CSCanada
Management Science and Engineering
Vol. 8, No. 3, 2014, pp. 46-49
DOI:10.3968/5221

ISSN 1913-0341 [Print]
ISSN 1913-035X [Online]
www.cscanada.net
www.cscanada.org

A Multi-Authentication Architecture Based on DIAMETER

XIE Xiaomin[a],*; BAI Hai[b]

[a]Lecturer, Sichuan Agriculture University, Ya'an, China.
[b]Senior Engineer. Three Gorges Vocational College of Electric Power, Yichang, China.
*Corresponding author.

Received 14 June 2014; accepted 16 August 2014
Published online 15 September 2014

Abstract

Comparing two AAA protocols, the authors find that the compatibility of the DIAMETER protocol is better and more advanced than that of the RADIUS protocol. The authors design a security model based on this protocol to conduct network management. The principle of this model is to use the extended features of EAP to force users to update the OS and the virus feature library. Using this model to implement network management can reduce objective threats of end users, reduce spam traffic, increase the payload of the network, and enhance the security of the network.

Key words: Multi-authentication; DIAMETER; EAP; Network admittance

Xie, X. M., & Bai, H. (2014). A Multi-Authentication Architecture Based on DIAMETER. *Management Science and Engineering*, *8*(3), 46-49. Available from: URL: http://www.cscanada.net/index.php/mse/article/view/5221
DOI: http://dx.doi.org/10.3968/5221

INTRODUCTION

In recent years, information leaks and other incidents continue to occur. The main reason is in the process of informatization, although safety education is enhanced, some safety precautions are not implemented due to a shortage of personnel and low professional quality.

In the mobile Internet era, big data services become inevitable, and information security becomes increasingly important. Services to prevent illegal access, services of system version management, and virus defense have become important work for network management.

1. INFORMATION SECURITY STATUS

1.1 The Trend of China's Network Security

Kaspersky Security Bulletin 2012 Overall Statistical Data shows that the number of information security incidents continues to rise.

The main types of information security incidents include computer OS, application vulnerabilities, bad URLs, human negligence, infection of computer viruses, worms and Trojans, junk emails, network scanning, attacks, and web tampering.

1.2 The Market Structure of the Operating System

According to the data from a statistical report on worldwide operating system market released by Onestat, an American high-tech market research company, by August, 2013, Microsoft window operating system accounted for 90% market share and Windows 7 was the world's most popular operating system, accounting for 49% market share.

1.3 The Condition of Microsoft Operating System Patches

The number of Microsoft patches throughout 2013 reached 106. In recent 5 years, it was the third time that the number of Microsoft patches had reached 100. The overall trend shows it increases annually and patches continue to emerge and the number is increasing.

2. AAA MANAGEMENT SOLUTION

2.1 AAA Description

AAA refers to authentication, authorization, and accounting. Since the birth of the network, the system of

authentication, authorization, and accounting has become the basis of network operations. The use of a variety of resources in private networks needs to be managed through authentication, authorization, and accounting.

For an AAA system, authentication is critical. Only by confirming the identity of the client can we know to whom to send the bill for the services provided; at the same time we can prevent unauthorized clients from destroying the network. After confirming the identity of the client, according to the service type that the client applied for when opening the account, the system can authorize the client the appropriate permissions. Finally, when the client uses the resources of the system, it requires appropriate equipment to count the client's occupancy of the resources and accordingly charges the client.

In general, the authentication process is completed by three entities: the client, the authenticator, and the AAA servers (the authentication server, the authorization server, and the accounting server). The authenticator is implemented in the network access server and they use PPP protocol. The authenticator and the AAA servers use the AAA protocol.

2.2 RADIUS Description

RADIUS originally means the distance from the center to the edge of a circle. The original aim was to conduct authentication and accounting for dial-up clients. Later, after many improvements, it has formed a common authentication and accounting protocol. RADIUS is a protocol of a C/S structure and its client originally was NAS (net access server). Now any computer running the RADIUS client software can become the client of RADIUS. The RADIUS authentication protocol mechanism is very flexible, and it can use various authentication approaches such as PAP, CHAP, and Unix login authentication. RADIUS is an extensible protocol and all the work it carries out is based on the vector of Attribute-Length-Value.

RADIUS is one of the most commonly used authentication and accounting protocol. It is simple, safe, easy to manage, and scalable; therefore it is widely used. However, due to defects of the protocol itself, such as UDP-based transfer, simple packet loss mechanism, no provisions on retransmission, and centralized billing service, it is less adapted to the current development of the network, needing further improvement.

2.3 DIAMETER Description

With the introduction of new access technologies (such as wireless access, DSL, mobile IP, and Ethernet) and the rapid expansion of access to the network, more sophisticated routers and access servers have been put into use, and they have proposed new requirements to AAA protocol, making the shortcomings of traditional RADIUS's structure increasingly evident.

DIAMETER is a straight line from one side of a circle to the other side, passing through the center of the circle. DIAMETER protocol is defined based on a basic protocol and a set of application protocols. This design allows the protocol to be extended to a new access technology. After discussion, the AAA Working Group of IETF agreed to use DIAMETER protocol as the next generation of AAA protocol standards.

The basic DIAMETER protocol assumes that the communication is conducted in a peer model and it emphasizes capability negotiation, message sending, and how the peer is ultimately rejected. The basic protocol has also developed specific rules for the exchange of information between all DIAMETER nodes. The basic DIAMETER protocol is aimed at providing an AAA framework for the use of various applications.

The basic protocol is used to provide the basic mechanism for reliable transmission of information sending and error handling. The basic protocol must work together with a DIAMETER application protocol. Each application protocol relies on the basic protocol service to support specific types of network access. Application protocols include NAS protocol, EAP protocol, MIP protocol, CMS protocol, and so forth. NASREQ application protocol supports dial-up PPP/IP and can alternate RADIUS.

The basic protocol defines basic DIAMETER information format. Data in DIAMETER information works as AVPs collection to carry out. AVP (Attribute Value Pair) is an information encapsulation method related to DIAMETER information. An AVP is like a RADUUS attribute. Some AVPs are used in DIAMETER basic protocols, and others are used in DIAMETER application protocols.

3. WSUS DESCRIPTION

Windows Server Update Services, known as WSUS for short, is free software provided by Microsoft. It provides distributions of critical updates for Windows family products. When important updates suitable for your computer are released, it will timely remind you to download and install.

There are two advantages to deploy WSUS server in the LAN. The first one is that when a large number of client computers are connected to Microsoft Update through automatic update, it will have a great impact on the network bandwidth outside of the enterprise. Therefore, deploying WSUS can greatly reduce the network bandwidth outside of the enterprise occupied for the client updates. The second advantage is to manage the update programs and to control the distribution of updated programs. It can approve the installation of the updates on the client computers, or simply detect whether the client computer requires this update, or just reject this update.

4. DESCRIPTION OF THE ENTERPRISE EDITION ANTIVIRUS SOFTWARE

There are three advantages to deploy enterprise edition antivirus software in the LAN. First, it can significantly reduce the network bandwidth outside of the enterprise occupied by client updates. Second, it can get world-class support from the security response center of the enterprise edition antivirus software's producer. With the enterprise edition antivirus software, the management personnel can rely on the latest protection to prevent newly outbreak of viruses, worms, Trojans, and other harmful information. Third, centralized control and strategy management tools make management easy and effective, and it provide quick response to antivirus.

5. EAP OVERVIEW

EAP (Extensible Authentication Protocol) can extend the authentication protocol for PPP authentication, and it can support multiple authentication mechanisms. EAP doesn't specify the authentication method in the link control phase, but postpone this process to the authentication stage. In this way, the authenticating party can decide with authentication method to use after asking for more information. This mechanism allows to use a *back-end* server to actually perform the authentication mechanism, and PPP authenticator merely passes authentication interaction information. Some devices do not need to understand every type of request packets, but as an agent, directly pass the authentication packets to the backend authentication server. The devices only need to care about whether the authentication result is a success or failure and then end the authentication phase.

5.1 EAP Packet Encapsulation Format

An EAP packet is encapsulated in the information field of PPP data link layer frames where Protocol field indicates the type is hexadecimal C227 (PPP EAP). The format of EAP packets is as follows:

Table 1
Format of EAP Packet

8 bit	16 bit	32 bit	Variable bit
Code	Identifier	Length	Data

The Code field identifies the type of the EAP packet. EAP Codes are assigned as follows: (a) Request, (b) Response, (c) Success, (d) Failure.

The Identifier field is used to match the response and the request information.

The length field indicates the length of the EAP packet, including Code, Identifier, Length and Data field. The format of the Data field is determined by the Code field.

5.2 The EAP Authentication Process

The EAP authentication process mechanism is shown as Figure 1:

In the first stage, after the link establishment phase is complete, the authenticator directly sends one or more requires to the authentication node. There is a type field in the request used to indicate the information requested by the authenticator, such as the challenge word of ID and MD5, the OTP, the Generic Token Card, and so forth.

In the second stage, the endpoint responds with a response to each request. Same as the request, the response also contains a type field corresponding to the type field in the response to the request.

In the third stage, the authenticator sends a success or failure message to end the authentication process.

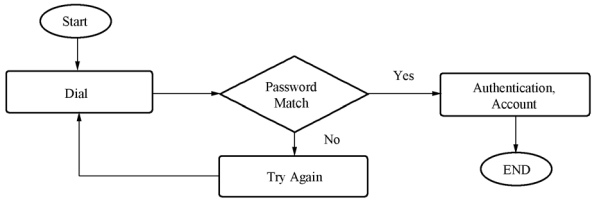

Figure 1
Authentication Process

6. THE DIAMETER-BASED EAP EXPANSION PROCESS

The expanded authentication process is shown as Figure 2:

In the first stage, the DIAMETER server authenticates whether the client's ID matches the password. The client requests for authentication. If they match, the server will send the packet code=3 to proceed to the next stage of the authentication, otherwise the packet code=4.

In the second stage, the local OS patch update server authenticates whether the client's OS version matches the latest OS version that the WSUS server requires. The client requests authentication. If they match, the packet code=3 to proceed to the next stage of the authentication, otherwise the packet code=4.

The third stage is to authenticate whether the client's antivirus software virus feather library version matches the latest virus feather library version required by the local virus database server. The client requires authentication. If they match, the packet code=3, to proceed to the next stage of the authentication, otherwise the packet code=4.

The fourth stage is to authenticate other attributes of the client. The client requests authentication. If they match, the packet code=3 and the authentication is successful and then accordingly to conduct the authorization and accounting process, otherwise the packet code=4.

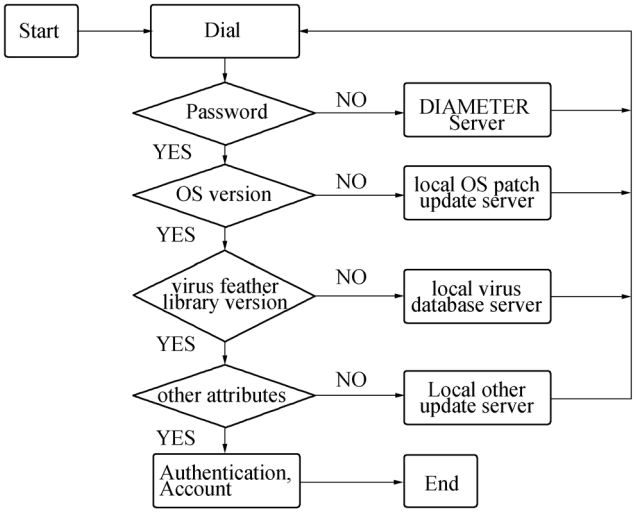

Figure 2
Expanded Authentication Process

The design idea is that each stage is a specific requirement. Only when all the requirements are met, the access object is taken as a qualified client to be authorized to access network resources. Set each extended attribute matching result is *C*, the number of extended attributes is *I*, then the authentication result of this model is $R = \sum (C*I - 3*I)$. If and only if R=0, the access client is authorized to access the network, account services, and so forth.

CONCLUSION

To reduce waste and harmful information on the Internet, we should conduct governance from the source. Strict access technology and access system are necessary. We should implement network admittance system for access objects. Only qualified objects are authorized to access network resources. Unqualified objects will be isolated until they are qualified.

We should strengthen the authentication management in the AAA system, increase authentication elements, and implement multi authentication to force access objects to meet the eligibility requirements. The DIAMETER-based network management can reduce illegal admittance and illegal access to network resources. In the EAP authentication process, we should enhance the OS authentication, which can force the client to timely plug the terminal's security holes before being invaded to fundamentally reduce the risk and reduce the spread of spams. In the EAP authentication process, we should strengthen antivirus authentication, which can force the client to timely recognize the latest virus before being infected and before the system is destroyed so as to reduce the impact of the virus on the network. According to the specific needs of the enterprise on network security, we can individually extend the authentication attributes in the EAP authentication process to make the enterprise network safer and more efficient.

REFERENCES

Calhoun, P. (2003, September). DIAMETER base protocol. RFC3588. Retrieved from http://www.faqs.org/rfcs/rfc3588.html.

Eronen, P. (2005, August). DIAMETER Extensible Authentication Protocol (EAP) App. RFC4072. Retrieved from http://www.faqs.org/rfcs/rfc4072.html .

Ma, Z. F., & Liang, L. (2006). The design and implementation of the authentication mechanism combined EAP with DIAMETER. *Computer Engineering,* 1000-3428.

Qiu, X. P., & Liu, H. P. (2003). Research on DIAMETER protocol. *Computer Science*, 1002-137X.

Tan, P., & Qian, G. M. (2007). The construction of EAP-based and VPN-based enterprise wireless LAN. *Computers and Modernization*, 1006-2475.

Wang, Z., & Liu, T. H. (2011). Research on the design of DIAMETER-based mobile IPv6 Identity authentication system. *The Journal of Shenyang Normal University (Natural Sciences)*, 1673-5862.

Zhao, Y. C., & Li, D. B. (2005). The structural analysis and expansion of the achievement of AAA protocol. *The Journal of Beijing Institute of Electronic Science and Technology*, 1672-464X.