http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (6): 1206-1212, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.1206.1212

An Authentication and Encryption Scheme of Network Management Message Based on Device Fingerprint

[1]Dengyin Zhang, [2]Jinlian Xu, [2]Chunling Cheng and [2]Qinghan Xue
[1]Key Lab of Broadband Wireless Communication and Sensor Network Technology,
Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China
[2]College of Computer, Nanjing University of Posts and Telecommunications,
Ministry of Education, Nanjing 210003, China

Abstract: With the continuous development of the converged network, the types of equipment increase and each has different device identification. The existing SNMPv3 program by using engineID to identify equipment's legal status and confirm the security of message transmission can't meet the safety management for complex equipments in converged network. The concept of device fingerprint is proposed in accordance to specify and mark kinds of equipments in converged network with its structure defined and generation method designed specifically. The local-key generation program based on device fingerprint and the improved authentication and encryption process of network message are described. Experiment by expanding the definition of MIB and dynamically generating device fingerprint show this scheme protecting the security of network communications in the message authentication and encryption process and achieving security management for complex equipments in converged network. Finally, this study analyzes the safety and practicality of using this scheme in converged network.

Key words: Converged network, SNMPv3, device fingerprint, authentication and encryption

INTRODUCTION

Converged network is an open communication network compromised multiple-heterogeneous networks (mobile network, fixed communication network, the Internet, cable television and a variety of new networks) and technologies. Its universality and openness have truly provided users with a personalized service at anytime and anyplace (Lu *et al*., 2010). After a combination of a variety of networks, the expansion of the network and increase in the number of different kinds of equipments bring a great challenge to the construction of network security management. Authentication of the terminal equipments and network information transmission security are important aspect of converged network security management and project safe operation. The authentication mechanism limits the illegal equipments thefting network resources and the encryption mechanism controls the disclosure of communication content (Ding, 2005).

Currently, the most widely used network management is the Simple Network Management Protocol (SNMP), which is a simple format and convenient to parse. It is easy to implement and can shield the physical differences of the different equipments, which is also used to manage network equipments in converged network. Besides it has three versions and the trend of network equipments is to support SNMPv3. Its user-based security model provides authentication and encryption mechanisms (Blumenthal and Wijnen, 2002). The premise of authentication requires management station and agent share the same local authentication key to calculate message authentication code. If the authentication code 3 of both sides matches, then the message is to be authenticated. Moreover, encryption mechanism is similar to authentication, which also needs station and agent share the same local encryption key to implement message encryption and decryption. The existing local key generation method of SNMPv3 is that each network device has an engine identifier (engineID) for indicating its identity and connects user password with the engineID through message digest algorithm to obtain a local key in the process of communication (Chen and Zhou, 2007). The value of local key, local authentication key and local encryption key is the same.

The engineID is an important parameter to ensure the safety of local key. In traditional TCP/IP network, the engineID of identifying device is composed by the

Corresponding Author: Dengyin Zhang, Science and Technology Park, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

parameters of the device itself, such as vendor enterprise number, IP address or MAC address and specific algorithm in series, yet in converged network interconnected by a variety of heterogeneous network, the engineID can't meet the requirement of identifying a device. Different heterogeneous network device has its own device identification, in TV Internet, you need to use the equipment identification code made up by the operators, batch, vendor code, models and other information to identify and regulate internet TV; Mobile terminal is identified by IMSI (international mobile subscriber identity), IMEI (international mobile equipment identity), ESN (electronic serial number) and MEID (phone device ID); In sensor network, the mark of sensor network, device type, device capability and device location are used to identify and manage sensor nodes (Zeng, 2008).

Therefore, improving the traditional local key generation method is necessary by extending the existing device identification when facing the management of converged network in which various devices interconnected. This study presents the concept of device fingerprint and unifies specification to identify network devices. The method is to utilize device fingerprint to protect user password and generate new local key through the message digest algorithm MD5 (Rivest, 1992), which would be used in digital signature authentication process of SNMPv3. After achieving the authentication of the message source, the new local key should be used in CBC-DES (Cipher Block Chaining digital encryption Standard) algorithm (Diffie and Hellman, 1977) to finish the message data unit encryption and achieve the privacy protection requirements of the communication process. So, this study gives an improving authentication and encryption scheme of network management messages to enhance the usefulness of SNMPv3.

DEVICE FINGERPRINT

Device fingerprint definition and structure: Device Fingerprint (DF) refers to an identification code which is calculated by MD5 though connecting information codes such as device type, vendor enterprise number, device location, device property parameters and extended parameters in series, it can be really and uniquely identifying physical devices in the converged network.

Device fingerprint parameter information code is 32 bytes long, which is expressed in hexadecimal number. The structure is shown in Table 1.

The DF parameter code consists of four codes:

- The first four bytes are defined as category code used to indicate the type of device. That is classified by type of network device functions, for example the value of the first byte is 1 which shows traditional Internet communication equipments forwarding data like router and others. The value of the first byte is 2 which represent TV Internet equipments receiving video services such as television. Moreover, the value of the first byte is 3 which indicate the terminal devices which can transfer audio-video data in mobile communication network such as phone. The second byte is further classification according to the device types represented by the first byte value, for instance the traditional Internet equipments can be divided into terminal equipments and data switching equipments and others. And the follow-up 2 bytes are also specific classifications in accordance with the device types represented by the previous byte value, such as data switching equipments can be divided into routers, switches and others and routers are also have broadband router, wireless router, wired router and others
- The next eight bytes are defined as signature code, which indicate some specific characteristics of the device. The 5-8th bytes show private enterprise number of the device provider, such as the number of Cisco private enterprise is No.9 and the four bytes section will be allocated to "00000009"; The 9-10th bytes represent the information of device geographical location which is related to the latitude and longitude values; The 11th byte represents the state of device, if the value is 1 that indicates the device is turned on and 2 indicates that it is turned off. The 12th byte indicates the temperature characteristics of the device environment
- The following 10 bytes are defined as property code, which indicate the property parameters of various devices. The 13th byte is defined how to use the other 9 bytes, if value of the 13th byte is 1, which shows the following 6 bytes are MAC address, the value of 2 shows that the following bytes are

Table 1: The structure of device fingerprint parameter information code

Category code	Signature code (bytes)				Property code (bytes)		Spreading code (bytes)
Device type							
Classification No.	Vendors enterprise No.	Location	Work-status	Temperature	Device property	Parameters	Extended parameters
1-4	5-8	9-10	11th	12th	13th	14-22	23-32

Table 2: Device type classification number definition

First byte	Second byte	Third byte	Fourth byte
1: Traditional Internet communication equipments	1: Terminal equipments	1: Computers	1: Digital computer
		2: Printers	1: Laser Printer
	2: Data switching equipments	1: Routers	1: Broadband router
			2: Wireless router
		2: Switches	1: Ethernet switch
2: TV internet equipments	1: Display terminals	1: Fixed terminal	1: Digital TV
		2: Handheld terminal	1: Flat panel display
	2: Signal swap equipments	1: Set-top boxes	1: IPTV Set-top box
3: Telecommunications network equipments	1: Transmission equipments	1: Cable equipments	1: PDH
		2: Fiber optic equipments	1: SDH
	2: Communication equipments	1: Wired device	1: Telephone
		2: Wireless device	1: Radio
4: Sensor network equipments	…	…	…
……	…	…	…

Table 3: Device property code parameters definition

13th byte	14-22 bytes
1	MAC address of a device
2	mobile device electronic serial No.
3	device private specific model
…	…

electronic serial number of mobile devices and 3 means that following bytes are the specific model number provided by the device manufacturer, etc. Take a minimum 10 bytes and supplement insufficient bytes with zeros

- The last 10 bytes are defined as spreading code, which indicate the device expansion parameters. Defining parameters privately that can identify the device on the basis of specific device circumstances

In addition, the parameters value of 4 bytes category code is defined roughly as shown in Table 2.

As defined in Table 2, we can judge the category code of a wireless router in hexadecimal number is: 01020102, a telephone category code is: 03020101, etc.

And the definition of the parameters value of device property code is shown in Table 3.

As defined above are just only examples, which are not including all classification numbers of device type and values of device property parameters. Thus the definition should be based on the actual situation during the process of the application.

Because the device fingerprint parameter information code of 32 bytes long which is plaintext must be expressly unsafe in the network transmission, so we design the value of 16 bytes which is calculated through MD5 encoding process as device fingerprint.

Device fingerprint generation: This article is based on the SNMPv3 protocol to accomplish message authentication and encryption. Device fingerprint is generated in the network management communication process. The core of SNMPv3 system is MIB (Breitgand *et al*., 2002), which is a collection of managed

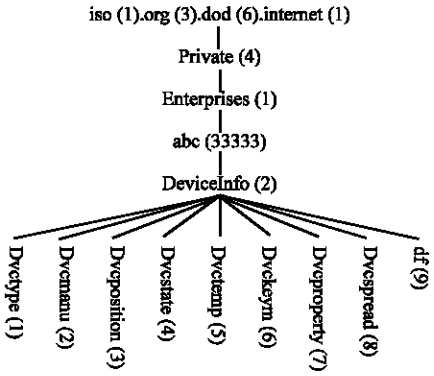

Fig 1: Device fingerprint parameter information branch tree deviceInfo

objects and defines the managed object by using a hierarchical tree structure. MIB of the agent side should be extended before generate a device fingerprint, so that it is capable of storing parameter information codes which constitute the value of device fingerprint. In this study, the expansion of MIB library is achieved by adding the device fingerprint parameter table (deviceInfo) which includes all the information managed by the node. Figure 1 shows the deviceInfo branch tree which is added to the MIB library of agent device.

The first eight field name meanings of the device fingerprint parameter information branch tree deviceInfo in the extension MIB above-mentioned specifically referred in Table 1, such as the ninth field df (9) for storage the value of device fingerprint.

MESSAGE AUTHENTICATION AND ENCRYPTION STRATEGY BASED ON DEVICE FINGERPRINT

In the process of network management message authentication and encryption, the agent firstly queries parameter values which constitute a device fingerprint. Extend MIB library by constructing the devicefingerprint

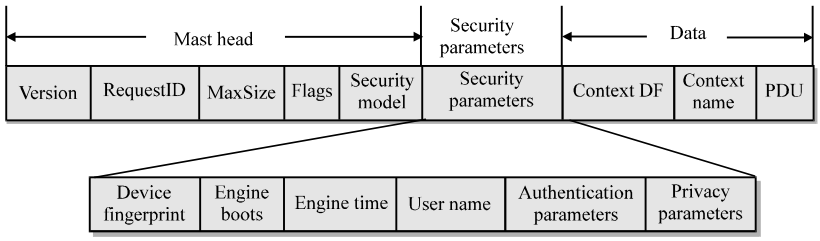

Fig. 2: Improved network management message security parameter fields

parameter branch tree to generate and save device fingerprint. Then use it to protect the user password and get the local key which would be used in the message authentication and encryption.

Figure 2 shows the format of SNMPv3 message and improved security parameter fields. Network management message contains three parts: The mast head, security parameters and data. Meanwhile in security parameters, device fingerprint field representatives the value of device fingerprint. Authentication parameters field represents the message authentication parameters that is used in the certified operator as message authentication code. Privacy parameters field represents message encryption parameters, which is used as salt in the process of forming initial parameter of CBC-DES algorithm (Huang, 2007).

Local key generated dynamically based on device fingerprint: Each user has an unique password key. Join the user key to the proxy device fingerprint at its ends and calculate a new 8 bits local key of 16 bytes long through a MD5 coding process. This local key is required as the local authentication key and the local encryption key and both of them are the same.

Network management message authentication based on device fingerprint: The management station uses the device fingerprint to generate new local authentication key according to the above-mentioned local key generation. Implement authentication parameters of the message with 12 8-bit of 0 string, then combine the local authentication key with message in series to generate the authentication code by MD5 and use this code to fill the blank authentication parameters. After receiving message, agent firstly saves authentication parameters and resets this field to 0 string. Using the device fingerprint of MIB library to generate new local authentication key and combine the resetted message to calculate a new message authentication code. If the two codes are equal, then the source identity is certified and confirming that the message has not been modified during transmission, otherwise it would be discarded.

Network management message encryption based on device fingerprint: Encryption adopts CBC-DES algorithm and it is similar to the authentication process. Management station firstly generate a new 16 bytes local encryption key by using the acquired device fingerprint and then let its bottom 8 bytes XOR with salt to get the initial vector. In addition the unit of the message is divided into 64-bit data blocks and let each data block XOR with the previous ciphertext, then use the front 8 bytes value of the local encryption key to deal with the result of XOR by designing a DES algorithm and the result is used in the continuous process of next data block encryption. The decryption process is similar to the encryption by using the device fingerprint of MIB library to generate a local decryption key which is used in CBC-DES decryption and then acquire the whole message plaintext.

MESSAGE AUTHENTICATION AND ENCRYPTION PROCESS

In order to fulfill the authentication and encryption scheme proposed in this study, a converged network management message communications scene should be built like this: Management station may initiate a get message request (Get operation) to an agent (Agent010) to get the value of the MIB object sysName.0 and the management station user A has password0. When the station initiates a communication request, the agent firstly search for information about device type, device characteristics and device property parameters in the MIB library, then generates and saves its device fingerprint DF010 dynamically. This device fingerprint only represents Agent010.

Figure 3 shows the process of converged network management message authentication and encryption based on device fingerprint:

- **Step 1:** The management station NMS firstly initiates a communication request. Because there is no device fingerprint of the agent Agent010 in the first

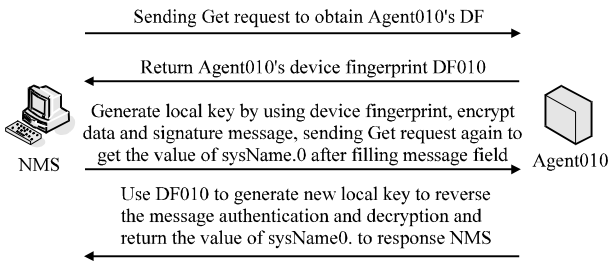

Fig. 3: Converged network management message authentication and encryption process

communication, so the device fingerprint field of the request message is set to NULL, then send this message to Agent010 without any authentication and encryption parameters

- **Step 2:** Agent010 receives this network management request message and find the device fingerprint field is NULL, then collect the real-time information from the MIB library to construct a new device fingerprint parameters branch tree deviceInfo. Combining values of its first eight leaf nodes serially to generate device fingerprint DF010 by MD5 coding dynamically, saving it and then report the error to NMS and send a response message. This message contains the value of DF010 saved by NMS when it receives this response message. Thus achieve the dynamic generation of device fingerprint and the communication of first handshake
- **Step 3:** NMS sends a request message again to Agent010 to obtain the value of its MIB object sysName.0. The device fingerprint field of this message is value of DF010 generated in step 2. Join password0 to DF010 at its ends to calculate local key by MD5 for being used in data encryption and signature authentication. Then send the complete request message to Agent010
- **Step 4:** After receiving the request message, Agent010 has to reverse authentication and decryption. Firstly saving message authentication code MAC1 and taking the device fingerprint in the MIB library to generate new local key, then binding the pretreated message with this key to generate new message authentication code MAC2. If the two codes are equal, then the message identity is authenticated. Press of decrypting ciphertext is similar to encryption process
- **Step 5:** When the request message is being successfully authenticated and decrypted, searching the value of sysName.0 in the MIB library and filling the value field of response message. The fulfilling of the other message fields is just like step 3 and then send whole message to NMS. NMS would authenticate and decrypt reversely to get the variable values. At this point, it is the end of the communication process that NMS initiates a request operation to Agent010 for getting the value of sysName.0. Therefore the network management message authentication and encryption is ultimately finished

SCHEME EVALUATION

Security and practicality analysis: This scheme provides message origin authentication, information confidentiality and data integrity services through authentication and encryption strategy which is based on device fingerprint, effectively prevent network attacks including identity camouflage, information leakage and message tampering.

Firstly, the handshake step of authentication and encryption process makes the station obtains the agent's device fingerprint. This value is the digest of device fingerprint parameter information code which is generated dynamically. Since MD5 algorithm is irreversible, it is impossible to crack the relevant parameters plaintext from device fingerprint, so this scheme will not disclose information about the device in transmission process, thus protects the privacy of devices.

Secondly, the device fingerprint is used in the follow-up session communication process to encrypt and authenticate message. Due to the principle of message digest authentication method, any minor changes in the source data will cause different digest code. If the message authentication code which is generated by device fingerprint is the same as message authentication parameters, it means the network management message is really from the same agent. When receiving the message from the station, the agent uses the same device fingerprint to authenticate messages to ensure that the message comes from the right station. All these can resist the threat of impersonation, prevent camouflage users and also ensure the integrity of the message.

Besides the effective payload of message is the field of PDU, which contains the key data in the message

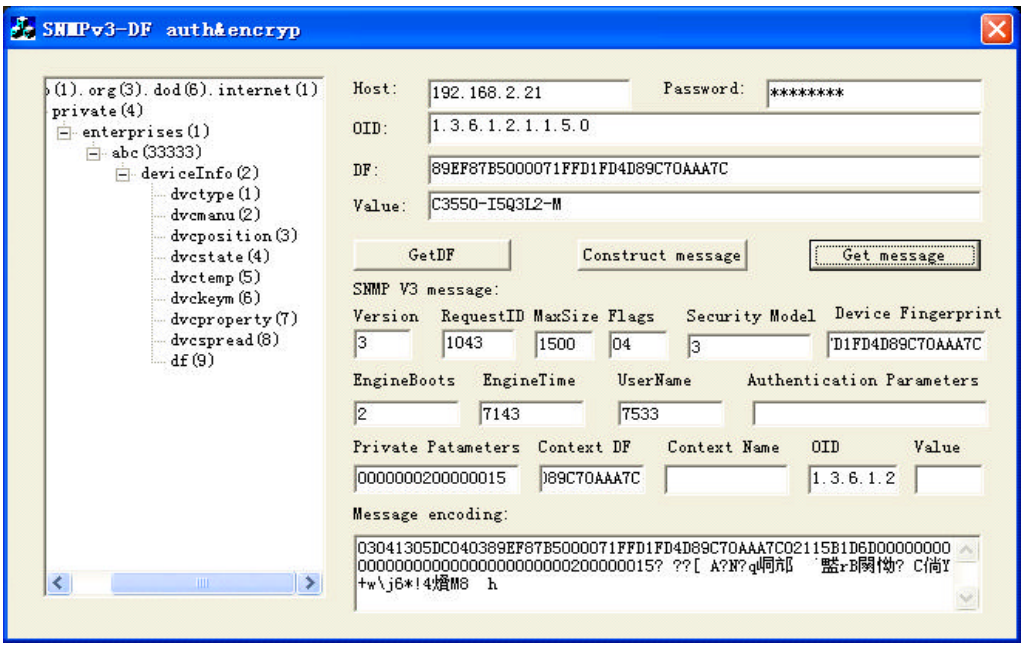

Fig. 4: Experimental test results

Table 4: The device fingerprint parameter branch tree deviceInfo members value

OID	Value
1.3.6.1.4.1.33333.2.1 (dvctype)	01020100
1.3.6.1.4.1.33333.2.2 (dvcmanu)	00000009
1.3.6.1.4.1.33333.2.3(dvcposition)	0D33
1.3.6.1.4.1.33333.2.4 (dvcstate)	01
1.3.6.1.4.1.33333.2.5 (dvctemp)	1E
1.3.6.1.4.1.33333.2.6 (dvckeym)	02
1.3.6.1.4.1.33333.2.7 (dvcproperty)	0019E7A78B01231FA1
1.3.6.1.4.1.33333.2.8 (dvcspread)	F325FF49304196BEC83D

interaction. The data portion of the program is encrypted by CBC-DES and the encryption key and the initial vector are generated by device fingerprint. Due to the unknown of the key, so even if the attacker could intercept the cipher text and message parameters, he can't determine the initial vector and also can't decrypt the packet message. Therefore this strategy is able to protect important data information.

What's more, this scheme proposed in the study extends the applications of SNMPv3 protocol in the integration of converged network management. Nowadays the modern converged network equipments are heterogeneous and multi-manufacturers, it must be necessary to improve the traditional SNMPv3 to make it adapt to the integrated network management of heterogeneous equipments. The scheme achieves changes of part of the parameter section in network management message, improves the versatility of the message communication process and ensures the efficiency of the SNMPv3 security mechanisms.

Experimental evaluation: Based on the source code (http://www.agentpp.com/snmp_pp3_x/snmp_pp3_x.html), this study achieves network management message authentication and encryption process. This process is depended on device fingerprint and operated between the agent side and the management station. The test environment is: WinXP operating system and VC^{++} 6.0 software loaded with the improved snmp_pp library. Test contents are: value of device fingerprint which is generated by agent devices dynamically and to verify whether the authentication and encryption process are successful through the Get operation. Then use the MFC interface to display the results.

During the experiment, initialing the eight object members of the private branch tree deviceInfo in MIB library to hexadecimal values first which is showed in Table 4.

And then set SNMPv3 packet parameters and construct message. Enter the agent IP address in the address bar and select the device object OID. Then send GetDF operation to the agent through the management station and parse out the value of the agent device fingerprint from the results. Finally, send the Get command to the agent again and return the value of the object sysName.0 which is required. Figure 4, shows the value of DF and sysName.0 will be acquired and the data portion of the packet which is observed is encrypted garbled string.

The experimental results show that management station and agent reach the correct communication on the security level of authentication and encryption. Then, set other device and packet parameters the results are all expected, which verify the correctness of the message authentication and encryption process which is based on device fingerprint. Therefore achieve that the SNMPv3 supports the complex converged network devices management.

CONCLUSION

Due to the problem of local key generation in the process of converged network management message authentication and encryption, this study proposes a new solution which extends the application of the device fingerprint technology and defines the device fingerprint to calculate the local key, which enhances the applications of SNMPv3 in converged network. Besides, the message authentication and encryption process is safe and reliable, which is very important in converged network message communications and security equipment management.

REFERENCES

Blumenthal, U. and B. Wijnen, 2002. User-based security model (USM) for version 3 of the simple networks management protocol (SNMPv3). IETF RFC3414. http://dl.acm.org/citation.cfm?id= RFC3414

Breitgand, D., D. Raz and Y. Shavitt, 2002. SNMP GetPrev: An efficient way to browse large MIB tables. Selected Areas Communi., 20: 656-667.

Chen, Y. and T. Zhou, 2007. SNMPv3 security mechanism for key distribution system design and implementation. Comput. Appli., 25: 2755-2758.

Diffie, W. and M.E. Hellman, 1977. Exhaustive cryptanalysis of the NBS data encryption standard. IEEE Comput., 10: 74-84.

Ding, Y., 2005. SNMPv3 security analysis and the improving on it in network management application. Nanchang University.

Huang, X., 2007. SNMPv3 new security features research and implementation. University of Electronic Science and Technology, Chengdu.

Lu, J., S. Yao, H. Huang and M. Zhou, 2010. An information security policy in converged network. Proceedings of the IEEE International Conference on Information Theory and Information Security (ICITIS), Demember 17-19, 2010, Beijing, pp: 335-339.

Rivest, R., 1992. The MD5 message-digest algorithm. RFC1321, MIT Laboratory for Computer Science and RSA Data Security, Inc., http://www.ietf.org/rfc/rfc1321.txt

Zeng, J., 2008. Network convergence is an evolving process. China's New Commun., 10: 86-87.