Research on the communication mechanism between entities based on end-to-end credible state assessment

Baohua Zhao$^{1,2,3}$, Zhihao Wang$^{1,2}$, Ningyu An$^{1,2}$ and Chunhui Ren$^{1,2*}$

$^1$Global Energy Interconnection Research Institute Co.Ltd, Beijing, 102209, China
$^2$Artificial Intelligence on Electric Power System State Grid Corporation Joint Laboratory (GEIRI), Beijing, 102209, China
$^3$Beijing University of Technology, Beijing, 100124, China
$^*$Corresponding author’s e-mail: renchunhui@geiri.sgcc.com.cn

Abstract. In the information age, with the development of internet technology, there are more and more various business services, at the same time, network security issues are also increasing. However, traditional protection methods are gradually hard to cope with the complex network environment. Aiming at the credible connection establishment and data communication problems that need to be solved urgently in the credible network, an inter-entity communication mechanism based on end-to-end credibility assessment is proposed. This mechanism combines trusted computing with network access control mechanisms, integrates network access authority control technology, server identity authentication technology, communication subject measurement technology and network link transparent encryption technology, adopts real-time monitoring of terminal status, dynamic adjustment of access authorities, optimized network access control mechanism and data transmission method, against security issues of the network communication. After security analysis, this mechanism improves the security of the connection and communication between the terminal and the network. It can effectively avoid security threats to information systems, and make the service of the information system safe and reliable.

1. Introduction
With the popularization of internet technology, people’s dependence on communication networks has increased day by day, but various security risks such as information leakage and virus spread are also threatening the entire network communication system at all times. The safety of the network communication is very significant to the information system. The access of dangerous devices is often a potential hazard in the outbreak of the entire network crisis[1]. However, traditional defense methods continue to show limitations and disadvantages, making it more hard to cope with the complex network security status. Generally, most of them adopt security technologies such as setting up intrusion detection systems and firewalls, and scanning ports. Although this protects network security to a certain extent, it ignores the security issues caused by malicious terminals in the internal network.

The application of trusted computing technology provides ways for solving existing problems[2]. However, only protecting the terminal security cannot guarantee the completeness of the entire system, and a secure network environment is also required.

Therefore, the article is based on the trusted connection structure of the trusted computing. It conducts a lot of research on the attack methods of the information system, and integrates network
access authority control technology, server identity authentication technology, communication subject measurement technology, and network link transparent encryption technology, then proposes an inter-entity communication mechanism based on end-to-end credible state assessment. It uses trusted computing ideas to improve the safety of the data interchange between the terminal and the network, through real-time monitoring of terminal status, dynamic adjustment of access authorities, improved network access control mechanism and data transmission method. Furthermore, it effectively protects the information system from being threatened and protects sensitive information to be stolen, and makes the information system communication services security and credibility. So, there has important theoretical significance and practical value to do this research.

2. Related work
With the improvement of information technology, there are many various services, and often have data interchange between enterprise systems and external servers. However, hackers are attacking in an endless stream, and it is difficult to effectively control the behaviors of users, making network communications unable to be secure and reliable.

In[3], authors proposed a scheme to use port scanning and SNMP trap technology to detect illegal devices in the network, which improved the overall protection capability of the information system to a certain extent; in[4], it used proxy methods to help SDN controllers identify malicious access points through passive and active monitoring measures in the SDN campus network environment.

It can be seen that constantly scanning and monitoring the network communication connection environment, this security protection mode lacks consideration of the attack situation of legitimate users and equipment.

The current mainstream network connection security technologies mainly include TNC[5] (Trusted Network Connection Technology), NAC[6] (Network Access Control Technology), and NAP[7] (Network Access Protection Technology). Among them, the most popular application is TNC.

In[8], it conducted a detailed study on the related content of trusted network connection, and analyzed its advantages and limitations as a whole; in[9], it studied the technical that needed to realize the trusted network connection, and gave the scenarios suitable for the trusted connection architecture.

To advance the design of trusted connection architecture, in[10], it used the CK model to analyze and optimize the integrity evaluation layer protocol of the architecture, and proposed a trusted access protocol model TNC-PS, which can effectively prevent platform replacement attacks; in both[11] and[12], they optimized the network security protocol and access control protocol centered on EAP-TNC data packets to enhance the security and controllability of trusted network connections.

However, there are still many problems when facing attacks on the network. In[13], in order to prevent counterfeit IMC measurement data attacks, an enhanced integrity measurement collector containing device ID is used to ensure the authenticity of terminal measurement information and secure connections to trusted networks; in[14], it used dynamic root of trust technology to prevent privacy information leakage and proxy deception and set up third parties that provide access policies to improve the trusted connection between terminal devices and the network control center; in[15], it added the binding between the trusted connection architecture network access layer and the integrity assessment layer, and then against man-in-the-middle attacks. In this way, it valid defense the data communication between terminals.

In[16], it proposed a data transmission method suitable for trusted connections, by deploying a trusted transmission system with the same structure on each network node, and combining with a trusted transmission protocol. And then it makes the data transmission between network nodes be dependable.

In summary, the current network communication protection needs to be improved in the following aspects:
- It is impossible to effectively detect the vulnerabilities in the business system.
- Unable to effectively supervise the illegal operations of the internal personnel of the system.
• It is difficult to completely prevent the unintentional or intentional implantation of viruses from external or internal personnel from spreading in the information system server.

• There are few secure communication methods that dynamically evaluate the credibility of nodes in combination with network status and interactive behavior, which cannot meet people's fine-grained requirements for communication quality guarantee.

As a result, this article has combined trusted computing technology, and proposed an inter-entity communication mechanism based on end-to-end credible state assessment. It improves the safety of the data interchange between the terminal and the network, and effectively prevents the proliferation of information system security threats and the theft of sensitive information.

3. Proposed method
This method is mainly optimized and designed from three aspects: state assessment, communication mechanism and access control.

3.1. Trusted state assessment
The architecture mainly includes five entities, and each entity communicates with each other through various interface protocols. Figure 1 shows the trusted state assessment architecture.

As shown, the access requester submits an access request, and assists in completing the integrity check by collecting the trusted information of the terminal, then builds a connection; the strategic decision point judges the access application based on local security measures; the policy enforcement point responds access request based on the result of the judgment; the metadata access point server is used to collect the operating status and policy information of the network terminal; the metadata access point client is used to feedback the access devices’ status to the server in real time. Moreover, the returned messages of the server can be used to formulate system policies, and then dynamically control and change the access behavior.

This method sets up a management center and an integrity measurement collector in the internal network. The management center is composed of a WEB management platform, a strategy and audit database, and a communication agent. Users can install the management center through a one-click installation package. After installation, they can log into the WEB management center directly through a browser for system management, security policy configuration, and audit review; the integrity measurement collector collects the security status of each node in the internal network, authenticates it through the verifier, so the internal network completes the information measurement of the access terminal. By sorting out untrusted terminals, makes the network access safe and reliable. The trusted level controller analyzes and evaluates the operation of the terminal, combines the trusted status of the
terminal to dynamically redistribute terminal access permissions. It not only makes the terminal access be controlled efficiently, but also enhances the safety of trusted network connection and data communication.

3.2. Secure communication mechanism
Set up the corresponding security protection mechanism in the communication process.

This process is performed on the measurement and assessment layer. When the server receives an access request, it triggers the metric collector to collect the authentication and status messages of the network and the terminal respectively, and verified by the metric verifier. Then verifier gives the encapsulated result to the server, and the encrypted node information to the terminal. Through this two-way measurement authentication, the terminal can obtain the status messages of the nodes within the network, and the network can also clarify the condition of the terminal to be accessed, so that the terminal access and network communication are always in a safe and reliable environment.

According to actual necessity, the establishment of communication and transmission needs to obey and execute the established access control mechanism, so as to pledge the safety of communication connection and servers’ data interchanges. This process is happened in the network access layer.

3.3. Access control mechanism
This method designs the communication connection and data access and transmission. Figure 2 shows the access control architecture.

3.3.1. Server secure connection authentication.
Each host in the enterprise information system has a unique identity. When initiating communication between hosts in the internal network, this method adopts two-way authentication technology to provide digital certificate certification to the opposite end. It can effectively prevent the host from illegal access by internal members from establishing contact with the internal system, which leads to the destruction of the information system by illegal attacks. The specific authentication process is described as follows:

1) The process M of pA prepares to access the process N of pB. First, pA sends its platform certificate and private key encryption string to pB.
2) pB receives pA's platform certificate and private key encrypted string, then RootCert starts to verify the pA certificate. If wrong, give the failure instruction to pA; if right, go to step 3.
3) Use the certificate of pA to decrypt the ciphertext. If it is not successfully decrypted, send a decryption failure instruction to pA; if it is successfully decrypted, send an identity
authentication success instruction to pA, and send the platform certificate and private key encryption string to pA.
4) pA gets the authentication instruction, then checks the result. If unsuccessful, refuse the connection; if it succeeds, it executes step 5.
5) Receive the pB’s platform certificate and the private key encrypted string, RootCert starts to verify the pB certificate. If unsuccessful, refuse the connection; if it succeeds, it executes step 6.
6) Use pB’s certification to decrypt the ciphertext. If it is unsuccessful, the conversation is refused; otherwise, it has been completed the authentication process and can start to build the communication session.

3.3.2. Process identification metric. According to the network access requirements of the business host within the information system, when the host initiates a communication connection request, it also triggers the process collection mechanism to continuously collect the source communication process and the target communication process. Then begin to infer the credibility of the communication based on the content of the communication. It stops the proliferate of the virus in time and avoids irreversible data loss or programs malfunction.

The process measurement is used to keep the learning process and the process when the trusted connection is actually implemented consistently. This prevents the occurrence of behaviors such as replacement of programs with the same name and port pretense by untrusted processes. The Hash algorithm of the process adopts the SHA1+password method. When using SHA1 to calculate the file content Hash process, add your own password to get your own unique algorithm result value. The specific process measurement process is described as follows:
1) pA calculates the HASH value of the process and sends slp/sProc/sHash/dProt.
2) pB receives slp/sProc/sHash, and reads the local process measurement strategy to match the information. If it fails, it gives a measurement failure order to pA; if the match succeeds, then execute step 3.
3) Continue to perform Hash verification, reverse the process according to dPort, calculate dHash, and send dip/dHash to pA.
4) pA receives the measurement result of the opposite end and judges whether it is successful. If it fails, the measurement fails; if it succeeds, go to step 5.
5) Receive dip/dHash and read the local process measurement strategy to match the information. If the match fails, the measurement fails; otherwise, go to step 6.
6) Perform Hash verification. If it is successful, the measurement is successful, and vice versa.

3.3.3. Communication transmission encryption. When end-to-end communication occurs between business hosts within the system, the transmitted network messages will be transparently encrypted and decrypted. The method adopts OPENSSL to make communication messages be encrypted, and uses a certificate to establish a trusted encrypted channel after verification, handshake, and session key negotiation. For each original connection, a unique encrypted channel is created, and the encrypted channel guarantees its uniqueness. The session key is determined by OPENSSL's own negotiation mechanism, and the session key of each encrypted channel is unique, and the user's existing network topology and system application will not be influenced.

The particular process is described as follows:
1) The TCP client sends the Clienth*llo command to initiate a handshake and establish a TCP connection.
2) The TCP server gets the handshake order, and gives the Serverh*llo command, as well as the certificate containing the server’s authentication messages and public key to the client.
3) The client gets the instruction and certificate, makes a secret instruction that encrypted by server's public key, and gives it back to the server.
4) The server uses the private key to decrypt, the negotiation of the session key is completed, and the communication starts.
4. Conclusions
Under the conditions of today's information age, facing the increasingly complex network ecological environment, network communication security issues have become more noticeable and more urgent. However, for traditional network security management solutions, there are still many deficiencies in management security and application security. To this end, in response to the credible connection establishment and data transmission issues that to be resolved in the trusted network, this paper proposes an inter-entity communication mechanism based on end-to-end credibility assessment, which combines trusted computing with network access control mechanisms. It not only optimizes the security protocol and access control of network communication, but also enhances the security protection capability of network connections, and meets people's fine-grained requirements for data transmission and communication security.

Acknowledgments
This work is supported by the science and technology project of State Grid Corporation of China: “End-to-End Security threat analysis and accurate protection technology of Ubiquitous power Internet of things” (Grand No.5700-201958466A-0-0-00).

References
[1] Lin Y.T. (2014) Design and implementation of terminal security access system in private network. Chengdu: University of Electronic Science and Technology.
[2] Shen C.X., Zhang H.G., Wang H.M., Wang J., Zhao B., Yan F., Yu F.J., Zhang L.Q., Xu M.D. (2010) Research and development of trusted computing. Scientia Sinica: Informationis, 40:139-166.
[3] Feng J.L., Li H.Q. (2018) Research on terminal access monitoring technology based on fingerprint recognition. Information System Engineering, 101.
[4] Cox J.H., Clark R., Owen H. (2017) Leveraging SDN and WebRTC for rogue access point security. IEEE Transactions on Network and Service Management, 14:756-770.
[5] Trusted Computing Group. (2009-05-01)[2017-03-26] TCG trusted network connect TNC architecture for interoperability. https://www.trustedcomputinggroup.org.
[6] (2007) Network admission control introduction. http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html.
[7] (2008) Introduction to network access protection. http://technet.microsoft.com/en-us/network/cc984252.aspx.
[8] Zhang H.G., Chen L., Zhang L.Q. (2010) Research on trusted network connection. Chinese Journal of Computers, 33:706-717.
[9] Zhou W.Y. (2019) Thought and technology exploration of trusted network connection. Communication design and application, 26:70-71.
[10] Ma Z., Ma J.F., Li X.H., Jiang Q. (2011) Provable security model for trusted network connect protocol. Chinese Journal of Computers, 34:1669-1678.
[11] Wang M.S. (2016) Design of trusted network connection security protocol and access control architecture. Radio Communications Technology, 42:14-17.
[12] Gu H.M. (2017) Research on security management and architecture design of trusted network connection. Journal of Shangqiu Vocational and Technical College, 16:95-97.
[13] Song S.Y. (2017) TNC improvement based on bidirectional authentication and enhanced IMC. Communications Technology, 50:1776-1783.
[14] Wu Q.X. (2015) Research on improvement of trusted network access technology. Video Engineering, 39:45-50.
[15] Zhao B., Xiang C., Zhang H.G. (2019) A trusted network connect protocol for resisting Man-in-the-Middle attack. Chinese Journal of Computers, 42:1137-1148.
[16] Hu J., Zhang S.G., Bai X., Lin L. (2017) A data transmission method suitable for trusted connection. China, ZL201410149430.X.