DOI: 10.7763/IPEDR. 2012. V49. 20

An Access Authentication Model Based on Trusted Network

Shaoqing Huang and Xiubin Qian

Department of Emergency, Beijing Information Security Test and Evaluation, Beijing, China
huangsq@bjeit.gov.cn, qianxb@bjeit.gov.cn

Abstract—At present, the traditional information security focus on protection of the information systems and networks, but ignores the security check for access terminal itself, which affecting the entire network environment. In this paper, we make use of the thought of access authentication in trusted network, such as NAC, NAP and TNC, which combine with the information management and security evaluation, and present an access authentication model based on trusted terminal. This model could present legal solutions in practical network and devices to achieve the information management and security evaluation for all terminals, with resolving the dependencies on proprietary products and protocols. Finally, this article describes the practical application of access authentication in Code Division Multiple Address for POS system, which demonstrates the openness of this model.

Keywords: Access Authentication, Trusted Network ,Openness, POS System

1. Introduction

In recent years, we all focus on the security of information system and network border but ignoring the security of terminals, which make 85% of the source of network security incidents. At present, the information of authentication just be managed by network equipment and protocols on traditionally, such as 802.1x protocol and PPPoE protocol supported by switches, VPN supported by remote communication, etc[1][2][3]. However, all the information just authenticated for the user's identity, but not evaluated the security of all, which leading to the existence security risks of uncontrolled access terminal to the network, thereby intentionally or unintentionally affect the security of the entire network environment.

2. The technology of access authentication to terminal

In those years, there is new technology which named information management based on trusted network for access authentication. This technology make checks to the terminal according to the security policy and only allows terminal access policy compliance, and will secure terminals isolated from outside the network. At present, there are three types of network access authentication technologies which are representative.

NAC is a short form of Network Admission Control which proposed by the Cisco. Before the terminal which isn't in accordance with security policy enters the network, its level of security will be judged and its permissions will be controlled. Then the terminal which does not meet the security policies will be isolated. Those terminals only be allowed to access to limited resources to facilitate repair work.

NAP is a short form of Network Access Protection which is proposed by the Microsoft. It controls the system's permission of access which is not accordance with regulations according to the users. All of the terminals which enter the network will be security by the NAC.

TNC is a short form of Trusted Computing Group which is proposed by the Trusted Computing Group. TNC manage the completeness of terminal's status and the legality of terminal. TNC architecture provides network environment from a different terminal integrate data collection and exchange of a common framework, it also provides the framework for this product interfaces.

The three technologies described above make assessment and modification for the terminals with risk based on the existing traditional methods of authentication, such as 802.1 X, PPPoE and VPN. But there are also disadvantages in those technologies. The first one is that most of the proprietary technologies only belong to one company such as NAC is just applicable to Cisco's equipment, and NAP is just applicable to Microsoft's equipment with limited openness. The second is that there are few standards supported by those

technologies, such as NAC support EAP, Radius and other agreements, NAP supports DHCP, RADIUS and other agreements, TNC is supported 802.1 X, IPSec and other protocols. All of those have certain limitations in the actual application.

So, in order to solve the problem of dependence and limitations, this paper present a model of information management based on the trusted terminal for access authentication, which based on the idea of the three terminal access authentication technologies described above.

3. An access authentication model based on trusted network

The model is based on TNC access authentication methods retain three roles which are AR short form of Access Requestor, PEP short form of Policy Enforcement Point and PDP short form of Policy Decision Point. The model import PPP short form of Policy Provider Point in order to provide the implementation of different security strategies and decisions according to the different needs of end-user access to PEP and PDP. Also this model import SRP short form of Safe Recovery Point in order to solve the problem that AR does not meet the security policy can't access the network. This will allow AR re-request access network according to the security policy requirements under the PPP, shown in Figure 1.

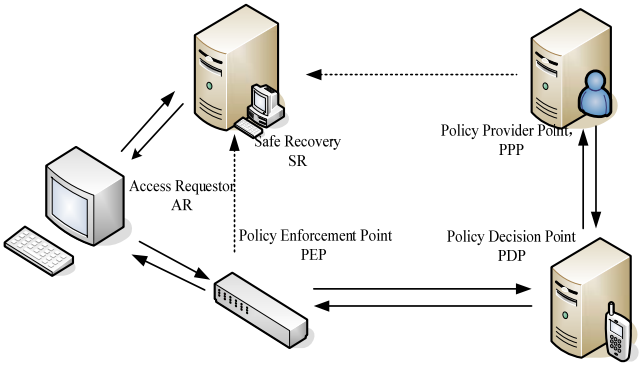

Figure 1. The model of access authentication based on trusted network

In Figure 1, the access requester AR can be personal computers, laptops, PDA, mobile phone and other terminals according to the actual situation. PEP can be network firewalls, security gateways and other network security equipments, which send the information of AR and receive the policy of PDP. PDP can be the authentication server and the device management server such as Radius, Diameter, etc., which receive the information of PPP's policy and the information of AR sent by PEP. PPP according to the actual needs of network administrators can be expressed as a trusted third party and make security strategy. Also it can provide repairing strategies to this, and issued for the PDP to develop strategies and to provide specific end-user security SRP repair strategy to the users. AR can provide the service of security repairing which failed to the PPP's certification strategy according to the PPP. It can be selected by the anti-virus server, patch server servers and other security fixes.

All the entities of the certification information management model can not be only a single physical entity, but also be the integration of multiple logical entities.

4. The architecture of access authentication based on credible terminal

The model of information management in this paper is based on trusted network terminal access authentication. From the horizontal point of view, they are Security Recovery, Access Requestor, Policy Enforcement Point, Policy Decision Point and Policy Provider Point. From the vertical point of view, they are Network Access Layer, Integrity Evaluation Layer and Integrity Measurement Layer. All of layers are abstract from the bottom up in figure 2.

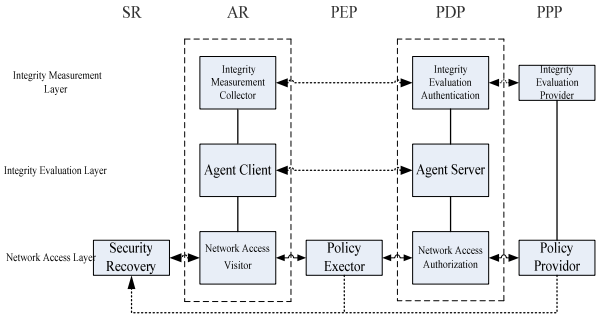

Figure 2. The architecture of access authentication based on trusted terminal

Network Access Layer mainly contains AR, PDP and PPP on the network connection requests with the appropriate entity authentication. Everyone which accesses the network access can be run in the software and hardware on the AR. Also it is responsible for consultation and establishment of one or more network connections. PDP with power of network access authorization can to decide whether allow AR visit. PPP which is the access policy for network access providers can be the base of verify authorization to determine access rights of AR.

Integrity Evaluation Layer mainly contains all the entities which collect the integrity of the assessed value in AR, PDP and PPP. AR collects the information of the attribute assessment and makes a report to the PDP proxy server which is on the performance of the proxy client. PDP receive all the property information of AR's integrity assessment from the client.

Integrity Measurement Layer mainly contains all the entities which collect the integrity of the measured value in AR, PDP and PPP.AR which is on the performance of the assessed value of collector collects and sends the integrity measurement information of hardware, firmware, operating systems and applications. PDP receives the information of integrity measurement from the collector. Also it compares the parameters of PPP to provide verification from AR. PPP provides the contrast parameters of integrity measurement.

5. The solution of POS terminal secure access CDMA network

The proposed use of the terminal based on the trusted network access authentication information management model, this section through the POS terminal for secure access CDMA network application examples. The program mainly for POS terminals to evaluate the safety status information to determine the CDMA network equipment to POS terminal network element of network access control policy implementation and application services, content constraints, and the corresponding results based on the assessment of security fixes.

This section through the POS terminal for secure access CDMA network application examples based on the trusted network access authentication information management model. The program evaluates the safety status information of POS terminals to determine the network access control policy and application services of CDMA network equipment. Then it makes repairing according to the results.

There are four entities in the figure about POS terminals access CDMA network in the following. The first one is POS terminal in the form of AR, which includes the POS terminal operating system, POS terminal business software and proxy clients. The second is gateway and firewall of bank in the form of PEP, which controls the external network access to internal business platform. The third one is security control system which can make evaluation and certification. It includes the Radius authentication server of bank for remote dial-in user authentication service, and the information of status sent by agents. The last one is platform of service provide of PPP and SR. This platform provides relevant access control policy for the terminal access, and provides security repair services to the terminals which not meet the security policy. All of above showed in figure 3.

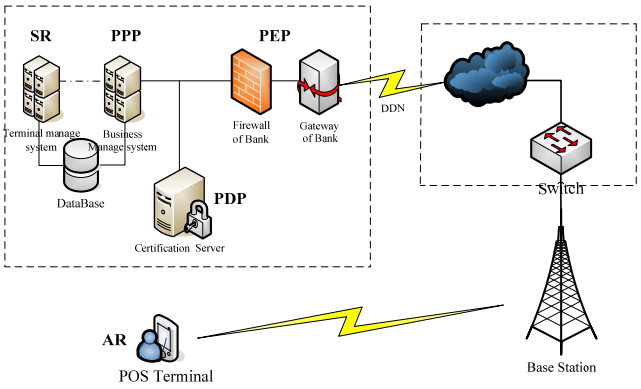

Figure 3. The solution of POS terminal secure access CDMA network

Proxy client is responsible for collecting security information related to POS terminals, and processing parameters refined control system sent to the security. Safety control system receives the information to evaluate and verify the situation to determine the safety of POS terminals and Certification. If the POS terminal is not security, the system will send all packets to the security device to filter redirects, or notice the platform the upgrade or update the POS terminal operating systems, components and related application software. After repairing then allowed the terminal re-access. If the terminal is not an authorized user, then all packets will be ignored in the firewall and gateway which just allowed the terminal with security and authorization access.

6. Conclusion

This paper presents an access authentication model based on credible terminal combining with the information management and security evaluation, which according to the thought of access authentication in trusted network, such as NAC, NAP and TNC. In this paper, we discuss the entities of model, architecture and authentications. The model breaks through the limitation of NAC, NAP, TNC and other authentication methods to the products and protocols. It can design appropriate access to trusted network security solutions according to actual network environments and equipment. Finally, this article describes the practical application of access authentication in Code Division Multiple Access for POS system, which demonstrates the openness of this model.

7. Acknowledgment

First and foremost, I would like to show my deepest gratitude to my supervisor, Mr. Xinbin Qian, a respectable, responsible and resourceful supervisor, who has provided me with valuable guidance in every stage of the writing of this thesis. Without his enlightening instruction, impressive kindness and patience, I could not have completed my thesis. His keen and vigorous academic observation enlightens me not only in this thesis but also in my future study.

Last but not least, I'd like to thank all my friends, especially my lovely colleagues, for their encouragement and support.

8. References

[1] Shiyi Xu, “The design and analysis of trusted computer system” [M]. Beijing: Tsinghua University Press, 2006.

[2] Qinggang Le, Donghui Guo, Boxi Wu, “PPPoE and its application in the brandband access system”[J]. The research in application of computer, 2003.3, PP: 130～132, 136.

[3] Hongwei Liu, Guobin Wei, “The application of trusted computing in VPN”. Computer Application, Vol.26, No.12, 2006.

[4] Yongfeng Huang, Wang Bin, Xiaodong Xu, “The application of RADIUS in 802.1x”. The engineer and design in computer. Vol.27, No.5, 2006.

[5] Cisco Network Admission Conlro1.http://www.infosec.co.uk/ Exhibitor Library /78/Cisco NAC.PDF.

[6] Trusted Computing Group. TCG Trusted Network Connect TNC Architecture for Interoperability Specification Version 1.1. 2007.10.26 http: // www.Trusted - computing group.Org.

[7] Microsoft Corporation and Trusted Computing Group. Standardizing Network Access Control: TNC and Microsoft NAP to Interoperate.2007. 10. 26 http://www.Trusted computing group. Org

[8] Li Jian, Jieqiang Liu, Zhou zheng. “Study of Policy Model of Software Secure Loading for Trusted Mobile Platform” [J]. Computer Engineering, 2009, 35(4) , PP:148-150.

[9] Shuyi Chen; Yingyou Wen; Zhao Hong. “Conceptual Design of Trusted Mobile Platform” [J], Journal of Northeastern University (Natural Science).Vol.129, No.8 2008.9.

[10] Zheng Yu, Dake He, Mingxing He. “Trusted Computing Based User Authentication for Mobile Equipment”[J]. Chinese Journal of Computers, 2006, 29(8), PP:1255–1264.

[11] Sun Yong, Chen Wei, Yixian Yang. Trust Computing of Embedded System [J]. China Information Security. 2006.9, PP: 50-52.