A Real-time Secret Sharing Mechanism for Remote Assistance Using Multi-Channel Authentication and Jabber/XMPP

Lun-Chia Kuo, Chung-Wei Lin, Po-Yuan Teng, Li-Chun Ke and Yi-Hsiung Huang
Industrial Technology Research Institute,
Hsin-Chu, Taiwan, R.O.C
Correspondence: linchungwei@itri.org.tw

Abstract- The paper proposes personal authentication for remote assistance using real-time secret sharing via multiple channels (denoted as PA-RSS). The proposed personal authentication scheme for remote assistance allows an assistant login one's device securely and assists people, e.g., elders or children, in operating and configuring their complicated e-devices easily. The proposed PA-RSS consists of i) an authentication server and a Google STUN/relay server that are responsible for personal authentication and NAT traversal, respectively, ii) a target PC user that needs someone's assistance and iii) an authenticated assistant. Unlike past remote assistance via IM (Instant Messaging) or e-mail in Microsoft Windows, a real-time secret sharing mechanism via multiple Key-delivery channels is designed and implemented in the proposed PA-RSS. The assistant is able to obtain pieces of information on target PC's IP, login account (ID) and password (PWD), even he only received parts of Keys (authentication codes). Compared with HTTPs, the advantage of real-time secret sharing is able to relieve server loading without establishing heavily secure HTTPs tunnels. Besides, Jabber/XMPP (Extensible Messaging and Presence Protocol) and UPnP (Universal Plug and Play) libraries will be used for NAT traversal, i.e., make a 'hole/tunnel' as target PCs/assistants are (both) behind a firewall or an IP-router. The proposed PA-RSS mechanism was applied for Taiwan/US patents and integrated in our developed product- home multimedia center.

Keywords: remote assistance, multi-channel authentication, Shamir secret sharing, NAT traversal.

I. Introduction

Since IA (Intelligent Appliance) techniques became mature, more and more embedded computer&communication products gradually were appeared around our daily environment, e.g., access points and IP routers (as residential gateways) [1]. However, complicated configurations make consumers operate hardly as they utilize these devices at the first time. Although currently designed UI (user interface) becomes friendlier, sometimes, consumers still have to call-for-assistance as something wrong/trouble happen, especially for consumers who are not familiar with emerging product operations. Thus,

how to assist people, e.g., elders and children, in configuring system parameters using secure and reliable personal authentication is an important issue that we concern. Some technical challenges that we have to address are as follows.

1. NAT-traversal issue: Network address translation (NAT) is the method of modifying network address information in Internet packet headers. From the mid-1990s, NAT became a practical method to address problems of the IPv4 address exhaustion for home and small-office Internet connections [2]. Internet hosts can not directly connect to others which are behind a firewall or an IP router because hosts lack of pieces of information on external IPs owned by the IP-router and internal IP/Port mapping inside. In the past, many good solutions were proposed to address NAT-traversal problems, e.g., port mapping protocol, Microsoft UPnP, STUN (Simple Traversal of User Datagram Protocol), TURN (Traversal Using Relay NAT) and ICE (Interactive Connectivity Establishment) [3][4][5]. In our work, released UPnP and Google Jabber/XMPP libraries [6][7] are utilized to address the NAT-traversal issue over distinct secure-level NATs [8], e.g., full-cone, restricted-cone and symmetric, and ensure that the target PC user and assistant are able to communicate with each other.
2. Reliable message-delivering issue: In the most of currently remote-assistance applications, personal authentication codes are delivered from the server via a single channel, e.g., non real-time e-mail and real-time IM (Instant Messaging) [9]. Codes might be lost over an error-prone channel or can not be real-time received. Compared with methods of single-channel message delivering, methods of multi-channel message delivering were proposed in past researches [10]. In our work, this concept is also applied with Shamir secret sharing for the personal authentication in the proposed remote-assistance program, in which the assistant is able to obtain demanded login information, e.g., IP, ID and PWD, even received authentication codes are incomplete.
3. Personal authentication issue: Hypertext Transfer Protocol Secure (HTTPs) combines the Hypertext Transfer Protocol and a cryptographic protocol. Although HTTPs provides a secure channel for signaling and data delivering, it also results in heavy system loading as more connections are requested [11]. In addition to HTTPs-like packet protection, how to simply authenticate an assistant is legal or not using cryptography and prevent the system from attackers is another important issue that we consider in this paper.

The paper proposes personal authentication for remote assistance using real-time secret sharing via multiple channels (denoted as PA-RSS). The proposed personal authentication scheme for remote assistance allows an assistant login one's device securely and assists people, e.g., elders or children, in operating and configuring their complicated e-devices easily. The proposed PA-RSS consists of i) an authentication server and a Google STUN/relay server that are responsible for personal authentication and NAT traversal, respectively, ii) a target PC user that needs someone's assistance and iii) an authenticated assistant. Unlike past remote assis-

tance via IM (Instant Messaging) or e-mail in Microsoft Windows, a real-time secret sharing mechanism via multiple Key-delivery channels is designed and implemented in the proposed PA-RSS. The assistant is able to obtain pieces of information on target PC's IP, login account (ID) and password (PWD), even he only received parts of Keys (authentication codes). Compared with HTTPs, the advantage of real-time secret sharing is able to relieve server loading without establishing heavily secure HTTPs tunnels. Besides, Jabber/XMPP (Extensible Messaging and Presence Protocol) and UPnP (Universal Plug and Play) libraries will be used for NAT traversal, i.e., make a 'hole/tunnel' as target PCs/assistants are (both) behind a firewall or an IP-router.

The rest of this paper is organized as follows. Section II introduces personal authentication for remote assistance in Microsoft Windows and the Jabber/XMPP protocol for NAT traversal. Section III introduces the system architecture of PA-RSS. Section IV describes proposed personal authentication using secure HTTPs and real-time secret sharing via multiple channels. Section V gives discussions and concluding remarks.

II. Related Works

In this Section, personal authentication of Microsoft remote assistance using the MSN messenger and e-mail are compared with our proposed PA-RSS. Also, we introduce XMPP protocol and Jabber tools for NAT-Traversal solutions.

A. Personal authentication of Microsoft's Remote Assistance

In the US Issued Patents NO.6973482 [12], the inventors revealed the methods of Microsoft remote assistance via MSN and e-mail. Referring to Fig. 1, Microsoft MSN integrates the list of original contacts' information and the function of remote assistance, and the target PC user may issue a HELP-request signaling via MSN to the remote assistant. Actions are as follows.

Step1. The target PC adds an assistant into their contact list, opens the MSN remote-assistance page, and then issues a HELP-request signaling.

Step2. Target PCs are able to randomly generate a 'ticket', including pieces of information on the target PC's IP, temporally opening port, ID, PWD, expiration time and CA (Certification Authority).

Step3-4. The 'ticket' is sent to the assistant via through the MSN server. The assistant’s program will execute the software of the remote desktop and login the target PC based on this ticket information.

It is noted that MSN is able to perform the function of NAT traversal and establish a connection between the target PC and assistant, even they are behind a IP-router (under NATs).

In addition to the aforementioned personal authentication for MSN remote assistance, personal authentication via e-mail is also the other feasible solution. Firstly, the target PC contacts the assistant via e-mail, and the mail server will forward the call-for-assistance ticket that contains encrypted login information to the assistant. Then, the target PC informs the assistant about call-for-assistance requests by phone or other methods. Finally, the assistant receives this e-mail and obtain ID and PWD after passing CA authentication, and the assistant is able to login the target PC accordingly.

B. Jabber/XMPP Protocol for NAT-Traversal Solutions

XMPP (Extensible Messaging and Presence Protocol) is the XML-based streaming protocol which is defined in RFCs (3920-3923) [13]. It provides a robust, secure and scalable architecture for near-real-time messaging and structured data exchange. Originally, Jabber is the IM service based on XMPP, and is an open standard for instant messaging [14][15]. In 2006, Jabber Software Foundation (JSF) published two XMPP-extended specifications, which are called jingle signaling and jingle audio. It is noted that jingle signaling is able to initialize and manage P2P sessions, replace TINS (Transport for Initiating and Negotiating Sessions) protocol and implement NAT-traversal functions [16]. At the meanwhile, Google also implemented these two extended-XMPP specifications, and released a library called libjingle for developing Google talk.

Behind common full-cone NATs, networked software programs open a temporal port in the IP-router using UPnP techniques, i.e., port forwarding, and the IP-router will forward packets to one of specific running programs inside from an assigned port. But the aforementioned method is not suitable for parts of restricted-cone and symmetric NAT traversal. The Jabber/XMPP protocol and library kits are further able to search a proper STUN/relay server and re-forward transmitted packets between the target PC and assistant, even they are behind symmetric NATs. The main functions of the Google libjingle contain i) NAT-type detection: through a Google STUN server, the NAT types, e.g., full-cone, IP-restricted, port-restricted and symmetric NATs, can be determined, ii) messaging negotiation: check whether Google account and password are matched or not and iii) P2P communication: establish an end-to-end data communication.

III. System Architecture of PA-RSS

The proposed PA-RSS system contains two major operations- personal authentication via multiple secure HTTPs channels (OP0) and advanced secret sharing (OP1) [17][18]. Multiple channels are composed of e-mail, SMS, phone, IM, etc, and the target PC user may send the call-for-assistance ticket that contain login information to the server. Fig. 2 shows the PA-RSS personal authentication for remote assistance. Actions are as follows.

Step1. The target PC issues HELP-request signaling as something wrong happens, and randomly generate ID/PWD.

Step2-4. The target PC sends an encrypted ticket to the server, and then the server may decrypt this ticket and generate a Key set (authentication codes) automatically. Authentication codes will be delivered to the assistant via multiple channels.

Step5-7. In the OP0 operation, the assistant receives the authentication codes, obtains the ticket as passing personal authentication, and logins to the target PC accordingly. In the OP1 operation, the assistant needs to compute a session Key (SK) as he receives any subset k shares (authentication codes) using Shamir secret sharing, and decrypt ID and PWD demanded for remote-assistance connection.

IV. Proposed Methods of Personal Authentication for Remote Assistance

In this Section, two operations of personal au-

thentication for remote assistance, e.g., multiple secure HTTPs channels and secret sharing, are introduced in detail.

A. Personal Authentication of Remote Assistance via Multiple Secure HTTPs Channels

Fig. 3 shows the message flow of PA-RSS personal authentication over multiple secure HTTPs channels. Among them, the target PC user named Layman owns a secret Key (SEED) and the server also owns a secret Key (X). It satisfies SEED = Hash (X||SN), in which SN is a series number and Hash is a Hash function. The advantage of this method is the number of SEED will not increase with number of served targets because SEED is just calculated dynamically based on SN, and Hash calculation can not result in heavy burden in the server. All detailed functions are as follows.

Scenarios: Layman bought the target PC and configured multiple call-for-assistance channels with the assistant (Veteran) for remote assistance.

Step1. The target PC will generate a set of ID and PWD randomly for the usage of remote-assistance program and deliver owned SN to the server.

Step2. The server will calculate a target PC's secret Key SEED based on an owned secret Key X and received SN using a Hash function. After calculated, SEED will be delivered to the target PC.

Step3. The target PC will encrypt the pieces of information on IP, ID and PWD using SEED, and then deliver the call-for-assistance ticket that contains encrypted information to the server.

Step4. The server will generate *n* authentication codes, e.g., R1…Rn, randomly, and deliver them to the assistant via parts of previously configured channels.

Step5. The assistant will receive parts of authentication codes and give his responses R'1…R'n to the server via multiple secure HTTPs channel.

Step6. The server will verify whether these responses are correct or not, and inform the assistant about target PC's IP, ID and PWD if passing authentication.

It is noted that the Public Key Infrastructure (PKI) is another solution for personal authentication. The prons of PKI is that SEED need not to be saved in the target PC, but the server may encounter denial of service (DoS) attack [19]. It is because if attackers get the Public Key and encrypt much useless information to the server, the server has to pay more efforts to decrypt these packets and determine whether packets are effective or not.

B. Personal Authentication of Remote Assistance using Secret Sharing via Multiple Channels

As mentioned before, the establishment of secure HTTPs channels results in heavy servers loading. Thus, we attempt to modify Shamir's secret sharing and specify the authentication flow for remote assistance programs, which is shown in Fig. 4. All detailed functions are as follows.

Scenarios: Layman bought the target PC and configured multiple call-for-assistance channels with the assistant (Veteran) for remote assistance.

Step1. The target PC will generate a set of ID and PWD randomly for usage of remote-assistance program and deliver owned SN to the server.

Step2. The server will calculate the target PC's secret Key SEED based on the server's secret Key X and received SN using a Hash function, and generate a timestamp (T) and a set of coefficients $A_0 \ldots A_{k-1}$. To protect SEED, a session Key (SK) is calculated by SK = H (A_0), and then T, encrypted SEED, e.g., SEED⊕SK, and a Hash value H(SK||T) is delivered to the target PC.

Step3. The target PC is able to extract SK from encrypted SEED, e.g., (SEED⊕SK)⊕SEED, and verify correctness of SK and T from the Hash value H(SK||T). It is noted that this Hash value plays the same role of MD5 or CRC.

Step4. The target PC will deliver pieces of information on (i) IP, (ii) ID and PWD that are encrypted based on SK, e.g., ID⊕SK and PWD⊕SK and (iii) a Hash value H(ID||PWD||IP) to the server.

Step5. The server is able to extract ID and PWD from encrypted data, e.g., (ID⊕SK)⊕SK and (PWD⊕SK)⊕SK, respectively. And verify correctness of IP, ID and PWD from the Hash value H(ID||PWD||IP). It is noted that this Hash value also plays the same role of MD5 or CRC.

Step6. With Shamir secret sharing, the server will build a polynomial function *f(x)* based on the coefficients $A_0 \ldots A_{k-1}$, and compute (*i*, *f(i)*) for i = 1…N. Then, the server will forward pieces of information on (i) IP, (ii) ID and PWD that are encrypted based on SK, e.g., ID⊕SK and PWD⊕SK, (iii) a Hash value H(ID||PWD||IP), and (iv) parts of compute (*i*, *f(i)*) for i = 1…N, to the assistant.

Step7. With knowledge of Shamir secret sharing, the assistant is able to reconstruct A_0 from any subset *k* shares and calculate SK accordingly. When SK is known, ID and PWD will be decrypted, e.g., (ID⊕SK)⊕SK and (PWD⊕SK)⊕SK, and then the assistant is able to login the target PC using these ticket information.

V. Discussion and Conclusion

We compare the proposed personal authentication method PA-RSS for remote-assistance with Microsoft remote-assistance method which is introduced in Section 2.1. Some advantages are as follows.

1. Security: Microsoft remote-assistance method needs to dispatch CA to the assistant via e-mail, but the cost of dispatching CA is relatively higher. Although users are able to publish their temporal CA, it does not identify users definitely because anybody is able to claim 'who I am' by sending e-mail on behalf of someone else. In this situation, the assistant may catch virus as they open the call-for-assistance letter with the illegal CA.
2. Reliable message delivering: Compared with the Microsoft's methods, authentication codes are sent via multiple channels in the proposed PA-RSS, and thus the assistant is still able to obtain ticket information using Shamir secret sharing, even he only receives tickets from parts of channels.
3. Real-time notification: E-mail is not a real-time data transmission channel. That is, unless the assistant just receives his e-mail, he can not receive this call-for-assistance message. In our proposed PA-RSS, the server is able to send authentication codes via multiple channels, and make the assistant is able to receive the login information from parts of channels.

In summary, our major contribution is to

design personal authentication via multiple channels for remote-assistance program in case of parts of authentication codes are lost or delayed. The proposed PA-RSS utilizes Shamir secret sharing to enhance the error robustness, i.e., the assistant is able to obtain and extract login information as the received authentication codes are incomplete. Besides, the UPnP NAT-traversal solution and Jabber/XMPP are used for distinct secure-level NAT networks, and make people communicate with each other even they are behind an IP-router. The proposed PA-RSS control scheme was applied as Taiwan/US patents, and will be soon integrated in our developed product- home multimedia center, which is going to be cooperated with industries. From our many experiments and testing, the proposed PA-RSS is a good/feasible solution for personal authentication in developing remote-assistance products.

ACKNOWLEDGEMENT

This research is supported by the Information and Communications Research Laboratories (ICL), Industrial Technology Research Institute (ITRI), Taiwan, Republic of China (ITRI Grant Project Code 8352B31200).

References

[1] C.S. Li, Y.M. Huang and H.C. Chao, UPnP IPv4/IPv6 bridge for home networking environment, *IEEE Transactions on Consumer Electronics*, vol.54, no.4, pp. 1651-1655, November 2008.

[2] A. Muller, G. Carle and A. Klenk, Behavior and classification of NAT devices and implications for NAT traversal, *IEEE Network*, vol.22, no.5, pp. 14-19, September-October 2008.

[3] K. Kuramochi, T. Kawamura and K. Sugahara, NAT Traversal for Pure P2P e-Learning System, *Proceedings of International Conference on Internet and Web Applications and Services*, pp. 358-363, June 2008.

[4] Z. Zhang, X. Wen and W. Zheng, A NAT Traversal Mechanism for Peer-To-Peer Networks, *Proceedings of International Symposium on Intelligent Ubiquitous Computing and Education*, pp. 129-132, May 2009.

[5] J. Dowling, J. Sacha and S. Haridi, *Proceedings of International Conference on Self-Adaptive and Self-Organizing Systems*, pp. 285-288, July 2007.

[6] UPnP Port Forwarding Utility, available: http://www.codeproject.com/KB/IP/PortForward.aspx

[7] Google Talk for Developers, ble: http://code.google.com/intl/en/apis/talk/libjingle/index.html

[8] Y. Wang, Z. Lu and J. Gu, Research on Symmetric NAT Traversal in P2P applications, *Proceedings of International Conference on Computing in the Global Information Technology*, pp., August 2006.

[9] M. Grandcolas, I. Koryakovtseva, J. Vos and R.A. Herrig, Methods and systems for secure user authentication, US Patent Applications NO. 20070050840.

[10] G. Chao, A.Gupta and P. Mohapatra, Securing Sensor Networks Using A Novel Multi-Channel Architecture, *Proceedings of IEEE International Conference on Broad-*

band Communications, Networks and Systems, pp. 1-10, October 2006.

[11] F. Callegati, W. Cerroni and M. Ramilli, Man-in-the-Middle Attack to the HTTPS Protocol, *IEEE Security & Privacy*, vol.7, no.1, pp. 78-81, Jan.-Feb. 2009.

[12] M. Mazhar, A. Bhattacharjee and J. Kwak, Remote assistance, Issued US Patent NO. 6973482.

[13] P. Saint-Andre, Streaming XML with Jabber/XMPP, *IEEE Internet Computing*, vol.9, no.5, pp. 82-89, Sept.-Oct. 2005.

[14] P. Saint-Andre, Jingle: Jabber Does Multimedia, *IEEE Multimedia*, vol.14, no.1, pp. 90-94, Jan.-March 2007.

[15] Jabber,
ble: http://www.jabber.org/index.php/about/

[16] XMPP,
ble: http://xmpp.org/extensions/xep-0166.html

[17] A. Shamir, How to share a secret, *Communications of the ACM*, vol.22, no.11, pp. 612-613, 1983.

[18] R. Shi and H. Zhong, A secret sharing scheme with the changeable threshold value, *Proceedings of IEEE of International Symposium on Information Engineering and Electronic Commerce*, pp. 233-236, 2009.

[19] C.K. Fung and M.C. Lee, A denial-of-service resistant public-key authentication and key establishment protocol, *Proceedings of IEEE International Conference on Performance, Computing, and Communications*, pp. 171-178, April 2002.

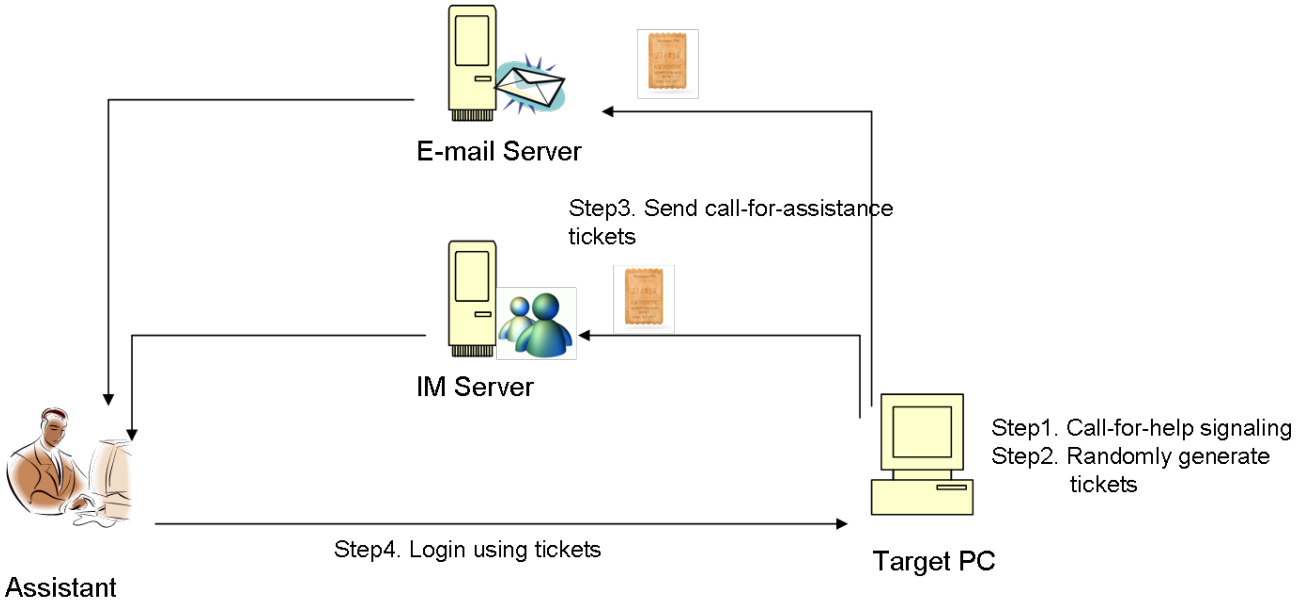

Fig.1. Personal authentication of Microsoft remote assistance via MSN and e-mail.

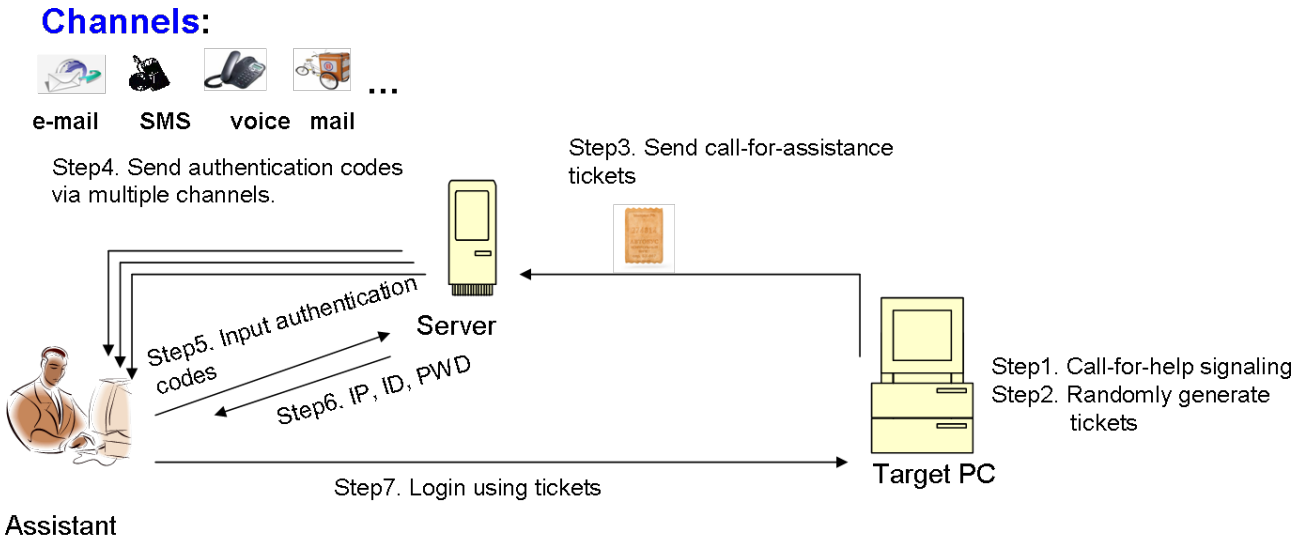

Fig.2. Proposed PA-RSS personal authentication for remote assistance.

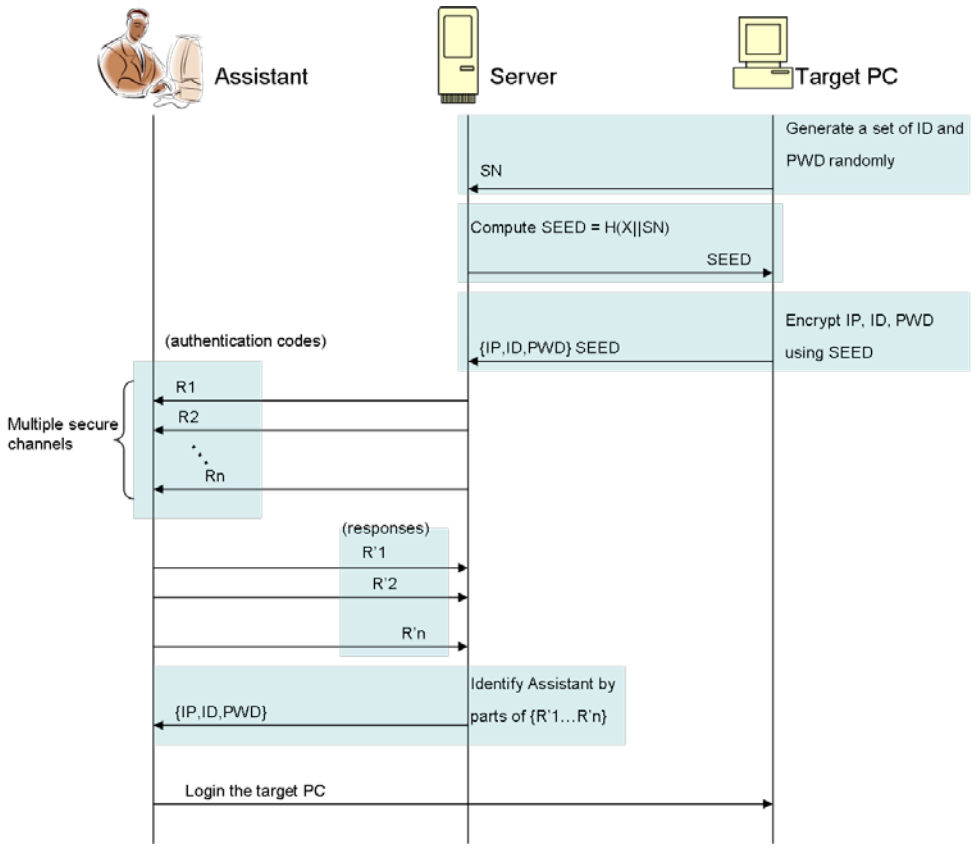

Fig.3. Personal authentication for remote assistance via multiple secure channels.

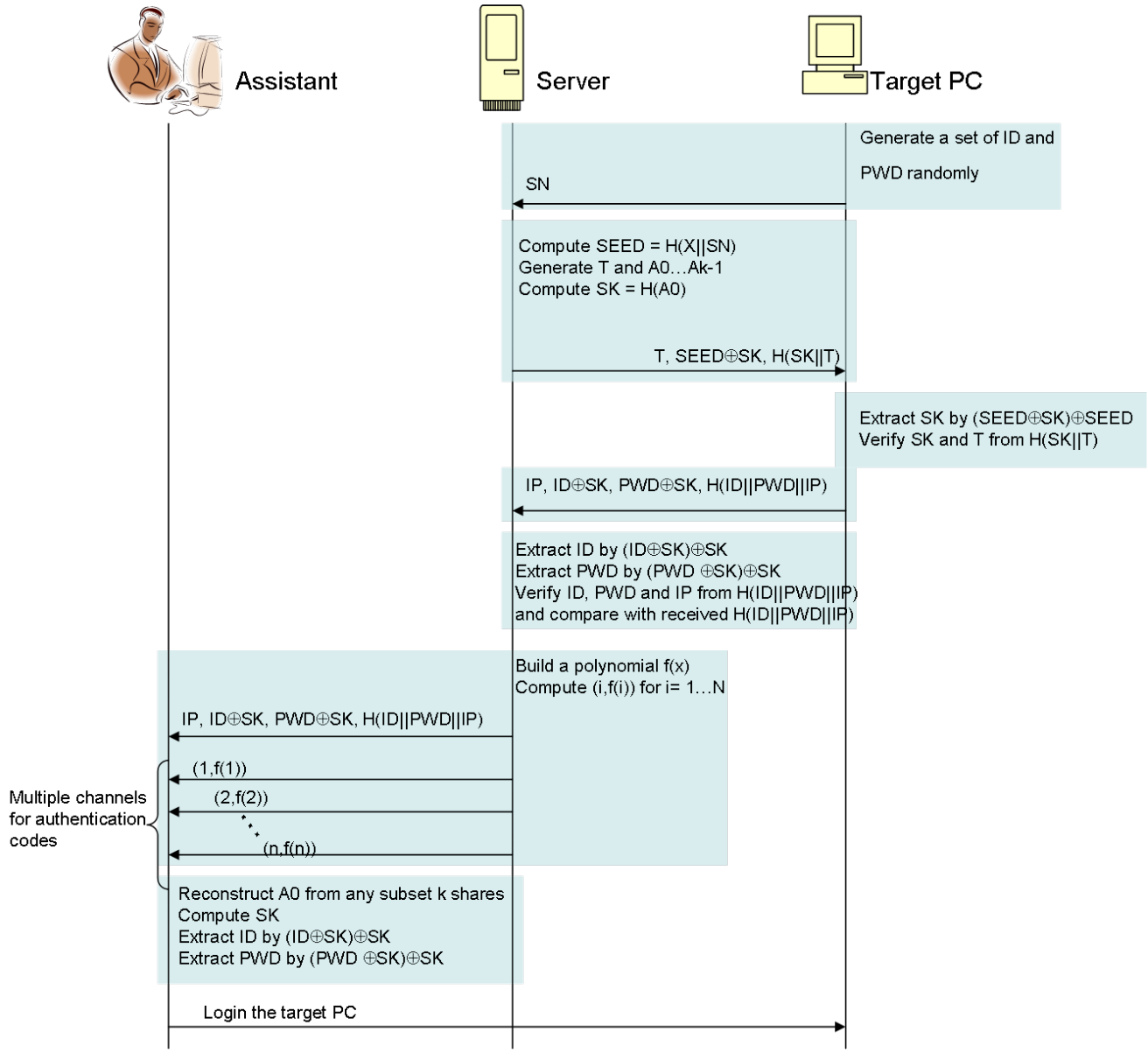

Fig.4. Personal authentication for remote assistance using secret sharing via multiple channels.