International Journal of Grid Distribution Computing
Vol.7, no.3 (2014), pp.221-232
http://dx.doi.org/10.14257/ijgdc.2014.7.3.23

Research of Remote Attestation Model and Protocol ofInteractive Terminals of Smart Grid

Kehe Wu[1], Fei Chen[2] and Yi Li[2]

[1]Beijing Engineering Research Center of Electric Information Technology, North China Electric Power University
NO.2 Beinong Road, Changping District, Beijing 102206, China
[2]Department of Control and Computer Engineering School, North China Electric Power University
NO.2 Beinong Road, Changping District, Beijing 102206, China
[1]epuwkh@126.com,[2]chenfei0428@126.com

Abstract

Trusted computing is one of the most important technologies to ensure the information security of smart grid. Remote attestation can guarantee the trusted access of interactive terminals of smart grid (SGIT).The existing remote attestation schemes have the following disadvantages: ① The verifier initiates authentication request, and the attestor returns the platform configuration information. This pattern is not suitable for smart grid application environment. ② There is a man in the middle attack, impersonation attack and platform configuration eavesdropping risk, and so on. In view of the above defects, this paper proposes a remote attestation model sponsored by attestor which is based on the binary certificate and combined with the practical application environment. Also, the remote attestation protocol is designed, and the performance and characteristics of the protocol is analyzed.Analysis of the protocol was made. The results suggest that this protocol can make sure the credible access of SGIT and has practical application value.

Keywords: *Trust Computing, Remote Attestation, Smart Grid, Interactive Terminal, Information Security*

1. Introduction

The Smart Grid is such an intelligent system which is based on competitive and bidirectional communication network, and through the use of advanced sensing and measurement technology, advanced equipment technology, advanced control method and decision support technology to realize the power grid operates safely, reliably, economically and efficiently. The interactive terminals are important equipment which is used to monitor and control the electric energy and costs of electric users and improve the reliability of power supply. They make use of advanced sensing and measurement technology to collect data which will be transmitted real-timely to the intranet of electric power information through the mobile communication network, and then receive control commands to accomplish the interactions with the management system. On the one hand, it could collect and analyze users' electricity consumption data scientifically, which will be the basis for decision-making. On the other hand, it will master users' electrical behavior to distribute electric load rationally. Nevertheless, the interactive terminals are designed and implemented on the basis of open embedded operating system and utilize open communication protocols to transfer data, they bring serious safety concerns. How to achieve the trusted access of interactive terminals

ISSN: 2005-4262 IJGDC

which could ensure the safety and stable operation of the Smart Grid has become an extremely urgent task.

The emergence of trusted computing technology is just to ensure the terminal safety. The terminal constructs the trusted platform by using the TPM chip and TSS (Trusted Software Stack), and takes TPM as the root of trust for measurement, the trusted storage root and the credible reports of root to report its hardware configuration and software running state to other terminals and allow them to judge whether it is secure. TCG defines this process as the remote attestation. The remote attestation scheme of TCG is as follows:

1. V: create non-predictable 160bit nonce
2. V→A : ChReq(nonce)
3. A attests platform integrity
   a. A: load protected $\mathrm{AIK}_{\mathrm{priv}}$ into TPM
   b. A: retrieve Quote =$\mathrm{sig}\{\mathrm{PCR}, \mathrm{noce}\}_{\mathrm{AIK}_{\mathrm{priv}}}$
   c. A: retrieve Measurement List ML
4. A→V: ChReq(Quote, ML)
5. V verifies the attestation
   a. V: determine trusted cert ($\mathrm{AIK}_{\mathrm{pub}}$)
   b. V: validate $\mathrm{sig}\{\mathrm{PCR}, \mathrm{noce}\}_{\mathrm{AIK}_{\mathrm{priv}}}$
   c. V: validate nonce and ML using PCR

--A:Attestor
--V:Verifier

It can be found that there exist the following shortcomings through analysis: ①The verifier initiates authentication request, and the attestor returns the platform configuration information. However, the interactive terminal is the attestor which initiates attestation request in Smart Grid. The attestation model is not suitable for Smart Grid. ②There is the risk of network intrusion in the TCG scheme. The intruder can make attacks to the remote attestation through interception, tampering and reply attacks in the network. Take the above remote attestation as example, A does not validate the identity of V, so if V is an intruder, it can get the attestation information of A and prove to another V as the man in the middle. In addition, the intruder can eaves drop the communication messages between A and V and get the plaintext of ML (Measurement List) in order to know the specific platform configuration and running software of A. On this basis, the intruder can attack A by using targeted virus and Trojan horse without scanning A.

In view of the above problems, this paper proposes a remote attestation model sponsored by attestor which is based on the binary certificate and combined with the practical application environment and designs according remote attestation protocol. The security of electric power information intranet operation system, the operation environment of interactive terminal and the credit of the identity is ensured by applying domestic security chips TCM carrying on integrity checking, authentication and data encryption transmission for the operating environment of interactive terminal, which will prevent interaction terminal from being controlled maliciously. The model not only provides security solutions for a large number of accesses of interactive terminals in the Smart Grid, but also explores applications of trust computing technology in smart grid mobile security, which is of realistic directive meaning.

In this paper, Section 2 introduces remote attestation related research work. Section 3 proposes a remote attestation model sponsored by attestor. Section 4 designs a corresponding remote attestation protocol. Section 5 analyzes the performance and characteristic of the protocol. Section 6 is the acknowledgements.

2. Related-Work Introduction

TCG gives the basic framework of remote attestation and an evaluation model based on the trust chain in trusted computing architecture [1]. Many domestic and foreign scholars and research institutions carried out a lot of study of remote attestation under the framework.

In the binary proof, the IBM institute put forward an integrity measurement scheme IMA [2]. The scheme measures the operational entities on Linux system and generates a unique identifier for them. The verifier takes TPM as trusted root to judge the attestor in remote attestation. On the basis of IMA, T. Jaeger *et al.*, proposed a policy-reduced integrity measurement architecture PRIMA [3]. The scheme make specification based on C-W information flow model for the entities needed to be attested and prevented the platform configuration exposure during the remote attestation to a certain extent.

Poritz, *et al.*, initiatively proposed property-based remote attestation scheme from the system architecture [4, 5]. The scheme solved the privacy problem during the remote attestation and ensured the flexibility of the solution.

In the proof mechanism, Ulrich Kühn, *et al.,* gave the software and hardware implementation of property-based remote attestation in the literature [6]. The literature [7, 8] gave out behavior-based remote attestation.

In the remote attestation protocol, Chen put forward property-based remote attestation protocol [9]. The literature [10] proposed a scheme which used remote attestation to extend SSL protocol. The communication terminals established trusted channel by negotiating security parameters and attesting platform configuration in SSL.

In the remote anonymous attestation, the literature [11] used ring signature to realize direct anonymous attestation. The literature [12] studied the methods of establishing the anonymity of trusted terminal platform based on TPM chip.

3. A Remote Attestation Model Sponsored by Attestor

3.1. The Existing Remote Attestation Model

Generally, the typical remote attestation models are as follows: direct attestation model, the “pull” model, the “push” model and the agent model. The attestor provides platform information and waits attested. While the verifier performs remote attestation on the object need to be attested. These four models have their own advantages and disadvantages.

(1) Direct attestation model

As shown in Figure 1, at the beginning, the verifier initially sends remote attestation request to the attestor. And then the attestor encrypts the measurement values of the platform configuration information stored in PCR and returns them to the verifier. At last, the verifier only needs to validate received messages. The verifier and the attestor interact between each other without any trusted third party in this model. But some limitation exists in it. The verifier needs huge integrity database in the hardware layer. Also, the integrity information provided by the attestor is easy to leak to potential untrusted verifier and its safety cannot be well protected.

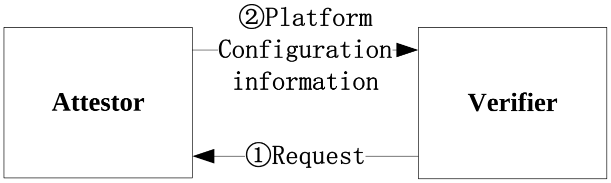

Figure 1. Direct Attestation Model

(2) “Pull”model

This model is similar to the direct model, as shown in Figure 2. Its advantage is the verifier does not need verification ability and only relies on trusted third party (TTP). It can lighten the verifier’s load. But it has the same disadvantage as the above that the private information of the attestor is easy to leak.

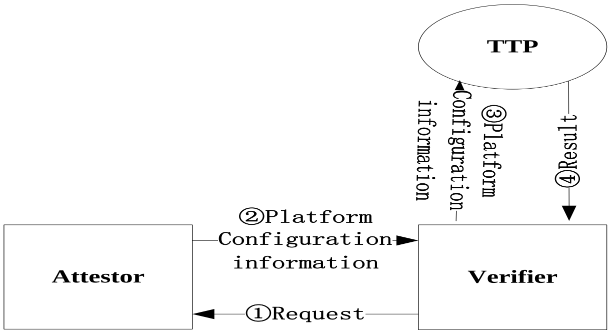
TTP
③Platform Configuration information
④Result
Attestor
Verifier
②Platform Configuration information
①Request

Figure 2. Pull Model

(3) “Push” model

In this model, the attestor pushes all information needs to be attested to TTP. After validating the information, TTP returns certificates to the attestor. The verifier only needs validate attestor’s certificates. As shown in Figure 3. There are some advantages. Above all, it ensures the platform privacy. Secondly, TTP will not have interactive congestion. Once again, the certificates can be used in subsequent communication. Yet it is not suitable for dynamic remote attestation. The change of platform configuration will directly affect the certificates issued by TTP. The certificate revocation problem has to be solved.

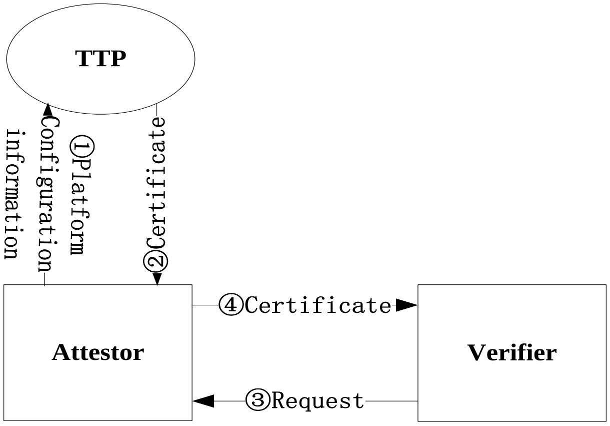

Figure 3. Push Model

(4) Agent model

As shown in Figure 4. The verifier firstly sends remote attestation request to TTP. Then TTP interacts with the attestor and gets platform configuration information from it. At last, TTP returns certificates to the verifier. The verifier validates the attestor. The great virtue of this model is less direct interaction between verifier and attestor. But it increases TTP's burden.

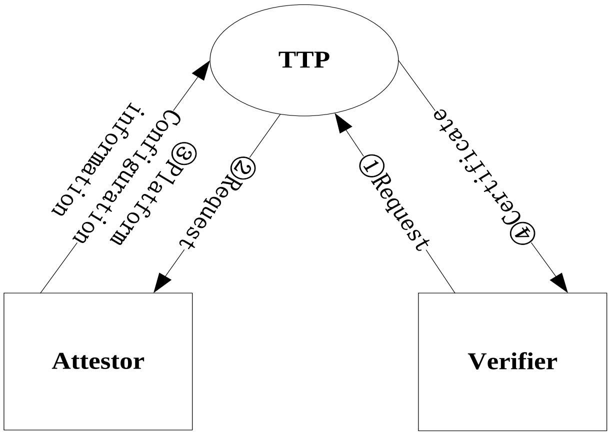

Figure 4. Agent Model

3.2. The Remote Attestation Model Sponsored by Attestor

In view of the defects of traditional remote attestation model, this paper provides a model sponsored by attestor applied to SGIT trusted access. Although the private CA (PCA) is also involved, it is not the policymaker. Its decision only plays reference role, the real policymaker is the verifier. In this case, the private CA and the attester can't intrigue with each other. In this model, PCA is responsible for issuing AIK (Attestation Identity Keys) certificates to attestor and identity certificates to verifier, as well as assisting verifier authenticating integrality of attestor online. In practical use, the verifier gets the root certificate of PCA through security measures in advance, while the PCA won't authenticate the certificate online, thus it can reduce communication overhead. The model is shown in Figure 5.

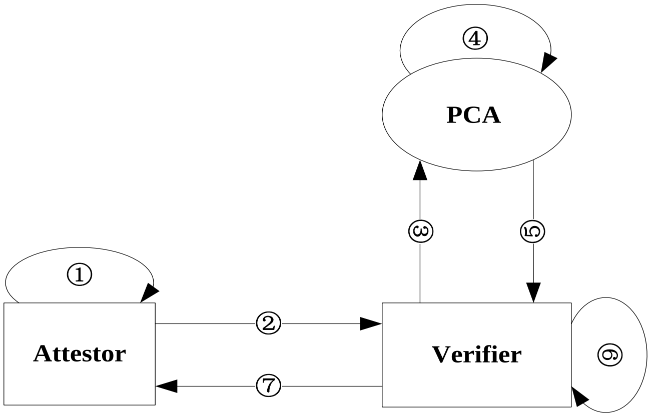

Figure 5. The Remote Attestation Model Sponsored by Attestor

Assumption 1: The attestor and the verifier achieve public key certificates issued by PCA including public key, period of validity, signature and so on. The certificates are imported into TPM before. In order to express simply, we use A to represent attestor, V to represent verifier, P to represent trusted CA. For an entity X, its identity certificate is as follows:

$$\mathrm{Cert_X} = \{\mathrm{ID_X}, \mathrm{Q_X}, \mathrm{V_X}, \mathrm{E_{D_P}}(\mathrm{ID_X}, \mathrm{Q_X}, \mathrm{V_X})\}$$

Among these, $\mathrm{ID_X}$ is the unique identifier of X, $\mathrm{Q_X}$ is the public key of X, $\mathrm{V_X}$ is the period of validity of $\mathrm{Cert_X}$, $\mathrm{D_P}$ is the private key of trusted third party, $\mathrm{E_{D_P}}$ represents encryption using private key $\mathrm{D_P}$.

Assumption 2: The function of A is simple and don't need update frequently. Thus we assume that the initial running environment of SGIT is secure. When A communicates with V for the first time, V stores integrity measurement values only and delivers them to PCA rather than authenticating integrity.

The signs related are defined below.

M denotes message, $\mathrm{Q_X}$ denotes the public key of the entity X, $\mathrm{D_X}$ denotes the private key of X, $\mathrm{R_X}$ denotes the random generated by X, S' denotes the digital signature, V'denotes the signature verification result, C denotes the certificate verification result, F denotes the determination from V, $\mathrm{F} \in \{0,1\}$.

$\mathrm{S}' = \mathrm{Signature}\{\mathrm{M}\}_{\mathrm{D_X}}$means signing M with the private key of X, and the result is S'.

$\mathrm{V}' = \mathrm{Verify}\{\mathrm{M}, \mathrm{S}'\}_{\mathrm{Q_X}}$means verifying the signature value S' of M with the public key of X, and the result is $\mathrm{V}'.\mathrm{V}' \in \{0,1\}$.

$\mathrm{C} = \mathrm{CertVerify}\{\mathrm{Cert_X}, \mathrm{Cert_{rootP}}\}$ Means verifying X's certificate with the root certificate of the private CA, and the result is C. $\mathrm{C} \in \{0,1\}$.

The process of remote attestation is as following.

①The TPM embedded in a measure the integrity of the platform configuration and saves the integrity value into PCR, then signs the value and the random $\mathrm{R_T}$with the private key of AIK. $\mathrm{S}' = \mathrm{Signature}\{\mathrm{PCR}, \mathrm{R_A}\}_{\mathrm{D_{AIK}}}$

②A encrypts PCR, ML (Measurement List) and $\mathrm{R_A}$ with the public key of V and sends it to V with its certificate $\mathrm{Cert_{AIK}}$and S'.

③V stores PCR, ML,$\mathrm{Cert_{AIK}}$andS', and sends the PCR encrypted with the public key of the private CA to the private CA.

④The private CA compares the value stored in database with the PCR decrypted with the private key of its own.

⑤The private CA returns the result to TAS.

⑥V proceeds to the next step according to the measurement results of PCA. If PCA returns false, V directly returns F=0 to A. Otherwise, V verifies the AIK certificate with the root certificate of the private CA, $\mathrm{C} = \mathrm{CertVerify}\{\mathrm{Cert_{AIK}}, \mathrm{Cert_{rootP}}\}$, and verifies the signature S' with the public key of AIK, $\mathrm{V} = \mathrm{Verify}\{\mathrm{PCR}, \mathrm{R_A}, \mathrm{S}'\}_{\mathrm{Q_{AIK}}}$, and then validates ML with PCR. If all verification is passed, then the integrity verification is successful. Otherwise, the communication is terminated.

⑦V returns F to A. A determines what to do next according to the value of F.

3.3. Application for AIK Certificates

Through AIK certificates, a trusted terminal can indentify itself. We can take AIK certificate as "identification card" in communication. AIK certificates are corresponding to private keys lie in TPM. The private keys of AIK are used to signing data generated by TPM.

An entity signed by AIK shows that it is treated by TPM, thus can either guarantee the source of data or provide data non reputation.

A appeals AIK certificates to PCA, after authentication the certificate is issued to A and stores into TPM at the same time. Figure 6 shows the procedure of application.

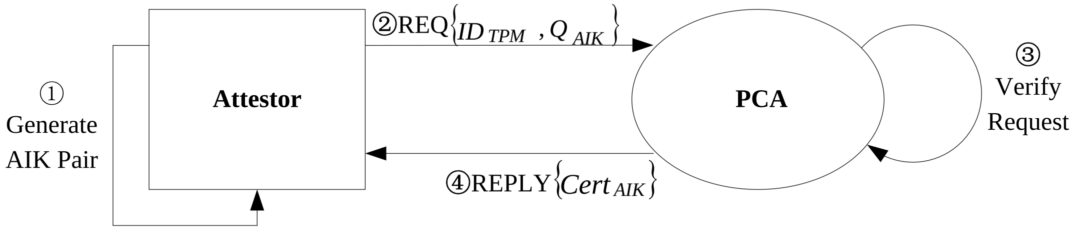

Figure 7. Application Procedure of AIK Certificates

①A uses key generator in TPM to generate RSA public and private key pair, and store the private key in a secure location in TPM.

②A sends information such as unique identifier of TPMID$_{TPM}$, AIK certificate and public key Q$_{AIK}$ to PCA to apply for AIK certificate.

③ PCA authenticates information presented by A and generate an AIK certificate using PCA private signature if authenticated.

④PCA issues AIK certificate to A and authorizes it to access private network. A puts the certificate into TPM for communication later.

In practical use, every interactive terminal should appeal AIK certificates to PCA for the use of identifying itself. The AIK private key is protected in TPM from being stolen. The certificate is appealed offline.

4. The Design of Remote Attestation Protocol

In the remote attestation of Smart Grid, SGIT denotes attestor, while the trusted access server (TAS) located on the network boundary denotes verifier. The trusted authentication is divided into three steps. Firstly, both communication sides verify the identity each other to realize the identity trusted between two parties involved. Secondly, TAS verifies the integrity of SGIT platform configuration to ensure the credibility of the terminal running environment. At last, both sides make session key agreement. Doubtlessly, it can enhance communication security through the above steps. The certification process is showed in Figure 5. S denotes SGIT, T denotes TAS.

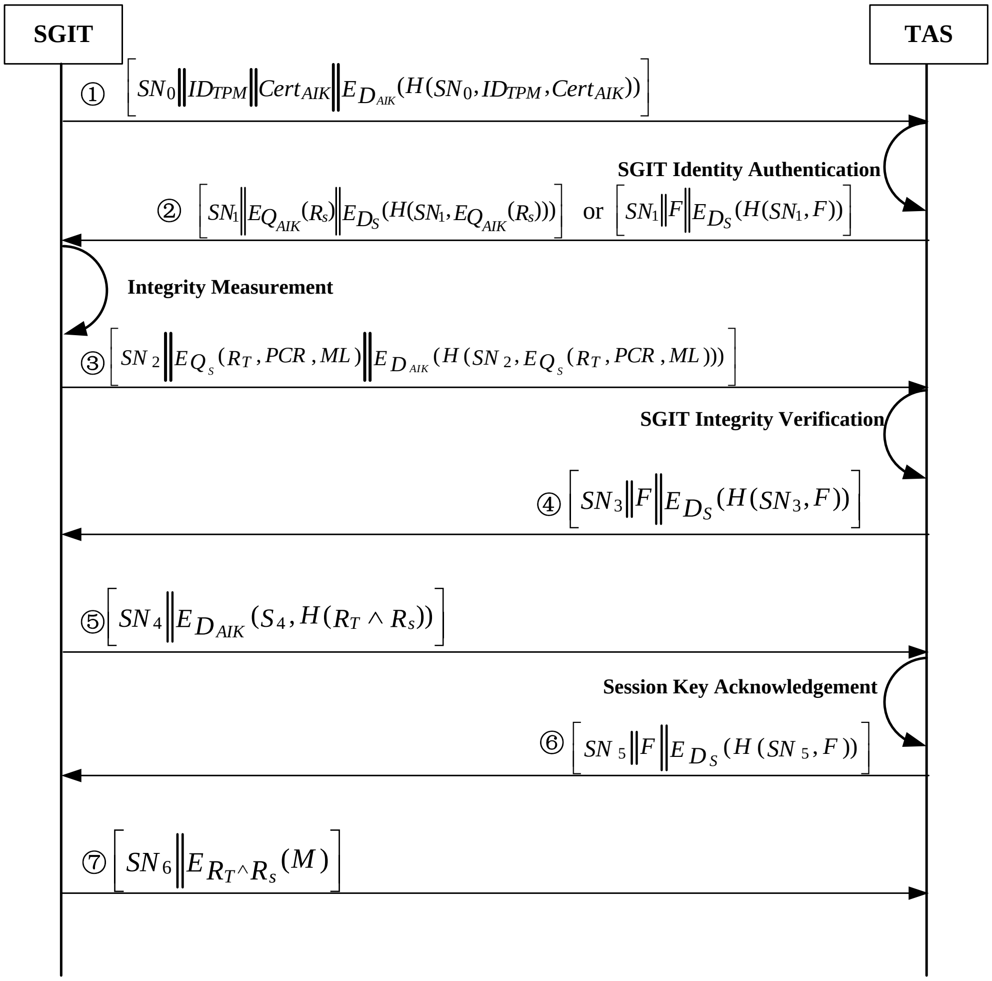
SGIT
TAS
① $[SN_0 \| ID_{TPM} \| Cert_{AIK} \| E_{D_{AIK}}(H(SN_0, ID_{TPM}, Cert_{AIK}))]$
SGIT Identity Authentication
② $[SN_1 \| EQ_{AIK}(R_s) \| E_{D_S}(H(SN_1, EQ_{AIK}(R_s)))]$ or $[SN_1 \| F \| E_{D_S}(H(SN_1, F))]$
Integrity Measurement
③ $[SN_2 \| E_{Q_s}(R_T, PCR, ML) \| E_{D_{AIK}}(H(SN_2, E_{Q_s}(R_T, PCR, ML)))]$
SGIT Integrity Verification
④ $[SN_3 \| F \| E_{D_S}(H(SN_3, F))]$
⑤ $[SN_4 \| E_{D_{AIK}}(S_4, H(R_T \wedge R_s))]$
Session Key Acknowledgement
⑥ $[SN_5 \| F \| E_{D_S}(H(SN_5, F))]$
⑦ $[SN_6 \| E_{R_T \wedge R_s}(M)]$

Figure 8. The Trusted Authentication Protocol

① SGIT → TAS: $[SN_0 \| ID_{TPM} \| Cert_{AIK} \| E_{D_{AIK}}(H(SN_0, ID_{TPM}, Cert_{AIK}))]$

SGIT binds the ID of TPM and AIK digital certificate with hash algorithm, encrypts the hash value with the private key of AIK, and then sends the signature to TAS. SN is the communication serial number. It is set randomly by SGIT to prevent replay attacks.

② TAS → SGIT: $[SN_1 \| E_{Q_{AIK}}(R_S) \| E_{D_S}(H(SN_1, E_{Q_{AIK}}(R_S)))]$

After receiving the message from SGIT, TAS uses the public key of AIK to verify the validity of signature, hashes SN_0,ID_{TCM}, SIM, and $Cert_{AIK}$ to judge whether the message is modified. Then TAS uses the root certificate of PCA to the SGIT identity. If the verification is passed, TAS generates a random R_S and encrypts it with the public key of AIK and sends it to SGIT. Otherwise, TAS returns a state value F to SGIT and terminates the communication.

③ SGIT → TAS: $[SN_2 \| E_{Q_S}(R_T, PCR, ML) \| E_{D_{AIK}}(H(SN_2, E_{Q_S}(R_T, PCR, ML)))]$

SGIT measures the integrity of platform configuration and generates a randomR_T, then encrypts PCR, ML and R_T with the public key of TAS, sends the cryptograph and signature to TAS to request for integrity verification.

④ TAS → SGIT: $[SN_3 \| F \| E_{D_S}(H(SN_3, F))]$

TAS gets PCR andR_T, measures the integrity of SGIT according to the steps in 3.2. Then returns the state value F to SGIT. If the integrity verification is passed, TAS combines $R_S$and $R_T$together to form the session key, otherwise TAS terminates the communication.

⑤ $SGIT \rightarrow TAS: [SN_4 \| E_{D_{AIK}}(SN_4, H(R_S \wedge R_T))]$

SGIT determines what to do next according to the value of F. If the integrity verification is passed, SGIT combines $R_S$and $R_T$together to form the session key and send it to TAS to make session key agreement.

⑥ $TAS \rightarrow SGIT: [SN_5 \| F \| E_{D_S}(H(SN_5, F))]$

TAS hashes the session key in step ④ and compares it with the hash value received from SGIT. Then returns F to SGIT. If the two values are equal, the session key is determined. Otherwise, the communication is terminated.

⑦ $SGIT \rightarrow TAS: [SN_6 \| E_{R_S \wedge R_T}(M)]$

The communication begins. SGIT encrypts message with the session key $R_S \wedge R_T$ and sends it to TAS.

5. The Analysis of Remote Attestation Protocol

5.1. Performance Analysis

(1) Efficiency

The trusted access mechanism in this article can reduce communication overhead and lower the timely issuing certificates load of PCA through the way of applying for the certificates offline. All interactive terminals apply to PCA for the AIK certificate before accessing and import the TAS certificate into TPM in advance. The exchange process of certificate doesn't need when subsequent communication shaking hands. The probability of successful data transmission can be greatly enhanced in the case of instable mobile communication network signals.

The encryption arithmetic and the random number generation in this article's trusted access mechanism which are completed by TPM chips do not consume terminal CPUs' computing capability and do not affect the normal and stable operation of the business program for the interactive terminals of limited resources and computing capabilities. As an independent computing unit, TPM can accelerate the implementation of the agreement and improve the efficiency of accessing.

Trusted access mechanism of this article authenticates identity legitimacy and credibility of the platform in the first round of interaction. If the verification fails, TAS will terminate the agreement after the first round of protocol interaction and reject the terminal accessing, which can reduce the TAS execution load to a certain extent.

(2) Controllability

The implementation of controllability relies on a unique identification number ID_TPM of TPM and the hardware features of the terminals. By binding both, all of the service requests can be ensured from the same terminal while during the authority time of available AIK certificates.

(3)Resistance to offensive

Transmission data can be operated just as interception, eavesdropping and analysis by passive attack. Therefore, the secure password system can ensure the ability to resist passive attack of the authentication protocol in this article. Random number introduced in access mechanism, the use of entity names of both sides of the communication and remote attestation method based on verifier can resist active attacks such as counterfeit attacks, replay attacks and MITM attacks.

5.2. Characteristics Analysis

The protocol in this article has the following characteristics:

(1)All certificates are the offline mode and TAS certificate will be imported into the terminal in advance, which reducing the certificate change process during communications. This not only reduces the burden of PCA communication, but also improves the efficiency of communication.

(2)The message length of the authentication protocol in this article is shorter and the identity of the terminal has already been verified in the first interaction round, which is to adapt to the defect of failing connecting the network and high bit error rate in the mobile communication network caused by factors such as communication bandwidth, instable signal and excessive data package.

(3)Terminal platform integrity verification adopt dual authentication. While PCA is only as a middle party verification, the final decision is determined by the TAS through comparing the verification results of PCA and its own, which could prevent the situation that terminals and PCA collude to cheat TAS. While there may be a corresponding increase in the communication handshake, communication efficiency is not influenced significantly.

(4)Communication process is divided into three stages that include terminal authentication, integrity measurement and session key agreement. Validation in any stage fails, which will directly interrupt the handshake and timely release the communication bandwidth.

(5) Encrypted communications only encrypt the application layer data, which will not affect the normal operation of the power business itself.

6. Conclusions

In view of the defects of traditional remote attestation model, this paper proposes a remote attestation model sponsored by attestor which is based on the binary certificate and combined with the practical application environment. Also, the remote attestation protocol is designed. The model can ensure the legitimate identity of the communicating parties and the accurate verification of terminal platform integrity, and guarantee that only the terminals which has trusted identities and trusted operating environment can access the information intranet. The result that analyzes the performance and characteristics of the access mechanism shows that the smart grid interactive terminal trusted access mechanism proposed in this article is of safety, efficiency and practicality.

Acknowledgements

The authors are thankful to those who have helped them with encouragement, advice, information and material, especially Wenchao Cui, Yun Zhang and Dong Zhang who have contributed to the research.

References

[1] "Trusted Computing Group", TCG Infrastructure Working Group Reference Architecture for Interoperability, **(2005).**

[2] R. Sailer, X. Zhang, T. Jaeger and L. Van Dorn, "Design and Implementation of a TCG-based integrity measurement architecture", Proceedings of the 13th Conference on USENIX Security Symposium, **(2004)** August 9-13, San Diego, CA USA.

[3] T. Jaeger, R. Sailer and U. Shankar, "PRIMA: policy-reduced integrity measurement architecture", Proceedings of the 11th ACM Symposium on Access Control Models and Technologies, **(2006)** June 7-9, California, USA.

[4] A.-R. Sadeghi and C. Stüble, "Property-based attestation for computing platforms: caring about properties, not mechanisms". Proceedings of the New Security Paradigms Workshop 2004, **(2004)** September 20-23, Nova Scotia, Canada.

[5] J. Poritz, M. Schunter and E. V. Herreweghen, "Property Attestation-Scalable and Privacy-Friendly Security Assessment of Peer Computers", IBM Research, Technical Report, vol. 3548, **(2004).**

[6] U. Kühn, M. Selhorst and C. Stüble, "Realizing property-based attestation and sealing with commonly available hard- and software", Proceedings of the 2nd ACM Workshop on Scalable Trusted Computing, **(2007)** November 2, Alexandria, VA, USA.

[7] X. Z. MasoomAlam, M. Nauman, T. Ali and J.-P. Seifert, "Model-based behavioral attestation", Proceedings of 13th ACM Symposium on Access Control Models and Technologies, **(2008)** June 11-13, Estes Park, CO, USA.

[8] X.-Y. Li, C.-X. Shenand and X.-D. Zuo, "An Efficient Attestation for Trustworthiness of Computing Platform", Proceedings of 2006 International Conference on Intelligent Information Hiding and Multimedia Signal, **(2006)** December 18-20, Pasadena, California, USA.

[9] L. Chen, R. Landfermann, H. Löhr, M. Rohe, A.-R. Sadeghi and C. Stüble, "A protocol for property-based attestation", Proceedings of the 1st ACM Workshop on Scalable Trusted Computing, **(2006)** November 3, Alexandria, VA, USA.

[10] Y. Gasmi, A.-R. Sadeghi, P. Stewin, M. Unger and N. Asokan, "Beyond secure channels", Proceedings of the 2nd ACM Workshop on Scalable Trusted Computing, **(2007)** November 2, Alexandria, VA, USA.

[11] L. Ji-Qiang, Z. Jia and Z. Yong, "Study of Remote Automated Anonymous Attestation in Trusted Computing", Chinese Journal Of Computers, vol. 32, no. 7, **(2009).**

[12] Y. Ai-Ming, C. Xiao-Bo and F. Deng-Guo, "Research of Platform Anonymous Identity Management Based on Trusted Chip", Chinese Journal Of Computers, vol. 33, no. 9, **(2010).**

Authors

Kehe Wu, he received his M.Sc. in Mechatronics (1995) and PhD in Computer Sciences (2005) from North China Electric Power University. He is currently a professor in information security in North China Electric Power University. He is a Director of the Chinese Association for artificial intelligence and a Senior Member of China Electric Power Information Standardization Committee. His current research interests include different aspects of Intelligent Software, Cloud Computing and Information Security.

Fei Chen, he received his undergraduate degree in Software Engineering (2008) from North China Electric Power University. Now he is a PH.D. Candidate in Control and Computer Engineering of North China Electric Power University. His research interest is mainly in the area of electric information security and Trusted Computing and he has published several research papers in scholarly journals and international conferences in the above areas.

Yi Li, he received his BS degree in computer science and technology from North China Electric Power University, Beijing, China, in 2010. He is now studying the PhD of computer application technology in North China Electric Power University, Beijing, China. His current research interests include Cloud Computing, Distributed Storage and Networking.