A Model of Trusted Measurement Model

Zhili Ma[1], Zhihao Wang[2], Liang Dai[1] and Xiaoqin Zhu[1]

[1]Electric Power Research Institute, State Grid Gansu Electric Power Corporation, Lanzhou 730050, China
[2]Global Energy Interconnection Research Institute, Beijing 102209, China

Abstract. A model of Trusted Measurement supporting behavior measurement based on trusted connection architecture (TCA) with three entities and three levels is proposed, and a frame to illustrate the model is given. The model synthesizes three trusted measurement dimensions including trusted identity, trusted status and trusted behavior, satisfies the essential requirements of trusted measurement, and unified the TCA with three entities and three levels.

Keywords. Trusted measurement, trusted identity, trusted status, trusted behaviour

1 Introduction

Trusted measurement is a complicated security mechanism, which involves a wide range of factors while the measurement methods are varied. Many scholars have conducted extensive research on it. In the paper [1-6], a famous formal trusted calculation model is proposed for the first time, and this model can accurately describe the trust, but because of the complexity which makes it difficult to be widely used. In the paper [5-17], the PTM model is supported by the European IST FP6, reflects that trusted derivation and trusted evolution are strict punitive, and well reflects the trust degree changes dynamically with the change of time and context. With the good computing performance and strong scalability, yet the model can't adapt to different application scenarios. In the paper [18-20], Hassan et al proposed another trusted measurement model, which is based on vector and establishes a mathematical model with some uncertainty. Because of the introduction of trust, history, time and so on, this model makes significant progress when comparing with other models. It has dynamic adaptability, has certain defenses against malicious behavior, but lacks of corresponding risk assessment mechanism. In the paper [21-24], Sun et al proposed a trust model based on entropy. On the basis of the fact that the nature of the uncertainty of trust relationship can be displayed according to the entropy in the information theory, the model can reflect the global trust degree by the trust chain transfer and update the trust dynamically. But Sun didn't give a specific mathematical model explicitly while the definition of the behavior was ambiguous. This paper presents a unified reliability model, which synthesizes three trusted measurement dimensions including trusted identity, trusted status and trusted behavior and extends the trusted measurement mechanism at present. The model bases on identity measurement and status measurement, regards the behavior measurement as the core, and carries out the comprehensive measurement for the status and identity of access requesters by the feedback of behavior.

2 The measurement model supporting behavior measurement

The measurement model supporting behavior measurement describes as Quintuple, defined as $M = (SID, IPM, BM)$

(1) ID is the result of identity measurement for access requester, the formal description is as follows, including the identity of sender and receiver.

(2) IM is the measurement of the platform configuration, the formal description is as follows:

$IPM = \{M\_BIOS, M\_OSLoader, M\_OS, M\_APP1, ..., M\_APPn, \}$, which represent the integral measurement of BIOS，OS Loader, OS Kernal and Applications

(3) BM is the result of behavior measurement for access requester, the formal description is as follows:

$BM = (SD, Data, EV)$, in which SD indicates the identity of sender and receiver, Data is the content of the behavior, EV is the environment of the behavior. The identity measurement model

In trusted network, the identity measurement focuses on the authentication of access requesters and the verification of authorization data, and the identity authentication comprises non anonymous authentication and anonymity authentication. Then non anonymous and anonymous authentication algorithm are described separately as follows.

2.1 Non anonymous authentication

2.1.1 Platform authentication

(1) The establishment of parameters: suppose (Ga, Gb) is a pair of bilinear group, $G1$ and $G2$ are both cyclic group, the given bilinear map is $e: Ga \times Ga \to Gb$, ga and gb are the generators of Ga and Gb respectively, the given hash function is $H\{0,1\}^* \to Zp^*$ without collision, then select $s \in Zp^*$ as private key of system and $Pks = ga^s$ as public key, finally the public parameter of system is $(G1, G2, ga, gb, p, Pks, H)$.

(2) The key generation: the trusted cyber requesters select $x \in RZ_P^*$ where x is the private key of requesters, then calculate $IDPK = ga^x$ which is regarded as public key of identity for requesters, send ID of requesters and $IDPK$ to the managers of trusted network policy. After that, the managers register users according to ID and $IDPK$ $IPK = ga^x$, meanwhile, issue a certificate including ID and $IDPK$ to the requesters, then managers calculate $I = IDPK^s$.

(3) Authentication: At first the trusted cyber requesters send $IDPK$ to the managers of certified trusted network policy, then the managers select $r \in RZ_P^*$ to the requesters who calculate $T = ga^{\frac{1}{x+r}}$ and sent it to managers back. Finally, the managers determine whether the requesters are legal by checking whether $e(T, Iga^r) = e(ga, ga)$ is OK.

(4) Since the legitimacy of identity of requesters has been judged, the requesters and managers will consult with a common session key K. Then, the managers encrypt K and the public key of TMP and sent them to users. The requesters encrypt users and authorization data by using K to send to server. The managers can complete the identity authentication of the requesters by verifying their authorization data. Finally the requesters and the managers can carry on the data transmission through the session key.

2.1.2 Security analysis

The security of the algorithm can be proved through that constructs an attacker A to interact with the IPK owner C, and then pretends to be C. Construct a function F which is the attacker of K-CCA hard problem, that is, this function knows the set of data as $\{h1, h2.....hk \in Z_p, g, g^x, g^{h1x}, g^{h2x}.....g^{hkx}\}$. The function F treats A as its own call subroutine, and simulates the honest *IPK* owners to produce the corresponding A.

2.2 Anonymous authentication

2.2.1 Platform authentication

(1) The establishment of parameters: suppose Ga, Gb is large prime number multiplication group of P order, g is the generator of G_a, the bilinear pairing is $e(G_a, G_a) \to G_b$, and $e(R, g^r PK) = I$, then the public parameters are $(G_a, G_b, g, P, e(R, g^r PK) = I)$.

(2) The key generation: the trusted cyber requesters select $x \in_R Z_P^*$ and compute $PK = g^x$, make PK as public key of user platform, and request certificates from the managers of certified trusted network policy, which include platform identity and public key.

(3) Authentication: At first the trusted cyber requesters send PK to the managers of certified trusted network policy, then the managers select $r_1, r_2 \in_R Z_P^*$ to the requesters who compute $R = g^{\frac{1}{r_2 + r_1 x}}$ and sent it to managers back. Finally, the managers determine whether the platform is legal by checking whether $e(R, g^r (PK)^{r_2}) = I$ is OK.

2.2.2 Security analysis

Authentication security depends on the security of platform identity authentication, so the following will analyze the security of the platform identity authentication process. The security of the algorithm can be proved through that constructs an attacker A to interact with the PK owner C, and then pretends to be C. Construct a function F which is the attacker of K-CCA hard problem, that is, this function knows the set of data as $\{h_1, h_2.....h_k \in Z_p, l_1, l_2.....l_k \in Z_p ? \neg g, g^x, g^{\frac{1}{h_1 + l_1 x}}, g^{\frac{1}{h_2 + l_2 x}}.....g^{\frac{1}{h_k + l_k x}}\}$. The function F treats A as its own call subroutine, and simulates the honest PK owners to produce the corresponding A.

Therefore in the stage of the identity authentication, firstly we should verify the legitimacy of PI, and then the trusted cyber policy manager will generate a session key K, use the PK of requesters to encrypt session key K, send the encrypted K to requesters. The requesters encrypt the user identity UI and authorization data AUD by using the session key K to managers, who will verify whether the authorization data is legal, and if so, the authentication will be passed.

3 The status measurement model

Current research on the platform status measurement including integrity measurement for TCG, based on this, this paper proposed the network connection method to measure the status of the access requesters. When an access requester successfully has passed identity measurement, he will go on the status measurement. The status measurement is conducted firstly according to security policy for trusted network management strategy, then according to the users' authorization data for real time status measurement. The status measurement process is described in detail as follows.

3.1 The status measurement for basic trusted configuration

Suppose $TPCR = \{TPCR[1], TPCR[2], ...TPCR[n]\}$ as the PCR of basic trusted configuration elements of requesters, the network service providers keep the requesters' desired configuration indicated as $PCR = \{PCR[1], PCR[2], ...PCR[n]\}$, the measure result function is defined as $MRbt$, whose description is as follows:

$$MC = \sum_{i=1}^{n} TPCR[i] \oplus PCR[i]$$

Given a MC and the threshold MC_0, if $MC > MC_0$, the measure result of requesters' basic trusted configuration conform to the security policy on trusted network server end.

3.2 The real time status measurement

The most important thing of real time measurement for network requesters is to confirm whether the network request process is malicious. Here we refer to malicious code measurement method to confirm whether the network request process is malicious. The most typical method to determine malicious code is static and the method has been widely used in all kinds of antivirus software, however, as the most serious defects, this method can't judge variant or unknown malicious code accurately.

The real time status of network requesters is the real time status of N processes of recorded access requesters, because of some shared characteristics of malicious processes such as unauthorized access of Trojan, virus self-replication and tampering with files, Worm network attacks, etc. Real time status measurement is mainly to measure the malicious process of the trusted network requesters, so the definition of the malicious degree of the network requesters' processes can confirm whether the real time status is credible. Suppose BQ indicates the malicious degree of processes, $BQ = \{bq[1], bq[2].....bq[m]\}$ indicates the malicious degree of each process, the trusted network service providers set the set of permissions.

$$MR = \sqrt{\lambda_1 bq^2[1] + ... + \lambda_m bq^2[m]}$$

Given a threshold Mt, if $MR < M_t$, the measure result of requesters' basic trusted configuration conform to the security policy on trusted network server end.

4 The behavior measurement model

The description is represented by the following quintuple $M = (SID, IPM, BM)$. This paper will introduce the relationship between identity, status and behavior, and the feedback effect of behavior on identity and state.

Suppose in the time of ΔT, if the behavior measurement of network requesters is trusted, the trusted network policy manager can improve the permission for user's access and modify the user's authorization data. The results of behavior measurement can change the user's identity and status information. Behavior feedback on identity information is mainly refers to the access permissions and authorization data information in the network access control mechanism, and the behavior is defined as feedback behavior. Besides, the behavior of requesters can be categorized as trusted and non-trusted behavior (Including threat and malicious behavior).

The behavior has a feedback effect on the identity and state of network request, such as in a given period of time ΔT, if network policy devices are trusted for the measurement on identity, status, behavior of requesters, then the trusted network policy manager can improve the permission for user's access and modify the user's authorization data. Whether it is trusted can be judged by the behavior feedback function F, which is defined as follows:

$$F(SID, IPM, BM) = True(SID, IPM, BM)$$

5 Conclusion

In view of the current state that trusted measurement mechanism lack of systematic measurement model and are based on static integrity, a multidimensional unified reliability model named UTM is proposed in this paper. And the model established unified measure relationship in trusted network through integrating trusted measure elements such as identity, status, behavior, etc. The model is a combination of static and dynamic measurement and an integration of multi-dimensional elements. With characteristics such as fine granularity, dynamic, behavioral measurement and so on, the model can provide the basis to develop a more fine-grained security policy. The model is based on the TCA with three entities and three levels, and the measurement method is easy to be integrated.

References

1. 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
2. Marsh, S. P., Formalizing Trust as a computational Concept. Doctoral Dissertion, University of Stirling, 1994: 7-33
3. 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
4. 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 M ultimedia. Washington: IEEE Computer Society Press, 2005: 674-679
5. 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
6. Li DY, Meng HJ, Shi XM. Membership clouds and membership clouds generator. Journal of Computer Research and Development, 1995, 32, 6: 15-20
7. Sailer, X Zhang, T Jaeger, L vail Doom, Design and implementation of TCG-based integrity measureme architecture. In Proceedings of USENIX Security Symposium. Lake Tahoe, California, USA: ACM Press, Aug. 2004: 223-238
8. 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
9. Seshadri M, Luk E, Shi A, *etal*. Pioneer: verifying integrity and guaranteeing execution of code on legacy platforms. In the Proc ACM SIGOPS Operating Systems Review, SOSP'05, Brighton: ACM Press, 2005: 1-16
10. Barka, E.; Ravi Sandhu. Role-based delegation model/hierarchical roles (RBDM1). Computer Security Applications Conference, 2004. 20th Annual Digital Object Identifier: 10.1109/CSAC.2004.31 Publication Year: 2004: 396-404
11. Gang L X, Bei G. Unified Trusted Measurement Model of Trusted Network[C]// Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference on. IEEE, 2012:1082-1084.
12. Yang L, Shi Y, Tang J. A trusted measurement scheme for wireless sensor networks[C]// Communication Software and Networks (ICCSN), 2015 IEEE International Conference on. IEEE, 2015.

13. Gong B, Zhang J, Xiaolie Y E, et al. A Trusted Measurement Scheme Suitable for the Clients in the Trusted Network[J]. Wireless Communication Over Zigbee for Automotive Inclination Measurement China Communications, 2014, 11(4):143-153.
14. Ning Z H, Shen C X, Zhao Y, et al. Trusted measurement model based on multitenant behaviors.[J]. Scientific World Journal, 2013, 2014:384967-384967.
15. Chunlei W, Dongxia W, Yiqi D. Towards a Unified Framework for Network Survivability Measurement[C]// Proceedings of the 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing - Volume 01. IEEE Computer Society, 2010:129-134.
16. Xiao Y, Cao J, Lai X, et al. Trusted network connect system based on tri-element peer authentication: US, US8191113[P]. 2012.
17. Brickell E F. Method of using signatures for measurement in a trusted computing environment: US, US8631507[P]. 2014.
18. Wang X, Liao G, Wang F, et al. Study of Rapeseed Information Website Trusted Measurement Based on Fuzzy Comprehensive Evaluation[J]. Chinese Agricultural Science Bulletin, 2015.
19. Xin S Y, Zhao Y, Liao J H, et al. Dynamic trusted measurement model of operating system kernel[J]. Journal of Computer Applications, 2012, 32(4):953-945.
20. Kanstrén T, Evesti A. Security Metrics, Secure Elements, and Operational Measurement Trust in Cloud Environments[M]// Security and Trust Management. Springer International Publishing, 2015.
21. Tang Y, Zhang Y P, Chen H Y. Trusted Component Measurement Model Based on Specific Areas[J]. Computer & Modernization, 2014.
22. Challener D C, Cromer D, Locker H, et al. Local verification of trusted display based on remote server verification: US, US8205248[P]. 2012.
23. Horman N R T, Paris E L. Network access control for trusted platforms: US, US8832811[P]. 2014.
24. Ning Z H, Shen C X, Zhao Y, et al. Trusted measurement model based on multitenant behaviors.[J]. Scientific World Journal, 2013, 2014:384967-384967.