International Journal of Grid and Distributed Computing
Vol.7, No.2 (2014), pp.185-198
http://dx.doi.org/10.14257/ ijgdc.2014.7.2.17

Access Mechanism of Interactive Terminals of Smart Grid

Kehe Wu, Fei Chen and Yi Li

Department of Control and Computer Engineering School, North China Electric Power University,
NO.2 Beinong Road, Changping District, Beijing 102206, China
epuwkh@126.com, chenfei0428@126.com, liyi174748@163.com

Abstract

SGIT(Interactive Terminal of Smart Grid) access to the intranet of electric power information, expanding the boundaries of network protection and bringing in risks of security. Based on safe requirement and trust computing theory, TCM(Trust Cryptographic Module) and TAS(Trust Access Server) are introduced to Interactive terminals and boundary of information network respectively. Trusted operating environment, trusted identity and credible communication are ensured through the cooperative work of TCM and TAS, which makes terminals be accessed credibly. The emphasis is the remote attestation model and trusted authentication protocols based on the verifier. The analysis of this mechanism was made, which indicates that this mechanism can make sure the credible access of SGIT and has practical application value.

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

1. Introduction

As the current hot spot of the global power industry, Smart Grid guides the future development direction of the grid. Interaction which refers to the bidirectional information and energy interactions between grid and users or between users is one of the major features of the Smart Grid. These bidirectional interactions, on the one hand, could collect and analyze users' electricity consumption data scientifically, which will be the basis for decision-making, on the other hand, will master users' electrical behavior to distribute electric load rationally. In order to achieve interactions, a large number of interactive terminals (such as smart meters, smart collection terminals, *etc*.,) with functions of measurement and communication are applied to the Smart Grid. These terminals 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. Due to the interactive terminals which were based on open embedded operating system design and implementation and utilize open communication protocols to transfer data, network security issues also spread to the Smart Grid. Currently, traces of hacker activities have also been founded in domestic and overseas electric power information system. How to achieve secure access of interactive terminals which could ensure the safety and stable operation of the Smart Grid has become an extremely urgent task.

At present, the existing network security solutions use two security protocols such as SSL/TLS or IPSec to get identity authentication for terminal, which can ensure the confidentiality and integrity of data transmission. However, the direct application of the two security protocols which access to the Smart Grid interactive terminal has the following three

ISSN: 2005-4262 IJGDC

issues. Primarily, the software and hardware environment of the interactive terminal using these two protocols is not feasible; Secondly, the two protocols do not consider the credibility of the terminal and have not tested the operating environment of the terminal, so it cannot guarantee the safety of the interactive terminal which access to the intranet. Furthermore, the amount of information to be exchanged in handshake process of the two protocols is relatively large. In the instable mobile signal, interactive terminals with poor network-processing capabilities cannot complete the handshake process, which will result in that data cannot be sent timely and control commands cannot be received timely. Existing terminal security solution is to embed specific security chips MTM(Mobile Trusted Module) in the terminal [3], which establishing credible security mechanism in the terminal to ensure the credible identity and operating environment of the terminal. Because the hardware and software environment of the interactive terminal is much simpler than PC and mobile terminals, the trust computing technology is easier to implement in interactive terminals. Although there already are some related researches that combine them both to solve the security access issues of the terminal, which are not suitable for the access of the Smart Grid interactive terminal.

For the above-mentioned issues, this article which is based on the trust computing theory and combine with the application environment of the Smart Grid interactive terminal designs interactive terminal credible access mechanism. 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. This mechanism 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 trusted computing related research work; Section 3 analyses risks and requirements of interactive terminal security access in Smart Grid; Section 4 proposes a credible access mechanism of SGIT and makes detailed analysis of the process of interactive terminal credible access; Section 5 analyzes the performance and characteristic of the mechanism. Section 6 is the acknowledgements.

2. Related-work Introduction

This field is explored by many researchers and research institutions which are abroad or domestic, and certain achievement was accomplished.

TCG mobile work team is devoted to expanding TCG related regulations, which will be used to solve the security problems of mobile platform. Corporations like Intel, IBM, NTT bring out the mobile terminal credible research program based on TCG and MTM, as well as the software structure, hardware structure and protocol specifications of trusted mobile platform [4].

Such trust computing related research is also processed in China and TCM standards with proprietary intellectual property rights is established has been formulated so that security chips which support TCM standard is manufactured by domestic IT manufacturers successively. Literature [5] brings out trusted mobile platform structure based on MTM, which is due to the characteristic of mobile terminal. Literature [6] focuses on the network user identity management puzzles and drawbacks of identity management solutions and puts forward the management plan and the protocol of trusted identity which is based on trust computing integrity check, protected storage, remote platform parity and such safe characteristics. Literature [7] focuses on the change of mobile terminal communication mode due to MTM chip and raises dependable mobile platform access mechanism based on mobile internet, then

designs the domain access and cross-domain access. Literature [8] proposes a complete dynamic update attestation scheme for Multiple Remote Attestation Instance in trust computing environment and researches on dependable computing long-distance method of prove based on TCM. Literature [9] researches on the application of trust computing method on electricity substation automation telecommunication and introduces trust computing modules into capacity electronic equipment then expands trust relationship to far-end through remote procedure call. Literature [10] presents the framework of a hierarchical distribution multi-agent active communication security defense utilizing Trusted Computing Theory and applies it to transformer substation communication security by using trust computing. Literature [11] puts forward the scheme of using remote attestation to expand SSL agreement, consultation on communication terminal safety parameters and attestation platform configuration on SSL, which will achieve the target on building remote dependable access.

3. Requirements of Interactive Terminal Security Access

3.1. Division of interactive application security domain

The Interactive Applications can be divided into three domains: Interactive Terminal Domain, Access Transmission Domain and Business Application Domain.

(1) Interactive Terminal Domain. It refers to equipments (*etc.*, smart electric meters, smart collection terminals and POS terminals) which access to mobile communication network through mobile communication modules. Specifically, it contains physical equipments, hardware and software.

(2) Access Transmission Domain. It mainly refers to mobile communication networks including GSM, CDMA and WCDMA to provide mobile communication services. Interactive terminals can access intranet application systems through this domain.

(3) Business Application Domain. This domain is constituted by kinds of application systems. It is responsible for receiving data from interactive terminals and deliver control commands to them in time.

From the aspect of security protection technology, the technologies in interactive terminal domain and business application domain mainly base on system security protection implementation. However, in access transmission domain, it mainly based on network security technology implementation [12].

3.2. Security Risks and Requirements

As there are differences between these security domains illustrated above in environment and characteristic, for the analysis of security risks and requirements in these domains, the environment and characteristic is depicted below.

(1) Interactive Terminal Domain. For the aspect of hardware, it utilizes the universal architecture based on ARM, and for software, it use embedded operating systems such as WINCE and Windows Mobile and use mobile communication generally support TCP/IP protocols to communicate with others. Equipments in this domain lie in remote location which is incredible and easy to lose.

(2) Access Transmission Domain. This domain is generally constituted by mobile communication networks and network infrastructure constructed by electric power or mobile service provider. It adopts standard protocols and restrict in maintenance and management.

(3) Business Application Domain. From aspects of hardware, software, network and storage, they all based on open standard technology architecture. Form the aspect of physical environment, equipments and systems can be located in trusted internal locations generally. The management system must be strictly followed for information systems during the time of running, using and maintaining.

Table 1 presents security risks each domain faced based on the analysis above.

Table 1. Analysis of Security Access Risks

Security Domain	Security Category	Risks	Description of Security Risks
Interactive Terminal Domain	Physical Security	Tampering of Equipments	The attackers can achieve data through tampering hardware or software using physical measures
		Loss of Equipments	Interactive terminals may lost and be achieved by potential attackers
	System Security	Masquerade of Equipments	Attackers may access to systems using unauthenticated equipments
		Malicious Software	Attackers may install software which may compromise the system
	Application and Data Security	Data Reveal & Destroy	Attackers may achieve or tamper data lie in equipments to attack the system
Access Transmission Domain	Link Security	Security Access	Unauthorized attackers access to mobile networks
	Transmission Security	Data Stealing & Destroy	Attackers may steal or compromise data in transmission
Business Application Domain	Network Security	Unauthorized Access of Equipments	Unauthenticated interactive terminals access to intranet
	Application and Data Security	Data Stealing & Destroy	Attackers probe into systems to steal or compromise application data
		Masquerade of Users	Unauthenticated users masquerade as authenticated users to access to the system

On the basis of analysis above, under the environment of Smart Grid, for Access Transmission Domain and Business Application Domain, physical equipments involved are managed and maintained well commonly, and access and transmission network utilize specified and strictly managed mobile communication network as bearing bed. As the business network has been divided and separated and has taken many kind of protection measures, the two domains mentioned above are not the keynote of trusted access mechanism concerned in this paper. While the Interactive Terminal Domain adopts open architecture and system platform, it lacks of corresponded security protection technologies, together with exposed to incredible environment, thus we put most concentration on this domain. Table 2 presents the analysis of security requirements in these domains.

Table 2. Analysis of Security Requirements

Security Domain	Security Category	Description of Security Requirements
Interactive Terminal Domain	Physical Security	Physical tampering protection
	System Security	Equipment identifying and discrimination; Configuration integrality protection; Protected computing environment
	Application and Data Security	Data confidentiality and integrality protection; Data self-destruction
Access and Transmission Domain	Link Security	Mobile terminal discrimination; Network access control; Network access audit
	Transmission Security	Data confidentiality, integrality and non-repudiation
Business Application Domain	Network Security	Interactive terminal access control
	Application and Data Security	User management; Terminal management; System integrality protection; Data confidentiality and integrality protection; security audit; System and data disaster recovery

With the development and application of smart grid interactive business, the requirement of interactive terminals will become more and more bigger. To make use of the advantage brings by interactive businesses and control the introduction of new kind of security risks at the same time, an interactive terminal access architecture should be constructed. For interactive terminal access, information security protection mainly focuses on two aspects as follows:

(1) Trusted interactive terminals. Trusted behavior of a terminal, on one hand, refers to the terminal only execute predetermined business logic while it won't execute logic make by other

attackers, on the other hand, the operational environment of the terminal is trusted and can get rid of malicious software.

(2) Controlled business applications. Firstly, interactive terminals are controlled to business application accesses thus only authenticated terminals can access to specified applications; secondly, interactive terminals can do nothing but transmit data to business applications positively and receive and perform control commands passively.

4. Trusted Access Mechanism of Smart Grid Interactive Terminals

The trusted access mechanism of smart grid interactive terminals introduced in this paper implements trusted access of interactive terminals through embed TCMs into SGITs, at the same time, introduce PCA (Private CA) to issue certificate to SGITs and deploy TAS on network boundary as policy deciders.

Figure 1 shows the trusted access mechanism in this paper. The entities involved mainly are SGIT, ISP, TAS and PCA. Among these, SGITs are entities which request access to systems and there are interactive terminals embedded TCMs. SGITs are responsible for sending access requests, receiving creditability measure and send it to TAS and wait for TAS returning evaluate results; ISP refers to Internet Service Provider, it provides APN service to interactive terminals; TAS is responsible for managing all the interactive terminals and authenticate whether the identity and running environment of TCM is trusted, on the basis of evaluate result TAS sets the corresponding access control policies to determine which application SGIT can access strictly; PCA is responsible for issuing AIK (Attestation Identity Keys) certificates and identity certificates for TCM and issuing SIM cards, as well as assists TAS authenticating integrality of SGIT online. When in practical use, TAS achieve the root certificate of PCA through security measures before to authenticate SGIT, while PCA won't authenticate the certificate online, thus it can reduce communication overhead.

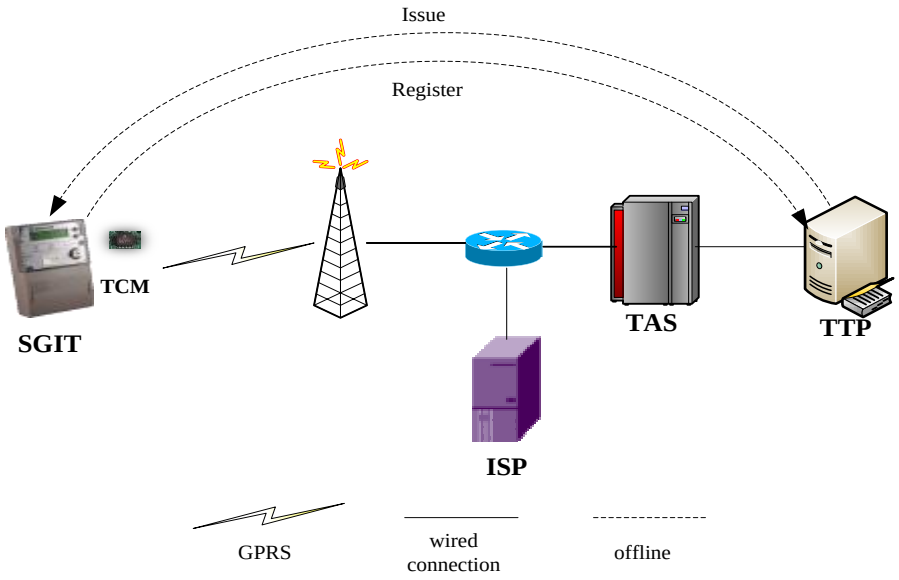

Figure 1. Smart Grid Interactive Terminal Access Mechanism

Assumption 1: SGIT and TAS achieve public key certificates issued by PCA including public key, period of validity, signature and so on. The certificate are imported into SGIT

before. We use T to represent terminals, S to represent servers, P to represent trusted CAs. For an entity X, its identity certificate can be depicted 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 SGIT is simple and don't need update frequently. Thus we assume that the initial running environment of SGIT is secure. When an SGIT communicates with TAS for the first time, TAS stores integrity measure only and deliver it to PCA rather than authenticating integrity.

4.1. 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 TCMs. The private keys of AIK are used to signing data generated by TCMs. An entity signed by AIK shows that it is treated by TCM, thus can either guarantee the source of data and provide data non-repudiation.

SGIT appeals AIK certificates to TTP, after authentication the certificate is issued to SGIT and stores into TCM at the same time. Figure 2 shows the procedure of application.

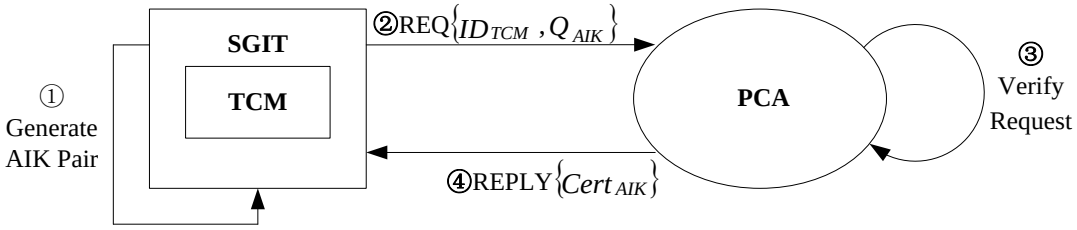

Figure 2. Application Procedure of AIK Certificates

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

② SGIT send information such as unique identifier of TCM $\mathrm{ID_{TCM}}$, AIK certificate and public key $\mathrm{Q_{AIK}}$ to PCA to apply for AIK certificate.

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

④c PCA issues AIK certificate and the corresponding SIM card to SGIT, authorize it to access private network. SGIT put the certificate into TCM 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 TCM from being grabed. The certificate is appealed offline.

4.2. The Remote Attestation Model based on the Verifier

Remote attestation [13] refers to an attester (usually is a terminal embedded a trusted computing chip) gives the report of its platform configuration to a verifier to request for trust evaluation. The TCM embedded in SGIT measures the integrity of the platform configuration

when SGIT starts and saves the integrity value into PCR (Platform Configuration Register), then signs the value with the private key of AIK and sends it to the verifier. After receiving the integrity value, the verifier verifies the signature and compares the value received with stored before. If both values equal, the terminal is supposed to be trusted.

The remote attestation method in TCG standard has some disadvantages [14]:

①The integrity measurement method is not flexible. If the running environment is changed, for example, software upgrades, the verifier can't be validate correctly.

②The security is restricted to the private CA. If the private CA intrigues with the attester, the verifier will be cheated. As shown in Figure 3.

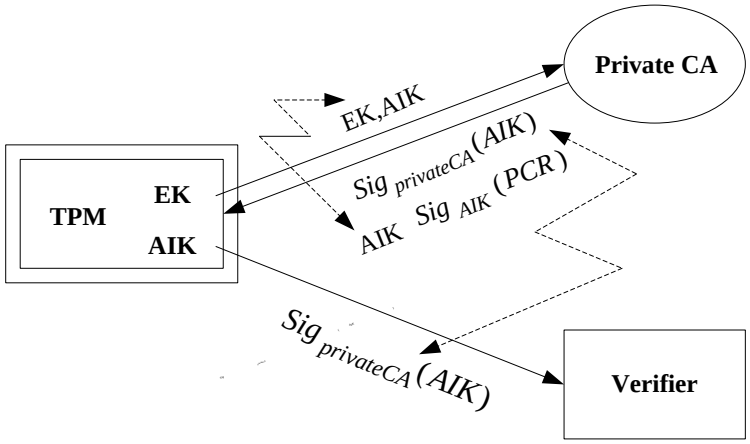

Figure 3. The Traditional Remote Attestation Model

In view of the traditional model is short of privacy and flexible, this paper proposes a remote attestation model based on verifier applied to SGIT trusted access. Although the private CA 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. The model is composed of SGIT(the attester), TAS(the verifier) and the private CA. As shown in Figure 4.

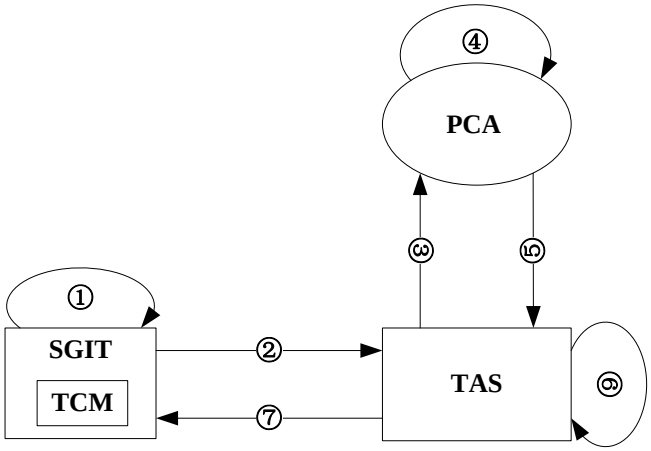

Figure 4. The Remote Attestation Model based on Verifier

The signs related are defined below.

M denotes message, Q_X denotes the public key of the entity X, D_X denotes the private key of X, 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 TAS.

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

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

$C = \text{CertVerify}\{\text{Cert}_X, \text{Cert}_{rootP}\}$ means verifying X's certificate with the root certificate of the private CA, and the result is C. $C \in \{0,1\}$.

The process of remote attestation is as following.

①The TCM embedded in SGIT measures the integrity of the platform configuration and saves the integrity value into PCR, then signs the value and the random R_T with the private key of AIK. $S' = \text{Signature}\{PCR, R_T\}_{D_{AIK}}$

②SGIT encrypts PCR and R_T with the public key of TAS and sends it to TAS with its certificate Cert_{AIK} and S'.

③TAS stores PCR, Cert_{AIK} and S', 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.

⑥TAS verifies the AIK certificate with the root certificate of the private CA, $C = \text{CertVerify}\{\text{Cert}_{AIK}, \text{Cert}_{rootP}\}$, and verifies the signature S' with the public key of AIK, $V = \text{Verify}\{PCR, R_T, S'\}_{Q_{AIK}}$, and then compares PCR with the value stored in its own database. If all verification is passed, then the integrity verification is successful. Otherwise, the communication is terminated.

⑦TAS returns F to SGIT. SGIT determines what to do next according to the value of F.

4.3. Trusted Authentication Protocol

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.

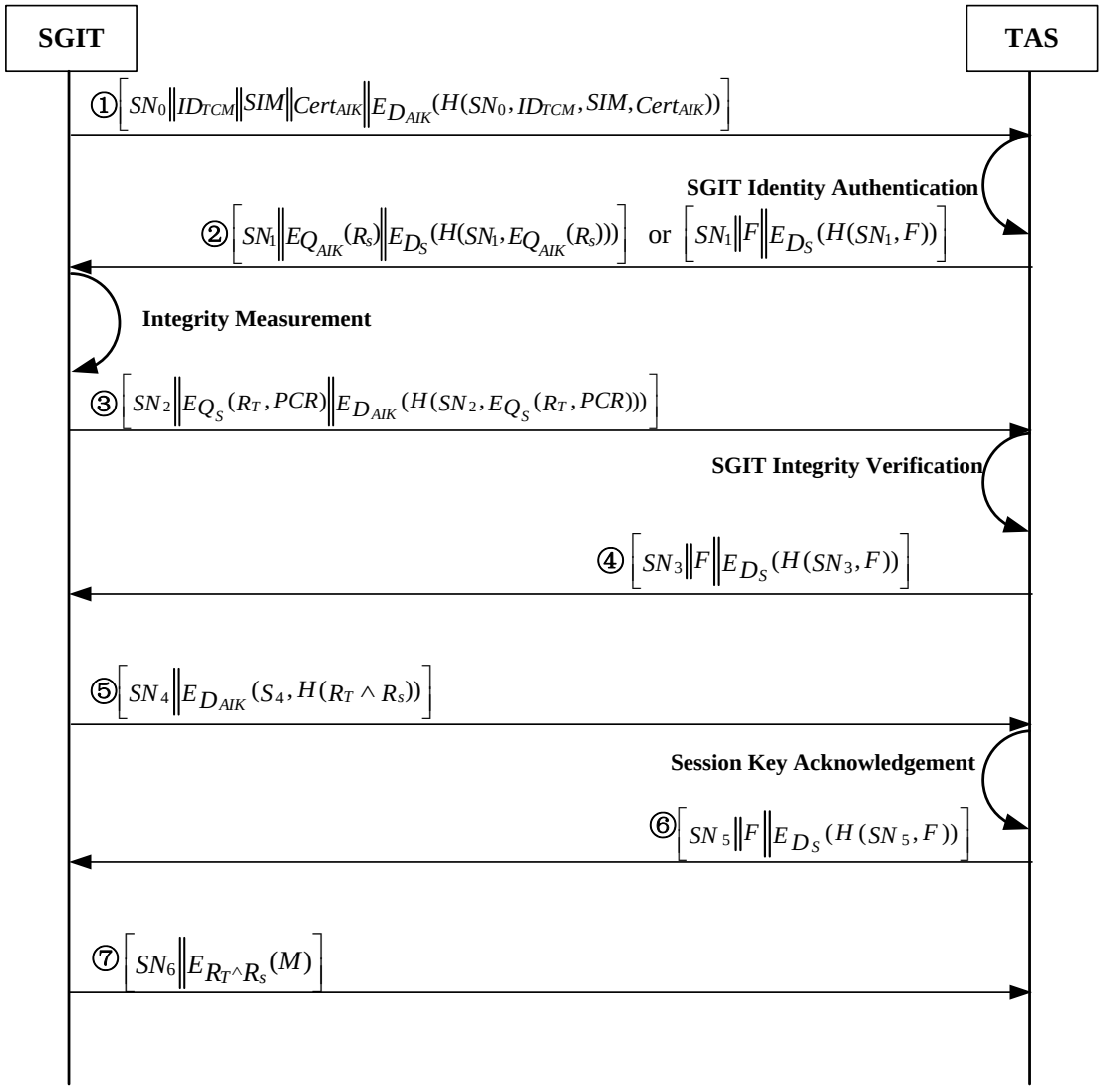

Figure 5. The Trusted Authentication Protocol

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

SGIT binds the SIM card number, the ID of TCM 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: $\left[SN_1 \| E_{Q_{AIK}}(R_S) \| E_{D_S}(H(SN_1, E_{Q_{AIK}}(R_S)))\right]$

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: $\left[SN_2 \| E_{Q_S}(R_T, PCR) \| E_{D_{AIK}}(H(SN_2, E_{Q_S}(R_T, PCR)))\right]$

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

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

TAS gets PCR and R_T, measures the integrity of SGIT according to the steps in 4.2. 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 Access Mechanism

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 TCM 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 TCM 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, TCM 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_TCM of TCM terminals and the SIM card number used in terminals. By binding both, SIM cards can be prevented from abusing and 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. Model Analysis

Access mechanism 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. Conclusion

For the security access issues of a large number of interactive terminals, this article which combines with the actual application environment of the interactive terminal proposes a trusted access mechanism for interactive terminal. The mechanism which is based on the analysis of interactive terminals' security threats and security needs uses remote attestation method which is based on the authenticator to ensure the legitimate identity of the communicating parties and the accurate verification of terminal platform integrity, which guarantees 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.

References

[1] T. Dierks and E. Rescorla, "The Transport Layer Security(TLS) Protocol Version 1.1", Network Working Group RFC 4346, Internet Engineering Task Force, http://www.ietf.org/rfc/rfc4346.txt, **(2006)**.
[2] S. Kent and K. Seo, "Security Architecture for the Internet Protocol", Network Working Group RFC 4346, Obsoletes: RFC 2401, Internet Engineering Task Force, http://www.ietf.org/rfc/rfc4301.txt, **(2005)**.
[3] Trusted Computing Group. TCG specification architecture overview (version 1.2), https://www.Trustedcomputingroup.org/, **(2007)**.
[4] TMP, Trusted mobile platform hardware architecture description, http://www.trustedmobile.org/.

[5] Z. Yu, H. Da-Ke and H. Ming-Xing, "Trusted Computing Based User Authentication for Mobile Equipment", Chinese Journal of Computers, vol. 29, no. 8, **(2006)**.
[6] L. Jian, H. Yong-zhong, S. Chang-xiang, Z. Da-wei and Z. Rui, "Access model spanning identifier domain based on trusted mobile platform", Application Research of Computers, vol. 26, 1**(2009)**.
[7] W. Zhen-qiang, Z. Yan-wei and Q. Zi-rui, "Access mechanism of TMP under mobile network", Journal on Communications, vol. 31, no. 10, **(2010)**.
[8] F. Deng-Guo and Q. Yu, "Research on Attestation Method for Trust Computing Environment", Chinese Journal Of Computers, vol. 31, no. 9, **(2008)**.
[9] W. Jun, D. Bin and H. Sheng-long, "Design of Remote Communication in Substation Automation Based On Trusted Computing Method", Automation of Electric Power Systems, vol. 29, n. 24, **(2005)**.
[10] T. Xiaoyang, "Proactive Defense Strategies for Wide-area Protection and Substation Communication Based on Trusted Computing", Automation of Electric Power Systems, vol. 35, no. 20, **(2011)**.
[11] 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, Alexandria, Virginia, USA, **(2007)** November 2.
[12] X. Zhen, L. Ren, Y. Aimin and W. Dan, "Mobile Application Security Technology for Smart Grid", Automation of Electric Power Systems, vol. 36, no. 16, **(2012)**.
[13] Trusted Computing Group, TPM Main Part 1, Design Principles, Specification Version 1.2, Revision 62, **(2003)** October 2.
[14] X. Li and Z. Yue-fei, "Study on trusted mobile computing and its attestation scheme", Computer Engineering and Design, vol. 29, no. 5, **(2008)**.

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.