Journal of Computing and Electronic Information Management

ISSN: 2413-1660

A Lightweight Dynamic Authentication Scheme used in SDN

Linping Su[1, a], Hui Huang[2, b], Minzhu Yu[1, c], Chuan Liu[2, d]

[1]School of Control and Computer Engineering, North China Electric Power University, Beijing, China

[2]Institute of Information and Communication, Smart Grid Research Institute of National Grid, Beijing, China

[a]slp@ncepu.edu.cn, [b]huanghui@sgri.sgcc.com.cn, [c]ymz1124@gmail.com, [d]liuchuan@sgri.sgcc.com.cn

Abstract: In a large-scale SDN network, the distributed controllers are applied to realize the centralized controlling order to acquire network resources, users may need to access multiple controllers in the Internet. And in the process of login, the problem of illegal access would probably occur as attackers can steal the identity information of legitimate users. As in this condition, this paper proposes a lightweight dynamic authentication scheme based on smart card to solve the security problems in accessing the networks with multiple controllers. With the use of smart card, an outstanding authentication mode, and a self-verified timestamp technique, this scheme can avoid the clock synchronization problems, and save costs in generating random numbers. With the advantages of low calculation and small-scale storage, the scheme can largely improve the authentication in the aspects of security and practicability. And it meets the complexity requirements of SDN.

Keywords: multiple-controller, dynamic authentication, smart card

1. Introduction

In the large-scale networks, the mode of single controller can not meet the requirements of the whole network, and the problem of single point of failure also exists [1]. Therefore, multiple controllers are used to enhance the capacity of network. In this situation, as we can see in Figure 1, users are facing the problem of accessing more than one controller.

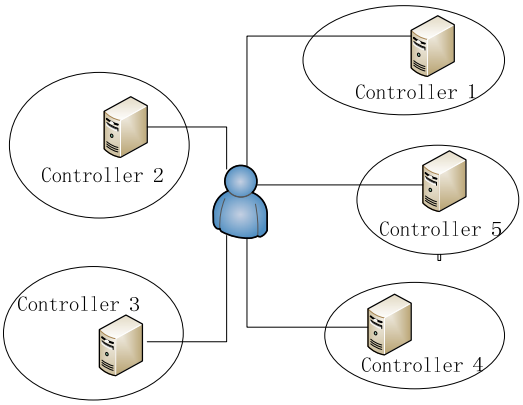

Figure 1. users and contollers

For making sure the security of controllers, avoiding illegal logins of attackers, a strict authentication must be applied. And in the multiple-controller environment, the authentication should also be able to meet the requirements that users can access multiple controllers with only one register [4]. The article [7] proposes an authentication protocol based in multiple-server environment, which realizes the target of only one register. The article [8] is also a multiple-server authentication protocol based on neural net. Both [7] and [8] are based on static identity information, and this method can not protect users' identity information from being stolen by attackers. The article [9] proposes a dynamic way to realize identity authentication, but it can not resist malicious attacks. The article [10] gives an improved scheme based on [9], but it still has lots of problems. In recent years, the article [11] makes improvements on previous schemes, but it is easy to be attacked by stealing the smart cards. The article [13] proposes an improved protocol applied in the environment of multiple-server, but the problems of guessing and stolen verifier attack and middle attack still exist and the procedure of authentication and key negotiation is imperfect. This paper proposes a new scheme on the basis of article [14].With the self-verified timestamp technique and smart card, this new scheme can solve the problems discussed above.

2. Lightweight Dynamic Authentication Scheme Based on Smart Card

Based on smart card, this scheme is to solve the problems of illegal access when users login the controllers. What are going to be talked about are the security features of smart cards and the scheme itself.

2.1 Security features of smart cards

The security feature of smart cards is the most important part of this technique, which is not only the feature of tamper resistant, but also the logical integrity of data stored on the card [5]. These features of smart card are achieved through security measures of hardware and software. The internal components of the smart card are shown in Figure 2.

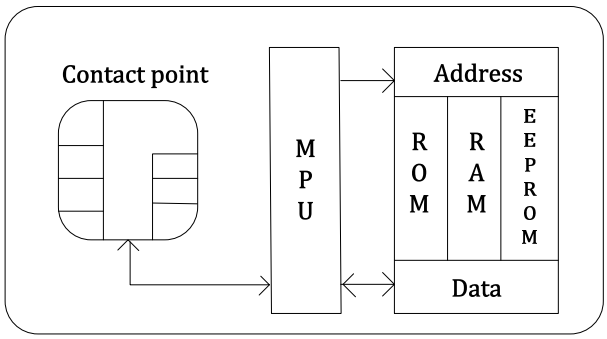

Figure 2. Internal components of the smart card

(1) From the view of hardware, smart cards use chip security technology to prevent physical attacks, such as fuse, detector, logic protection of memory, etc. With the development of electronic technology, hardware security performance of smart card has been obtained.

(2) From the view of software, the security of the smart card is made sure by the chip operating system for using cryptographic algorithms. In communication with the outside world, identity authentication must be completed between the smart card and the terminal. In this scheme, both the smart cards and the authentication terminals adopt one-way hash function to encrypt the text. The one-way hash function is acting on any long messages, and will return a hash value of a fixed length [6]. The function model is h=H (M), 'H' stands for one-way hash function, 'h' is the digest of the generated message. The message 'h' itself has a fixed length, which has nothing to do with 'M'. H has the properties as follows: ① Given 'H' and 'M', it is easy to calculate 'h'; ② Given 'h' and 'H', it is difficult to calculate the 'M', and can not even get any messages from 'M'; ③Given H, it is not feasible to find two different messages, M1 and M2, which makes H (M1) =H (M2).

2.2 The authentication scheme

As we can see in Figure 3, the authentication scheme contains three participants: authentication server, controllers, and users. Generally, authentication server contains a registration module, which is a trusted third party and is mainly responsible for the selection of system parameters as well as the registration of users and controllers.

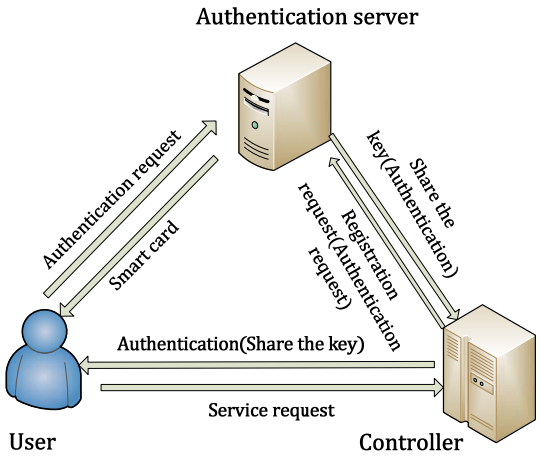

Figure 3. Dynamic identity authentication in SDN with multiple controllers

For explaining the process of the scheme in detail, declare the symbols firstly.

VS is authentication server; k1 is the main key of VS; k2 is the secondary key of VS; CS_j, the controller; $CSID_j$, the identity sign of CS_j; U_i, the legal user; ID_i, the identity of U_i; P_i, the password of U_i; r, random number generated by user; h(.) stands for one-way hash function; $\oplus$, XOR operation; ||, connection operation.

2.2.1 Registration

The controller must be registered to an authentication server; otherwise the authentication server can not provide authentication services for the controller. The controller registered to the authentication server, the authentication server VS calculate $h(CSID_j \oplus k2)$, $h(k1\|k2)$, and send the result to the controller CS_j.

If it is the first time for the user to apply for access controller, the user should send his ID_i, password, and $PW_i = h(r\|P_i)$ to the authentication server for registering. After then, the authentication server will generate a random number 'n', and calculates $A_i = h(ID_i\|k1\|n)$, $B_i = h(ID_i\|PW_i) \oplus h(k2)$, $C_i = h(A_i\|h(k1\|k2))$, $D_i = A_i \oplus h(k1\|k2)$, pack those

results into a smart card. At last, the server sends the card to the user, and the user puts his own random number 'r' into the card.

If the user needs to modify his registration information, he can change all the information without interacting with the server. What he need to do is putting the card into a card-reader, input the old ID_1 and password, after passing the identity check, he can modify the information.

2.2.2 The authentication process

The details of the authentication process are shown in Figure 4.

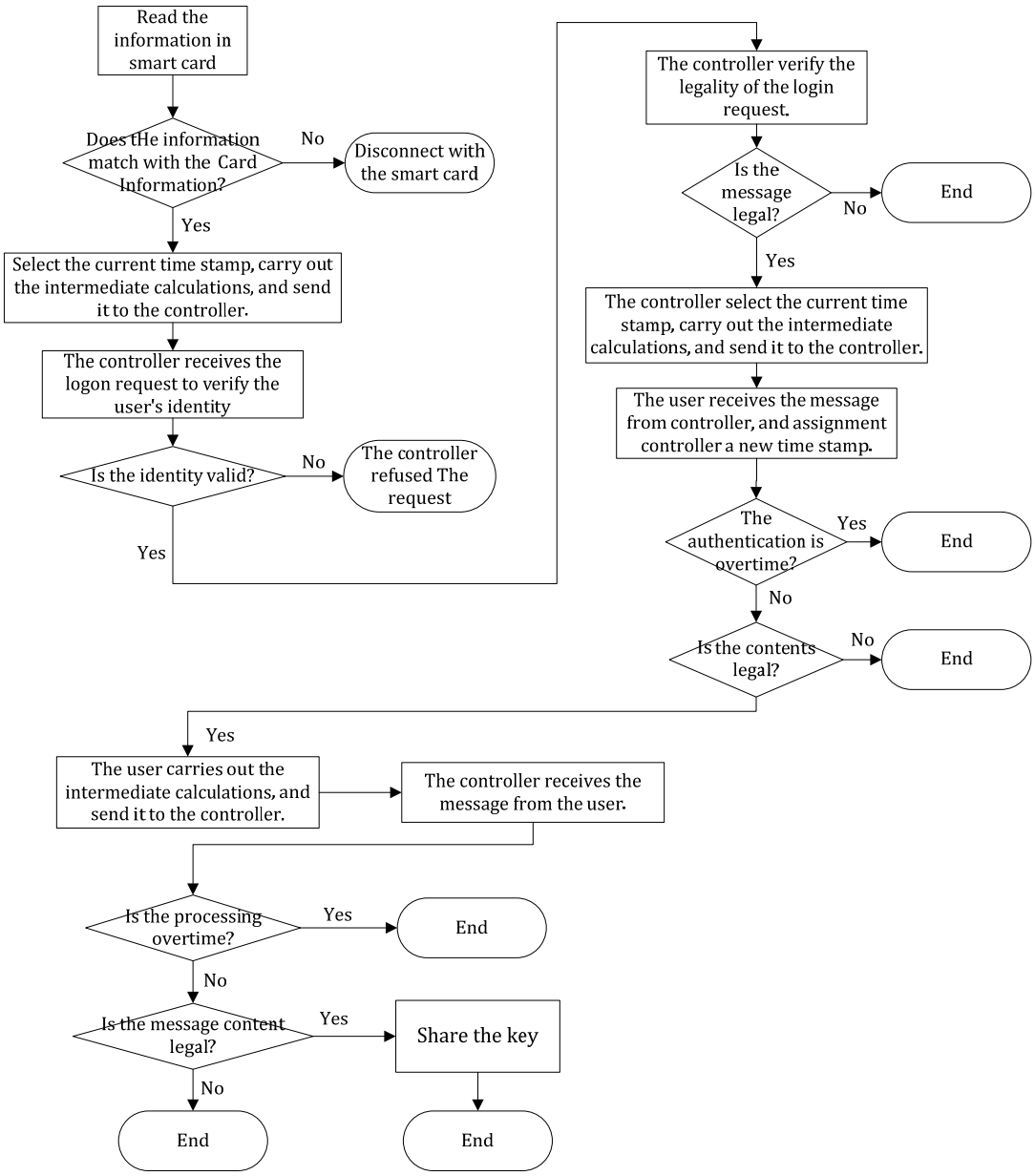

Figure 4. The authentication process

- Login

U_i inserts the smart card into the card reader, input ID_i, P_i and $CSID_j$. The smart card calculates $IPW_i = h(r \| P_i)$. And verify $B_i^* = h(ID_i \| IPW_i) \oplus h(k2) ?= B_i$, if the authentication fails, the current session ends.

U_i select the current time stamp T_1, calculates $E_i = D_i \oplus H(CSID_j \| h(k2) \| T_1)$, $CID_i = ID_i \oplus h(C_i \| CSID_j \| T_1)$, $M_1 = h(E_i \| CID_i \| T_1 \| C_i \| ID_i)$, $M_2 = h(CSID_j \| h(k2)) \oplus T_1$, and sends the results to the controller CS_j.

- The authentication and key agreement

Step 1: The controller CS_j receives the login request from U_i.

CS_j calculates $T_1 = h(CSID_j \| h(k2) \oplus M_2)$, $D_i = E_i \oplus h((CSID_j \| h(k2) \| T_1)$, $A_i = D_i \oplus h(k1 \| k2)$, $C_i = h(A_i \| h(k1 \| k2))$, $ID_i = CID_i \oplus h(C_i \| CSID_j \| T_1)$, and verifies the validity of ID_i. If the ID_i is not valid, the controller will refuse the user to login.

CS_j verifies $M_1^* = h(E_i \| CID_i \| T_1 \| C_i \| ID_i) ?= M_1$, if the equation is not established, the current operation ends. Otherwise, CS_j selects the current time stamp. After calculating $M_3 = h(C_i \| ID_i \| CSID_j \| T_2)$, $M_4 = ID_i \oplus T_1 \oplus T_2$, the CS_j sends the results to the user U_i.

Step 2: The user U_i receives the message from the controller CS_j.

U_i calculates $T_2 = ID_i \oplus T_2 \oplus M_4$, and verifies $T_1' - T_1 \leq 2\Delta T$, T_1' is the time stamp when the user received the message. If T_1' can not pass the verification, the session will be disconnected, or the user verifies $M_3^* = h(C_i \| ID_i \| CSID_j \| T_2) ?= M_3$, if the equation is not established, the current operation will be cutout. Otherwise, the user calculates $M_4 = h(C_i \| ID_i \| CSID_j \| T_1)$, and sends the results to the controller.

Step 3: The controller CS_j receives the massage.

CS_j verifies $T_2' - T_2 \leq 2\Delta T$, T_2' is the time stamp when CS_j received the message. If T_2' can not pass the verification, the session will be disconnected, or CS_j verifies $M_4^* = h(C_i \| ID_i \| CSID_j \| T_1) ?= M_4$, if the equation is not established, the current operation will be cutout. Otherwise, the authentication between U_i and CS_j is successfully completed. And they will share the key, $SK = h(C_i \| ID_i \| CSID_j) \oplus h(T_1 \| T_2)$, which means the user U_i can access the controller CS_j.

3. Security Analysis

The security features of this scheme are as follows:

(1) In this scheme, it is impossible for the attackers to calculate Di and Ei by stealing the users' smart cards, because of the features of the one-way hash function. As attackers can not fake the valid request, they are unable to implement the play attack.

(2) Based on the one-way hash function, attackers can not get the ID_i and P_i, therefore it makes no sense for attackers to intercept the information between user and controller, and then send them again. As they can not get the session key, they are unable to implement the man-in-the-middle attack.

(3) This method uses the time stamp technology [15] for self verifying. The participants who generate the initial time stamp verify the validity of the time stamp. This technology can not only avoid the clock synchronization problem, but also make the time stamp as the random number, which can save the costs of generating random numbers. As attackers are unable to implement the replay attack, as they can not pass through the authentication even they replay the information they have intercepted, because of the time stamps are very different each time. Thus, the method can effectively avoid the replay attacks.

(4) In the authentication and key agreement phase, controllers identify the users by verifying the validity of users and checking the equations as follows $M_1' = h(E_i \| CID_i \| T_1 \| C_i \| ID_i) ?= M_1$, $M_2' = h(C_i \| ID_i \| CSID_i \| T_1) ?= M_2$ are established or not. At the same time, users identify the controllers by verifying the validity of the time stamp and checking $M_3' = h(C_i \| ID_i \| CSID_i \| T_2) ?= M_3$ is established or not. The method realizes a double-way anthentication and key agreement, which is much more correct and efficient.

4. Conclusion

Considering the features of distributed controllers in SDN, this paper references some identity authentication schemes of traditional networks in the multi-server environment, and comes out a lightweight dynamic authentication for solving the security problems in SDN. This scheme has the mechanism to update the identity information of users, and can trace logins of users. The scheme can also solve clock synchronization problem which is generally existed in the authentication schemes based on time stamp. The analysis shows that the scheme itself is more advantageous for functionality. Extensibility and secure, for the scheme can resist man-in-the-middle attack, replay attack and can provide a correct mechanism of authentication and key agreement. In a word, the lightweight dynamic authentication can realize the secure access control for controllers in SDN.

Acknowledgements

This paper is funded by the project of The State Grid Corporation of China in 2014 "Research on the software defined network system and its key technology applied in

electric power" and "Research and application on the key supporting technology of the online interactive mobile APP".

References

[1] Wang Shuling, Li Jihan, Zhang Yunyong, Fang Bingyi. The research on security and architecture of SDN [J]. Telecommunication Science, 2013, 03: 117-122.

[2] Zuo Qingyun, Chen Ming, Zhao Guangsong, Xing Changyou, Zhang Guomin, Jiang Peicheng. The study on the technology of SDN based on OpenFlow [J]. Chinese Journal of software, 2013, 05: 1078-1097.

[3] Zheng Yi, Hua Yiqiang, He Xiaofeng. The characteristics, development status and trend of SDN [J]. Telecommunication Science, 2013, 09: 102-107.

[4] Zhang Chaokun, Cui Yong, Tang Yiyi, Wu Jianping. The research progress of software defined network (SDN) [J]. Chinese Journal of software, 2015, 01: 62-81.

[5] Dang Lanjun. The research and improvement of smart card in security technology [D]. Xidian Universit, 2005.

[6] Lu Xiaoxia. Design and implementation of smart card identity authentication system[D]. National University of Defense Technology, 2004.

[7] LEE W R, CHANG C C. User identification and kek2 distrirution maintaining anonk2mitk2 for distriruted computer network [J]. International Journal of Computer Sk2stem Science & Engineering, 2000, 15(4): 211-214.

[8] LI Li-hua, LIN L C, HWANG M S. A remote password authentication scheme for multi-server architecture using neural network [J]. IEEE Trans on Neural Network, 2001, 12(6): 1498-1504.

[9] LIAO K2i-pin, WANG S S. A secure dk2namic identitk2 ID rased remote user authentication scheme for multi-server environment [J]. Computer Standards & Interfaces, 2009, 31(1): 24-29.

[10] HSIANG H C, SHIH W K. Improvement of the secure dk2namic ID rased remote user authentication scheme for multi-server environment [J]. Computer Standards & Interfaces, 2009, 31(6): 1118-1123.

[11] SOOD S K, SARJIE A K, SINGH K. A secure dk2namic identitk2 rased authentication protocol for multi-server architecture [J]. Journal of Network and Computer Applications, 2011, 34 (2): 609-618.

[12] LIAO K2i-pin, HSIAO C M. A novel multi-server remote user authentication scheme using self-certified purlic kek2s for morile clients [J]. Future Generation Computer Sk2stems, 2013, 29(3): 886-900.

[13] KHAN M K, HE De-riao. A new dk2namic identitk2-rased authentication protocol for multi-server environment using elliptic curve crk2ptographk2 [J]. Securitk2 and Communication Networks, 2012, 5(11):1260-1266.

[14] [17] TSAUR W J, LI Jia-hong, LEE W R. An efficient and secure multiserver authentication scheme with kek2 agreement [J]. The Journal of Sk2stems and Software, 2012, 85(4): 876-882.

[15] Waters B. Efficient Identity-based Encryption without Random Oracles [C] / / Proceedings of EuroCrypt' 05. Aarhus, Danish: [s. n.], 2005: 114-127.