

A Model of Trusted Connection Architecture

Xun Zhang¹, Zhihao Wang², Yong Zhi¹ and Hui Yuan¹

¹Electric Power Research Institute, State Grid Gansu Electric Power Corporation, Lanzhou 730050, China

²Global Energy Interconnection Research Institute, Beijing 102209, China

Abstract. According to that traditional trusted network connection architecture (TNC) has limitations on dynamic network environment and the user behavior support, we develop TCA to propose a trusted connection architecture supporting behavior measurement (TCA-SBM), besides, the structure diagram of network architecture is given. Through introducing user behavior measure elements, TCA-SBM can conduct measurement on the whole network in time dimension periodically, and refine the measurement on network behavior in measure dimension to conduct fine-grained dynamic trusted measurement. As a result, TCA-SBM enhances the TCA's ability to adapt to the dynamic change of network and makes up the deficiency of trusted computing framework in the network connection.

Keywords. Behavior measurement, trusted network connection, fine-grained, adaptability

1 Introduction

At present, the trusted network connection architecture mainly focuses on the problem of network access, which is essentially a kind of network access control (NAC). NAC is a kind of computer network security method, which combines the technology of terminal security technology, user or system authentication and network security technology. Traditional network access control methods include: MAC address filtering, VLAN isolation, IEEE802.1Q authentication, access control list based on IP address and firewall control, host state inspection, isolation and recovery, etc. At present, the main network architectures include TCG trusted network connection (TNC), Cisco network admission control (NAC), Microsoft network access protection (NAP), and in our country the main network architecture is the trusted network connection architecture (TCA) with three entities and three levels [1-4].

TNC, NAC, NAP network connection all adopt the access control mechanism based on integrity measurement, on the time dimension, this access control focuses on the network connection establishment stage. With the increasing complexity of network applications, simply verifying the platform integrity in connection stage can't meet the requirements of credibility of the network system. The main limitations are as follows: lack of continuity integrity measurement mechanism; Lack of fine-grained trust metrics. Traditional trusted network connection control model has limitations, which result in that the trusted network connection mechanism can't ensure the credibility of the whole process in network connection, and can't adjust the trusted measurement to the dynamic change of network environment and the change of the user behavior, therefore, the application of trusted computing framework in real network system is restricted [5-15].

According to traditional trusted network connection architecture (TNC) has limitations on dynamic network environment and the user behavior support, this paper developed TCA to propose a trusted connection architecture supporting behavior measurement (TCA-SBM). Through introducing user behavior measure elements, TCA-SBM can conduct measurement on the whole network in time dimension periodically, and refine the measurement on network behavior in measure dimension to conduct fine-grained dynamic trusted measurement. As a result, TCA-SBM enhances

the TCA's ability to adapt to the dynamic change of network and makes up the deficiency of trusted computing framework in the network connection [16-35].

2 The design of TCA-SBM network connection architecture

2.1 The Structure diagram of TCA-SBM

Here we give the structure diagram of TCA-SBM: Figure 1.

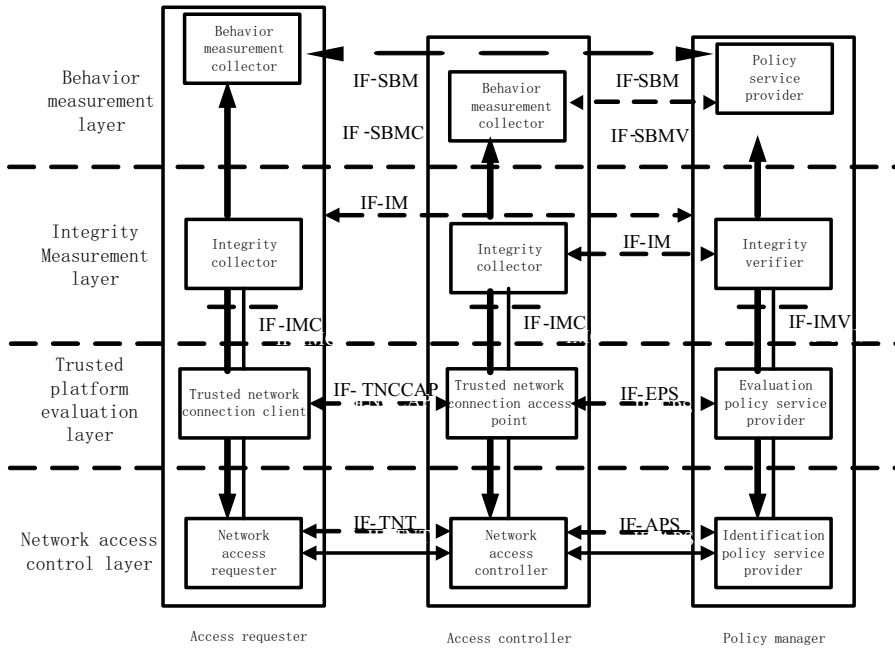


Fig.1.The architecture of TCA-SBM

2.2 The entity structure

2.2.1 Access requester

The main functions of access requester include: send request of accessing trusted network, and identify the user's identity with access controller; collect the platform integrity metric values of access requester and report to the access controller, complete the evaluation and report of trusted platform integrity between requester and controller; adopt the behavior report or behavior statement of requesters, and sent them to policy manager.

2.2.2 The access controller

The access controller is an entity that controls the requesters' access to a trusted network, whose functions mainly include: complete the user identity authentication, trusted platform evaluation and network behavior measurement between the access requesters; receive the integrity metric values of requesters and collect its own integrity metric values, and send the values to policy manager; adopt the behavior report or behavior statement of requesters, and sent them to policy manager; perform access control in case of the result generated during the processes such as user identity authentication, trusted platform evaluation and trusted behavior measurement.

This entity includes the following parts: network access controller, trusted network connection access point, integrity collector and Behavior measurement collector.

2.2.3 Policy manager

According to the different security requirements of trusted network environment, policy manager formulates the integrated security policy including user identity authentication, trusted platform evaluation and trusted behavior measurement, verify the validity of PIK certificates and platform integrity metric values from requesters and controllers, verify the results of trusted measurement for requesters' behavior, generate the results of user identity authentication, trusted platform evaluation and trusted behavior measurement performed by requesters and controllers; push network behavior statement, and verify the credibility of it.

This entity includes the following parts: evaluation policy service provider, identification policy service provider, integrity verifier and behavior policy service provider.

2.3 The architectural layers

2.3.1 Network access control layer

Network access control layer is the layer to realize the control in trusted network access, where network access requester, network access controller and identification policy service provider perform the protocol for verifying user identity, and realize the identification of user identity of requesters and controllers. As the trusted party in the protocol for verifying user identity, the service provider should verify whether the service provider can perform the verification for user identity, besides, it can perform the corresponding trusted network access control according to whether the results of user identity authentication, trusted platform evaluation and behavioral trusted measurement meet the integrated security policy.

2.3.2 Trusted platform evaluation layer

Trusted platform evaluation layer is the layer to perform the platform state evaluation, where trusted network connection client, trusted network connection access point and evaluation policy service provider perform trusted platform evaluation protocol, and realize the trusted platform evaluation for requesters and controllers. As the trusted party in the protocol for trusted platform evaluation, the evaluation policy service provider should verify the validity of PIK certificate of requesters and controllers, complete the platform integrity check of requesters and controllers by calling the integrity verifier from integrity measurement layer. The trusted network connection client and point generate the connection decision based on the corresponding trusted platform evaluation result, and send it to the requesters and controllers respectively.

2.3.3 Integrity measurement layer

Integrity measurement layer is the layer to perform the platform integrity measurement, where the platform integrity of requesters and controllers will be collected and verified. The integrity collector is to collect the integrity information in each component of platform, and the information include hardware factory information, software and hardware configuration, operating system certificate, browser certificate, third party application software certificate and so on, which the Integrity verifier should verify uniformly.

2.3.4 Behavior measurement layer

Behavior measurement layer is the layer to perform the behavior measurement for network visitor, collect the metric element information of behaviors, which try to access platform, such as create, delete, call, execution, access, upload or download and so on, determine whether the network visitor meet the network security policy according to the measurement results, besides, perform the corresponding access control for network visitor through network access control layer. Behavior measurement layer is the dynamic measure part during the trusted network connection, when having met the identity and integrity measurement policy and connected in trusted network, realizes the behavioral trusted measurement for network visitor during network connection, in addition, the metric elements and time accuracy of behavioral measurement can be self-configured according to behavior metric policy.

2.4 Functional components

2.4.1 Network access requester

Initiate an access request to access controller, perform user identity authentication protocol in company with network access controller and identification policy service provider, and realize the user identity authentication performed by requesters and controllers when they are in the network access control layer;

Forward the upper layer protocol data to the access controller and policy manager;

In case of the result of user identification the connection decision made by the identification policy service provider and the trusted network connection client respectively, control its own port, and realize the connection control of the access controller.

2.4.2 Network access controller

Activate user identity authentication protocol on the network access control layer, perform the user identity authentication protocol with requesters and service providers while realizing the two-way user authentication between them.

Forward the protocol data of the trusted platform evaluation layer and the behavior measurement layer to the access request and policy manager.

In case of the result of user identification, the result of platform state measurement and the result of behavior measurement, control its own port, and realize the access control of the access requester.

2.4.3 Identification policy service provider

Perform user identity authentication protocol in company with network access requester and network access controller, and as the trusted party in this protocol, realize the two-way user authentication between requesters and controllers.

2.4.4 Trusted network connection client

Request and receive the integrity values of measurement to the integrity collector through the interface IF-IMC, perform the trusted platform evaluation protocol with trusted network connection access point and evaluation policy service provider, let requesters and controllers realize the trusted platform evaluation.

In case of the trusted platform evaluation results generated by the service provider, make the connection decision and send it to the network access requester.

2.4.5 Trusted network connection access point

Activate user identity authentication protocol on the trusted platform evaluation layer, request and receive the integrity values of measurement to the integrity collector through the interface IF-IMC, perform the trusted platform evaluation

protocol with trusted network connection client and evaluation policy service provider, realize the two-way trusted platform evaluation between requesters and controllers.

In case of the trusted platform evaluation results generated by the service provider, make the connection decision and send it to the network access requester.

2.4.6 Evaluation policy service provider

Perform the trusted platform evaluation protocol with trusted network connection access point and trusted network connection client, and as the trusted party in this protocol, realize the trusted platform evaluation between requesters and controllers.

The evaluation policy service provider verifies the validity of the PIK certificate of the access request and the access controller, when after confirming the validity of the PIK certificate, send to the integrity verifier e platform integrity metric values of requesters and controllers through the interface IF-IMV, and then receive the verified result returned by the verifier, finally generate a trusted platform evaluation result to send to the requesters and the controllers.

2.4.7 Integrity collector

Collect the platform integrity information of access requesters and access controllers with integrity services provided by trusted computing platform.

2.4.8 Integrity verifier

Check the platform integrity information of access requesters and access controllers with integrity reference values provided by platform components in integrity management.

2.4.9 Behavior measurement collector

Behavior measurement collector receives the request, report and declaration sent by requesters, and transmits them to the policy service provider. Behavior measurement collector bases on whether the metric result provided by the policy service provider meets the behavior security policy to determine whether the network connection port is connected to the network or disconnect from the network, which is depended on the network access controller.

2.4.10 Behavior policy service provider

The behavior policy service provider and behavior measurement collector carry out the behavior measurement protocol, and as the trusted party in this protocol, measure the behavior. What's more, the service provider can synthetically determine whether the requesters' behavior meet the security policy. Finally, the service provider has integrated network behavior metric functions including individual similarity and swarm similarity evaluation, direct trust evaluation and risk assessment.

3 The design of TCA-SBM network connection process

Trusted network measurement is divided into three levels: before the trusted network connection is established they need to perform the identity measurement on network access requesters; after that they will further perform the platform status measurement; when the two metrics are meet the security policy, the access controller and the access requester establish the trusted network connection. After the establishment of network connection, they perform the behavior measurement for visitors successfully accessing network. Behavioral measure layer is a dynamic measure layer where they perform the behavior measurement for visitors successfully accessing trusted network, configure the frequency of

metric time according to behavior measurement policy, for the common safety requirements of system can adopt the snapshot, for all highly principal system can adopt the real-time behavior measurement.

The specific process and steps of the TCA-SBM network connection are as follows:

(0) Before the establishment of trusted network connection, client and access point must be respectively load their each IMC according to the platform specific binding function while evaluation policy service provider must load it its each IMV according to the platform specific binding function.

(1) The network access requester initiates an access request to the network access controller.

(2) Network access controller receives a request to access, and after that, performs user authentication protocol to realize two-way user authentication with network access requester and evaluation policy service provider, in which the service provider should not have to participate. If it participates in the user identity authentication protocol, the policy service provider acts as a trusted third party. In the protocol, the network access controller and the network access requester are also allowed to negotiate the session key.

If required to make the access decision immediately after the completion of user authentication, network access controller and network access requester generate the access decision respectively according to the user identity authentication results, and then perform the access control according to the generated access decision, otherwise go to the step (3).

(3) If network access requester requires the platform identification, network access requesters send the platform authentication request. If the network access controller requires the platform identification, network access controllers send the platform authentication request.

(4) A: Having received the platform authentication request messages, the network access controller starts the platform identification process, perform a round or multi round of platform authentication protocol to realize the authentication among platforms. If they did not receive the messages, they initiate a round of platform authentication protocol.

B: During the authentication process, client and access point interactive with their each IMC by IF-IMC respectively.

C: The evaluation policy service provider verifies the PIK certificate of the access controller and the access requester, and completes the integrity verification and evaluation by IF-IMC through calling its each IMV. The each IMV generate the component integrity evaluation results and send them to the policy service provider. Then, the providers generate the platform integrity evaluation results according to the evaluation strategy of component integrity evaluation results collected by evaluation protocol. Finally, they send the results, which include the PIK certificate validation results and platform integrity evaluation results, to the client and access point.

(5) When the access requester and access controller have completed the platform identification, they generate the access decision (allow, disallow, isolation), which is according to the PIK certificate validation results generated by the client and the access point and the platform integrity evaluation results, and then send the results to the client and the access point.

Network access requester and controller perform access controls according to the received access decision, realize the trusted network connect control, that is, they determine whether to connect this protected trusted network by the access decision and complete the measurement on identity and status in trusted network connection.

(6) After the establishment of the trusted network connection and before the behavior measurement, the trusted network connection client must bind to the specific platform to initialize the behavior measurement request.

(7) Behavior measurement collector carries out the measurement protocol by IF-SBM. Firstly, determine whether feasible network of the requester is same with access network on the attributes, if not, inform the controller to disconnect the network connection by control ports; if so, the performer and the requester negotiate a master key to negotiate key and establish a trusted pipeline to transmit confidential data.

(8) Behavior policy service provider conducts the policy evaluation for behavior metric reports, if it can meet the behavior policy, continue to keep the network connecting; otherwise, inform the network access control to

disconnect the network connection by control ports.

4 Conclusion

The scheme is mainly on the basis of TCA, integrates dynamic behavior measurement methods, ensure the credibility of the terminal identity and status through techniques of trusted computing platform and TCA integrity measurement mechanism, and ensure the credibility of the terminal behavior through the dynamic behavior measurement mechanism. This framework exploratively gathers measurement, report and declaration, verification mechanisms and so on, and combines the behavior measurement supporting the historical analysis. In theory, if the terminal does operations which do not meet the behavior security policy or malicious behavior and other events, it will be found by the behavior policy service provider, and the terminal will be isolated.

References

1. http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.
2. <http://www.microsoft.com/technet/network/nap/napoverview.aspx>
3. <http://www.microsoft.com/technet/network/nap/naparch.aspx>
4. <https://www.trustedcomputinggroup.org/groups/network/>
5. David Clark, Karen Sollins, John Wroclawski, NewArch Project: Future-Generation Internet Architecture [EB/OL]. <http://www.isi.edu/newarch/iDOCS/final.finalreport.pdf>
6. Neumann P.G., Principled assuredly trustworthy composable architectures [EB/OL].<http://www.csl.sri.com/neumann/chats4.html>
7. Rodriguez A, Egenhofer M, Determining semantic similarity among entity classes from different ontologies, IEEE Transactions on Knowledge and Data Engineering, 2003, 115, 2: 442-456
8. TCG Specification Trusted Network Connect -TNC Architecture for Interoperability Revision 1.1[EB/OL]. Trusted Computing Group, 2006.5, <http://www.trustedcomputinggroup.org>.
9. TCG Specification Trusted Network Connect IF-PEP: Protocol Binding for Radius Revision 0.7[EB/OL]. 2007.5, <https://www.trustedcomputinggroup.org>
10. TCG Specification Trusted Network Connect IF-T: Protocol Binding for Tunneled EAP Methods [EB/OL]. Revision 10, 2007.5, <https://www.trustedcomputinggroup.org>
11. TCG Specification Trusted Network Connect IF-TNCCS: TLV Binding Revision 10, 2008.1[EB/OL]. <https://www.trustedcomputinggroup.org>
12. TCG Specification Trusted Network Connect IF-IMC Revision 8 [EB/OL] .2007.2, <https://www.trustedcomputinggroup.org>
13. TCG Specification Trusted Network Connect IF-IMV Revision 8 [EB/OL] .2007.2, <https://www.trustedcomputinggroup.org>
14. TCG Specification Trusted Network Connect IF-M: TLV Binding Revision 30 [EB/OL]. 2008.1, <https://www.trustedcomputinggroup.org>
15. TCG Specification Trusted Network Connect IF-PTS Revision 1.0 [EB/OL]. 2006.11, <https://www.trustedcomputinggroup.org>
16. D.H.McKnight, N.L. Chervany, The Meanings of Trust, Technical Report MISRC Working Paper Series. University of Minnesota, Management Information Systems Research Center, 1996: 96-102

17. Kini A. and Choobineh J. Trust in Electronic Commerce: Definition and Theoretical Considerations. In 31st Annual Hawaii International Conference on System Sciences, Hawaii,1998, <http://ieeexplore.ieee.org/iel4/5217/14270/00655251.pdf>
18. Beth T, Borcherding M , Klein B, Valuation of Trust in Open Network //Proceedings of the European Symposium on Research in Security. 1994: 152-157
19. Grandison, T, Sloman, M., A survey of trust in internet applications. IEEE Communications Surveys and Tutorials, 2000, 4, 4: 2-16
20. Audun Jøsang, Roslan Ismail, Colin Boyd. A Survey of Trust and Reputation System for Online Service Provision. Decision Support System, 2007, 43, 2: 618-644
21. ITU-T Recommendation X.509, ISO/IEC 9594-8. Information Technology. Open systems interconnection. The Directory: Public-key and Attribute Certificate Frameworks. Draft ITU-T Rec. X.509, May, 2001: 22-44
22. Marsh, S. P., Formalizing Trust as a computational Concept. Doctoral Dissertation, University of Stirling, 1994: 7-33
23. Almenarez F, Matin A, Diaz D, Sanchez J. Developing a model for trust management in pervasive devices. In: Bob Werner, ed. Proc of the 3rd IEEE Int'l Workshop on Pervasive Computing and Communication Security. Washington, IEEE, 2006: 245-250
24. Jameel H, Hung LX, Kalim U, Asjjad A, Lee SY, Lee YK. A trust model for ubiquitous systems based on vectors of trust values. In Proc of the 7th IEEE Int'l Symp. on Multimedia. Washington: IEEE Computer Society Press, 2005: 674-679
25. Sun Y, Yu W, Han Z, Liu KJR. Trust modeling and evaluation in ad hoc networks. In: Proc of the Global Telecommunications Conf, Globecom 2005. Washington: IEEE Computer Society Press, 2005: 1-10
26. Li DY, Meng HJ, Shi XM. Membership clouds and membership clouds generator. Journal of Computer Research and Development, 1995, 32, 6: 15-20
27. Sailer, X Zhang, T Jaeger, L vail Doom, Design and implementation of TCG-based integrity measurement architecture. In Proceedings of USENIX Security Symposium. Lake Tahoe, California, USA: ACM Press, Aug. 2004: 223-238
28. Haldar, D Chandra, M Franz, Semantic remote attestation a virtual machine directed approach to trusted computing. In Proc of the Third virtual Machine Research a Technology Symposium. San Jose, CA, USA: USENIX, 2004: 29-41
29. Gong B, Zhang J, Xiaolie Y E, et al. A Trusted Measurement Scheme Suitable for the Clients in the Trusted Network. Wireless Communication Over Zigbee for Automotive Inclination Measurement China Communications, 2014, 11(4):143-153.
30. Ning Z H, Shen C X, Zhao Y, et al. Trusted measurement model based on multitenant behaviors. Scientific World Journal, 2013, 2014:384967-384967.
31. Li R H, Zhu Z S, Li C, et al. Trusted measurement model of runtime process behavior based on turing// Machine Learning and Cybernetics (ICMLC), 2010 International Conference on. IEEE, 2010:2183-2187.
32. Liang P, Jiang W, Gong B, et al. A New Behavior Measurement for Cloud Computing. International Journal of Advancements in Computing Technology, 2012, 4(14):9-16.
33. Qiao A, Song R, Shen L. Study of the Network Behavior Measurement. Application Research of Computers, 2005.
34. Filva D A, Guerrero M J C, Forment M A. Google analytics for time behavior measurement in Moodle// 2014 9th Iberian Conference on Information Systems and Technologies (CISTI). 2014:1-6.
35. Guo Z H, University W, University W, et al. Research on Trusted Network Connection. Chinese Journal of Computers, 2010, 33(4):706-717.