCertAndExtend\(e_1\)

MTM verify integrity of RTM/RTV according to RIM certificate and record verification result in PCR;

Stage 3: RTM \(\rightarrow\) Measure\(e_2\)

RTV \(\rightarrow\) LookUpRIMCert

MTM \(\rightarrow\) TPM \_VerifyRIMCertAndExtend\(e\)

RTM measure the integrity value of \(e_2\), RTV load RIM certificate of \(e_2\), and verify that if the on-site measurement and the reference value in RIM are the same. TM executes TPM\_VerifyRIMCertAndExtend to verify RIM certificate, and record result in PCR, and then \(e_2\) gains its execution right.

Stage 4: RTM \(\rightarrow\) Measure\(e_3\)

RTV \(\rightarrow\) LookUpRIMCert\(e_3\)

MTM \(\rightarrow\) TPM \_VerifyRIMCertAndExtend\(e\)

RTM measure integrity value of \(e_3\), RTV load RIM certificate of \(e_3\) and verify that if the on-site measurement and the reference value in RIM are the same. MTM execute TPM\_VerifyRIMCertAndExtend to verify RIM certificate and record result in PCR, then \(e_3\) gains its execution right.

Stage 5: RTM \(\rightarrow\) Measure\(e_4\)

RTV \(\rightarrow\) LookUpRIMCert\(e_4\)

MTM \(\rightarrow\) TPM \_VerifyRIMCertAndExtend\(e\)

RTM measure integrity value of \(e_4\), RTV load RIM certificate of \(e_4\) and verify that if the on-site measurement and the reference value in RIM are the same. MTM execute TPM\_VerifyRIMCertAndExtend to verify RIM certificate and record result in PCR, then \(e_4\) gains its execution right.

After the measurement and verification of RTM and RTV, integrity of all entities involved in the booting process are assured so that trusty of mobile platform can be achieved. If any return value of TPM\_VerifyRIMCertAndExtend is error or no proper certificate is found, the process will be ceased.

IV. TC-BASED UMTS ACCESS APPROACH

As mentioned above, we introduce trusted computing techniques to 3G network security infrastructure, and design an integrity measurement and authentication-based UMTS access solution, which can secure the 3G network by prohibiting the untrusted terminal from accessing the mobile network. We assume here that the Mobile Trusted Module (MTM) is embedded in the mobile terminals [14]. The function of MTM is to generate and manage the keys,
and protect the information by making use of the hardware functions.

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuC</td>
<td>Authentication Center</td>
</tr>
<tr>
<td>K\textsubscript{1}</td>
<td>A’s Public key</td>
</tr>
<tr>
<td>K\textsubscript{2}</td>
<td>A’s Private key</td>
</tr>
<tr>
<td>Cert\textsubscript{A}</td>
<td>The certificate for A’s public key</td>
</tr>
<tr>
<td>KEK</td>
<td>Endorsement Key</td>
</tr>
<tr>
<td>AV</td>
<td>Authentication Vector</td>
</tr>
<tr>
<td>RTM</td>
<td>Root of Trusted Measurement</td>
</tr>
<tr>
<td>RTV</td>
<td>Root of Trusted Verification</td>
</tr>
<tr>
<td>IS</td>
<td>DAA Certificate Issuer</td>
</tr>
<tr>
<td>RAND</td>
<td>Random number</td>
</tr>
<tr>
<td>AUTN</td>
<td>Authentication Token</td>
</tr>
<tr>
<td>XRES</td>
<td>Expected Authentication Reply</td>
</tr>
<tr>
<td>IDK\textsubscript{+}</td>
<td>K\textsubscript{E} signed d</td>
</tr>
<tr>
<td>RES</td>
<td>User authentication reply</td>
</tr>
<tr>
<td>AC</td>
<td>Access Controller</td>
</tr>
</tbody>
</table>

Table I. ILLUMINATION OF IDENTIFIERS

![Figure 4 Trusted access mechanisms of UMTS](image)

Some key processes of access are given below:

1. **ISSUER(AuC)ÆMTM:** \( K\textsubscript{IS}^+, K\textsubscript{IS}^- \)
   DAA signer generates key pair, and release the public key:
   \[
   K\textsubscript{IS} = \{ h, g, f, h, S, Z, R_0, R_1, y, t, \rho \} \quad (1)
   \]
   \* **MTMÆISSUER(AuC):** \( K\textsubscript{E}^+, U, N_1 \)
   After MTM receive the \( K\textsubscript{IS} \), it generates a piece of secrete information \( f \) based on \( K\textsubscript{E}^+ \) and a random number \( v' \), then separate \( f \) to \( (f_0, f_1) \), and compute \( U, N_1 \), finally, MTM sends \( K\textsubscript{E}^+, U \) and \( N_1 \) to DAA signer.
   \[
   U = R_{1}^{f_{1}} R_{0}^{f_{0}} S^{y'} \text{ mod } n \quad (2)
   \]
   \[
   N_1 = \zeta^{1}_{t'} f_{1} z_{1} \text{ mod } \Gamma \quad (3)
   \]
2. **ISSUER(AuC)ÆMTM:** \( A, e, v' \)
   DAA signer validates the authenticity of \( K\textsubscript{E}^+ \), choose random numbers \( e \) and \( v' \), compute \( A \) and send it to MTM
   \[
   A = \left[ \frac{Z}{US^v} \right]^{t/e} \text{ mod } n \quad (4)
   \]
   After MTM verify whether \( A \) is correct, then save \( (f_0, f_1, v' = v' + v'' ) \) as knowledge, which can be used to generate DAA signature in each identity authentication process.

Fig.4 shows the trusted computing based UMTS access solution. First, the mobile platform performs secure boots, and then whenever the mobile terminal access the network, the platform will not only authenticate the mobile terminal, but also verify the configuration status integrity of the mobile terminal. Integrity indicates whether the mobile terminal is healthy or configured as expected. Authenticity assures that the system can only be used by authorized users.
After HLR received the authentication request from VLR, it generates an authentication vector (RAND || XRES || CK || IK || AUTN), and releases the key $K_{RS}$ for verifying the DAA certification.

e) $\text{VLR/SGSN} \rightarrow \text{ME/MTM}: \text{RAND} || \text{AUTN}, \text{RPCRs}$

After VLR receives the authentication vector, it sends RAND and AUTN to ME/MTM, and requests the user to generate authentication data. Then, it sends platform integrity request $\text{RPCRs}$.

After ME received RAND and AUTN, it computes the value of XMAC (Expected Message Authentication Code). Then it compares the result with the MAC value in AUTN. If they are not identical, ME will send refuse message, and stop the procedure. If they are identical, ME verify if SQN is within the predefined range, if it is out of the range, meaning the synchronization fails, then it will send synchronization failure message, and stop the procedure. If both verifications succeed, ME believes VLR to be the authorized network of HLR, and then it computes $CK, IK$ and $RES$.

f) $\text{ME/MTM} \rightarrow \text{IMV/AC}: \text{RES, } [\text{K}_{AIK}, \text{Verifier}, t] \text{ RPCRs}, \text{K}_{AIK}, \text{K}_{AIK}, \text{SML}$

EM/MTM sends RES to IMV/AC to testify the authenticity of the user. It then uses $(f_0, f_1, f_2, f_3, v)$ to generate the DAA signature key $K_{DSL}$, and also the identification key pair $K_{AIK}$ and $K_{AIK}$. After that, it sends IMV/AC the $K_{DSL}$, signed $K_{AIK}$-information $[K_{AIK}, \text{Verifier}, t]K_{DSL}$, $K_{AIK}$ signed integrity measurement value $[\text{RPCRs}]K_{AIK}, K_{AIK}$, and security measurement log SML, in order to verify the integrity and authenticity of the platform.

After IMV/AC received the message from ME/MTM, it compares RES and XRES. If they are identical, it believes ME to be a legal user.

IMV/AC validates the DAA certificate with $K_{DS}$. If the certificate is legal, it believes the $K_{DSL}$, signed $K_{AIK}$-information to be authentic, thus the platform is also authentic. Then it validates $K_{AIK}$ signed PCRs with $K_{AIK}$. If the signature is authenticated, then it believes $K_{AIK}$ signed PCRs is authenticated. Furthermore, it hashes the SML, and compares the result with the value stored in PCR to verify the integrity of the platform. Based on the verification results, and according to the access control policy, IMV/AC then assign corresponding resource access privilege to user, or isolate it and repair the platform configuration, and forbidden it from accessing the network until the platform configuration is satisfied.

When all the above procedure is executed, the UMTS access solution mainly achieves the following tasks: a) the user authenticates the network, and the user assures that VLR is a HLR authorized network; b) the network authenticates the user, and the network assures that the user is a legal user; c) the key exchange of encryption key (CK) and integrity key (IK); d) MTM-based mobile terminal integrity verification.

V. VALIDATION AND ANALYSIS

In order to validate our solution, a predicate logic-based trusted computing model is proposed as the method for solution validation and analysis. Based on trusted computing specifications, we have defined a variety of predicates to indicate the characteristics of objects and the relationships among these objects, as well as the inference rules for deducing the trust relationship.

A. Formalized validation of the trusted access solution

Definition 1. Given $E$ the set of all entities in the trusted computing system, for $\forall e_i, e_i \in E$, and $i \in N$, the following predicates are defined:

- $\text{Trusted}(e_i)$, which means $e_i$ is trusted.
- $\text{Measure}(e_i, e_i, \text{Integ})$, which means $e_i$ measures the integrity of $e_i$ and trusts $e_i$.
- $\text{Trusted}(e_i) \land \text{Measure}(e_i, e_i, \text{Integ})$ is the rule of trusted domain extending. Initial trusted domain only includes $e_i$. After $e_i$ measures the integrity of $e_i$, trusted domain was extended and includes both $e_i$ and $e_i$.

During the booting process we proposed above, trusted chain includes only $e_i$ after platform is setup, namely trusted root RTM/RTV is credible, so initial state is $\text{Trusted}(e_i)$.

Our conclusion is that all of four entities in trusted chain are trusted after safety booting. Namely we have:

$$E = \{e_i[\text{Trusted} (e_i_i) ]1 \leq i \leq 4\} \quad (5)$$

According to inducing rule in [10], we have:

- $\text{Trusted}(e_i)$
- $\text{Trusted}(e_i) \land \text{Measure}(e_i, e_i, \text{Integ})$
- $\text{Trusted}(e_i) \land \text{Trust}(e_i, e_i, \text{Integ})$
- $\text{Trusted}(e_i) \land \text{Trust}(e_i, e_i, \text{Integ})$
- $\text{Trusted}(e_i) \land \text{Trust}(e_i, e_i, \text{Integ})$
- $\text{Trusted}(e_i) \land \text{Trust}(e_i, e_i, \text{Integ})$
- $\text{Trusted}(e_i) \land \text{Trust}(e_i, e_i, \text{Integ})$
- $\text{Trusted}(e_i) \land \text{Trust}(e_i, e_i, \text{Integ})$

$$\Rightarrow E = \{e_i[\text{Trusted} (e_i_i) ]1 \leq i \leq 4\} \quad (6)$$

By the above equations, based on initial conditions, using deduction rules, we can draw a conclusion that all components in platform are trusted.

B. Formalized validation of the trusted access solution

Definition 2. Given $E$ the set of all entities in the trusted computing system, for $\forall e_i, e_i \in E$, and $i \in N$, the following predicates are defined:

- $\text{Trusted} \text{ integrity measurement capability: } \text{Trust} (e_i, e_i, \text{Integ})$, which means $e_i$ trusts that $e_i$ has the capability of measuring the integrity.
- $\text{Trusted} \text{ certification issuing capability: } \text{Trust} (e_i, e_i, \text{Cert})$, which means $e_i$ trusts that $e_i$ has the capability of issuing and maintaining a certification.
• Trusted integrity: \(\text{Trusted} \left ( e_1, e_2, \text{Integ} \right )\), which means \(e_1\) believes that \(e_2\) has the attributes of trusted integrity.
• Trusted authenticity: \(\text{Trusted} \left ( e_1, e_2, \text{Auth} \right )\), which means \(e_1\) believes that \(e_2\) has the attributes of trusted authenticity.
• Certificate Issue: \(\text{Cert} \left ( e_1, e_2 \right )\), which means after \(e_1\) verifies the authenticity of \(e_2\), it signs a certificate to \(e_2\).
• Integrity Measurement: \(\text{Meas} \left ( e_1, e_2, \text{Integ} \right )\), which means \(e_1\) measure the integrity of \(e_2\), if the measurement result of \(e_2\) is as expected, \(e_2\) integrates.

**Definition 3.** Given \(E\) the set of all entities in the trusted computing system, for \(\forall e_1, e_2, e_3 \in E\) and \(i \in \mathbb{N}\), the following rules are defined:

- **Rule 1.** Integrity verification rule
  \[
  \frac{\text{Trust} \left ( e_1, e_2, \text{Integ} \right ), \text{Meas} \left ( e_2, e_3, \text{Integ} \right )}{\text{Trust} \left ( e_1, e_3, \text{Integ} \right )} \quad (8)
  \]
- **Rule 2.** Authenticity verification rule
  \[
  \frac{\text{Trust} \left ( e_1, e_2, \text{Cert} \right ), \text{Cert} \left ( e_2, e_3 \right )}{\text{Trust} \left ( e_1, e_2, \text{Auth} \right )} \quad (9)
  \]

**Rule 1** means \(e_1\) believes \(e_2\) has the capability of trusted integrity measurement, \(e_2\) measures the integrity of \(e_3\), verifies that \(e_3\) has trusted integrity, then \(e_1\) believes that \(e_3\) has the attributes of trusted integrity.

**Rule 2** means \(e_1\) believes \(e_2\) is the legal certificate signer, \(e_2\) signs a certificate for \(e_3\), then \(e_1\) believes the certificate of \(e_3\) is trusted, and \(e_2\) has the attributes of trusted authenticity.

The following procedure indicates how the formalized analysis of trusted computing based secure access of UTMS based on predicate logic is carried out. Firstly, present the predicate-based initial conditions and conclusions, clarify the consumptions according to the deducting requirements; secondly, apply the definition of predicates and inference rules, start from the initial conditions and assumptions, and deduce the conclusion; finally, analyze the rationality of the assumptions, and validate the correctness of the trusted computing model. As long as the assumption is rational, then the model is believed to be trusted, otherwise, look for the vulnerabilities of the model according to the irrationality of the assumptions.

Our proposed formalized validation for trusted computing model is as follows:

- Initial conditions
  In our proposed trusted computing based secure access solution, we assume the entities that represent the mobile terminal, MTM, visiting region and home region are respectively \(e_1\), \(e_2\), \(e_3\) and \(e_4\). At the initial state, \(e_2\) and \(e_3\) both trust \(e_1\) to be the legal DAA certificate signer, so the initial state is:
  \[
  \frac{\text{Trust} \left ( e_2, e_4, \text{Cert} \right ), \text{Trust} \left ( e_1, e_4, \text{Cert} \right )}{(10)}
  \]

  Beside, we assume if \(e_1\) can validate that \(e_2\) is the legal MTM, and then \(e_1\) believe \(e_2\) has the capability of integrity measurement:
  \[
  \frac{\text{Trusted} \left ( e_1, e_2, \text{Auth} \right ) \Rightarrow \text{Trusted} \left ( e_1, e_2, \text{Integ} \right )}{(11)}
  \]

  We also assume MTM is an indivisible part of the mobile terminal, so it can represent the authenticity of the platform. If \(e_1\) can validate \(e_2\) is authentic, the mobile terminal \(e_4\) which \(e_2\) embedded in can also be regarded as legal.
  \[
  \frac{\text{Trusted} \left ( e_1, e_2, \text{Auth} \right ) \Rightarrow \text{Trusted} \left ( e_1, e_2, \text{Integ} \right )}{(12)}
  \]

- Conclusions
  The conclusion is that \(e_3\) validate \(e_1\) to be the trusted mobile terminal, which has the correct attributes representing its authenticity and integrity, so the conclusion should be described as:
  \[
  \frac{\text{Trusted} \left ( e_1, e_2, \text{Auth} \right ) \land \text{Trusted} \left ( e_1, e_2, \text{Integ} \right )}{(13)}
  \]

  Deducing procedure
  Since the original authentication and key exchange procedure of UTMS access solution is already recognized by the public, we do not further discuss it. In this paper, we only validate the integrity and authenticity of our trusted computing based secure access solution. The deducing process is as follows:

  According to the access solution, before mobile terminal access the network, \(e_2\) has already signed a DAA certificate to \(e_2\). Based on **rule 2** and initial condition (10), the trusted authenticity of \(e_2\) can be:
  \[
  \frac{\text{Trust} \left ( e_3, e_4, \text{Cert} \right ), \text{Cert} \left ( e_2, e_3 \right )}{\text{Trust} \left ( e_2, e_2, \text{Auth} \right )} \quad (14)
  \]

  Conclusion (14) shows \(e_2\) is authentic, and is the trusted MTM. Based on assumption (11) and (12), the following conclusion can be deduced:
  \[
  \frac{\text{Trusted} \left ( e_1, e_2, \text{Auth} \right ) \Rightarrow \text{Trust} \left ( e_1, e_2, \text{Integ} \right )}{(15)}
  \]
  \[
  \frac{\text{Trusted} \left ( e_3, e_2, \text{Auth} \right ) \Rightarrow \text{Trust} \left ( e_3, e_1, \text{Auth} \right )}{(16)}
  \]

  Conclusion (15) shows that \(e_3\) believe that \(e_2\) has the trusted capability of integrity measurement. \(e_2\) measures the integrity of \(e_1\), stores the result of the integrity measurement in PCRs, and send it to \(e_3\). \(e_3\) can get the integrity status of \(e_1\) based on the integrity results and the logs that \(e_2\) generated.
  \[
  \frac{\text{Trust} \left ( e_1, e_2, \text{Integ} \right ), \text{Meas} \left ( e_1, e_2, \text{Integ} \right )}{\text{Trust} \left ( e_1, e_2, \text{Integ} \right )} \quad (17)
  \]

  According to conclusion (16) and (17) above, conclusion (13) can be deduced, which shows that \(e_2\) believe \(e_1\) to be the trusted mobile terminal, satisfying the requirement of integrity and authenticity:
  \[
  \frac{\text{Trusted} \left ( e_1, e_1, \text{Auth} \right ) \land \text{Trusted} \left ( e_1, e_1, \text{Integ} \right )}{(18)}
  \]

  As the assumption is rational, and from the initial condition we can deduce the integrity and authenticity of the platform, so the UTMS access solution is logically correct.

**C. Security and performance analysis**

The trusted UMTS access solution provides not only the authentication between user and network, but also the hardware-based identification and integrity verification of mobile terminals, which helps to secure the network from
source. With the introduction of MTM, our solution provide the hardware-based high level security assurance: a) secure storage is implemented based on the platform configure register embedded in the MTM hardware; b) trusted measurement and verification is implemented based on the measurement root and verification root embedded in MTM, and the authentication and integrity of the mobile terminal is assured; c) MTM provides an encapsulated and protected runtime environment for key generation, storage, encryption and decryption, signature authentication; d) platform status certification can be provided to the remote verification platform based on the MTM trusted report root.

<table>
<thead>
<tr>
<th>Solution</th>
<th>UMTS Solution</th>
<th>Our Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication (USIM)</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Authentication VLR</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>IK/CK exchange</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Terminal anonymity protection</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Terminal Authenticity Measurement</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Terminal Integrity Measurement</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>Security Level</td>
<td>Middle</td>
<td>High</td>
</tr>
</tbody>
</table>

From the data showed in Table II, the solution proposed in the paper is more secure and more adaptable than current solutions.

In this solution, since the DAA certificate is signed and distribute to the mobile terminal on its initial access to the network, the mobile terminal do not need to request the certificate for multiple times from DAA signer, so that the bottle neck at certificate signer is successfully avoided. The verification information is conveyed within the original UTMS authentication and key exchange process, and there’s no extra cost for integrity verification, so the total times of communication are not increased, although the average message length increases a bit, anyway, the change of message conveying method actually decrease the cost of communication.

VI. CONCLUSION

The architecture of trusted mobile platform based on Mobile Trusted Module is proposed and a trusted computing based UMTS access solution is proposed in this paper. The proposed solution can achieve not only the validity authentication between user and network, but also the authentication and integrity check of the mobile terminal, which can ensure that the mobile terminal will not bring security threats to UMTS network. The formalized analysis method of predicate logic based trusted computing model, which has the advantage of simplicity, efficiency and accuracy, is applied to the validation analysis of trusted UMTS access solution. The formalized analysis method provides us with a trust validation theory according to specific trusted computing application scenario. Our further work is to implement the trusted UMTS access system based on the proposed solution.

ACKNOWLEDGMENT

This work was supported in part by grants from the National Natural Science Foundation of China (Grant No.60803131) and The Science and Technology Plan of Shenyang(No.1091176-1-00)

REFERENCES


Yingyou Wen was born in Shenyang, China on March 12, 1974. He received the Ph.D. degree in computer science from Northeastern University, China, 2005. His main research include: network security, wireless communication and sensor network. He is an associate professor of Northeastern University, and vice president of Neusoft Reasearch, China. His current research focuses on Middleware of WSN and network security.

Xuena Peng was born in 1979, in Shenyang, China. She received her Ph.D. degree in computer engineering and science from Northeastern University in China, in 2007. Her main research interest include: Intrusion detection, 3G network security, security alert analysis, P2P streaming, and sensor network. Currently, she is working as a postdoc in Northeastern University, China. Her current research focuses on WSN Middleware and network security.

Shuyi Chen was born in Henna Province, China in 1972. He received the Ph.D. degree in computer science from Northeastern University, China, 2009. His main research include: network security and wireless communication. His current research focuses on security of 3G/4G network.

Hong Zhao was born in Hejian, China in 1954. He received the Ph.D. degree in computer science from Northeastern University, China, 1990. His main research include: computer network and information security. He is a professor of Northeastern University, and super vice president of Neusoft Group, China. His current research focuses on network security and wireless communication.