Study on the Transaction Linkage Technique Combining the Designated Terminal

Kyungroul Lee[1], Habin Yim[2], Insu Oh[3], and Kangbin Yim[3(✉)]

[1] R&BD Center for Security and Safety Industries (SSI), Soonchunyang University, Asan, South Korea
carpedm@sch.ac.kr
[2] Center for Information Security Technologies (CIST), Korea University, Seoul, South Korea
habinl03@korea.ac.kr
[3] Department of Information Security Engineering, Soonchunhyang University, Asan, South Korea
{catalyst32,yim}@sch.ac.kr

Abstract. While the scale of markets for Internet banking and e-commerce is growing, the number of financial markets using the Internet is increasing. However, there are a large number of hacking incidents against Internet banking services. For this reason, a countermeasure to improve the security of online identification is required. Security and authentication mechanisms applied to financial services such as Internet banking currently do not ensure security. In this paper, a transaction linkage technique combining a designated terminal is proposed to solve this fundamental problem, and the technique improves security for online identification mechanisms because it is possible to counteract all existing security threats. We consider that the security of Internet banking services will be enhanced by utilizing the proposed technique.

Keywords: Transaction linkage technique · Designated terminal
Internet banking service

1 Introduction

While the scale of markets for Internet banking and e-commerce is growing, the exchange of goods and services via the Internet has been established as a large part of the international economy. Although a variety of secure techniques is applied in the process of building these systems, hacking incidents on Internet banking services have occurred [1]. The damage resulting from such hacking and eavesdropping incidents on telebanking systems is continuous. In addition to general security applications, security techniques for online financial services are needed to ensure security requirements such as confidentiality, integrity, availability and non-repudiation [3]. Various cryptography-based mechanisms have been developed to satisfy these requirements over the past few decades [2], and their effectiveness was sufficiently verified by utilizing proven mathematical tools. Nevertheless, most security problems emerge during the process or in the environment of the security application rather than in the cryptography-based

J. J. Jung et al. (Eds.): BDTA 2017, LNICST 248, pp. 3–8, 2018.
https://doi.org/10.1007/978-3-319-98752-1_1

technology. Hence, we understand the need for studies that focus on research to find vulnerabilities other than the cryptography-based technology and to counteract these vulnerabilities properly.

Online identification methods do not ensure security owing to existing and new security threats against the identification methods previously mentioned. Hence, we propose a transaction linkage technique combining a designated terminal to solve the problem of exposure to threats on Internet banking services. In the case where existing transaction linkage techniques have been used, these techniques can solve exposure problems from security threats, which are analyzed in this paper. Nevertheless, the techniques ca be abused when the transaction linkage device is stolen; that is the biggest problem of possession-based identification methods, and the linkage code is exposed because the code is inputted by keyboard. In addition, the techniques do not satisfy mutual-authentication because they are authenticated one-way, and do not satisfy non-repudiation of financial institutions for a user because the transaction history is stored in the financial institutions. Therefore, we propose a new transaction linkage technique combining a designated terminal, that is an approved transaction-only designated terminal, to solve the above problems. The proposed technique deals with transaction-only designated terminal registered by the user. This technique counteracts when the device is stolen, supports non-repudiation by storing transaction history into the transaction linkage device, and provides mutual-authentication. Hence, the technique can counteract most existing security threats by applying the above functions; therefore, we consider that it improves the security of online identification methods for Internet banking services.

2 Related Works

The transaction linkage technique is shown in Fig. 1. When a user inputs transaction information such as account number, transfer amount, and so on into the transaction linkage device, the device displays the linkage code (verification code) generated based on the sharing key between the Internet banking server and the device. Next, the user inputs the displayed code into the web browser; then, the code is transferred to the Internet banking server.

The existing transaction linkage technique, however, can be abused when the device is stolen and the linkage code can be exposed because the code is inputted from the keyboard. Moreover, the server only authenticates the device as one-way authentication, not mutual authentication that authenticates between the server and the device; the technique does not support non-repudiation because the transaction history is only stored in the financial institutions.

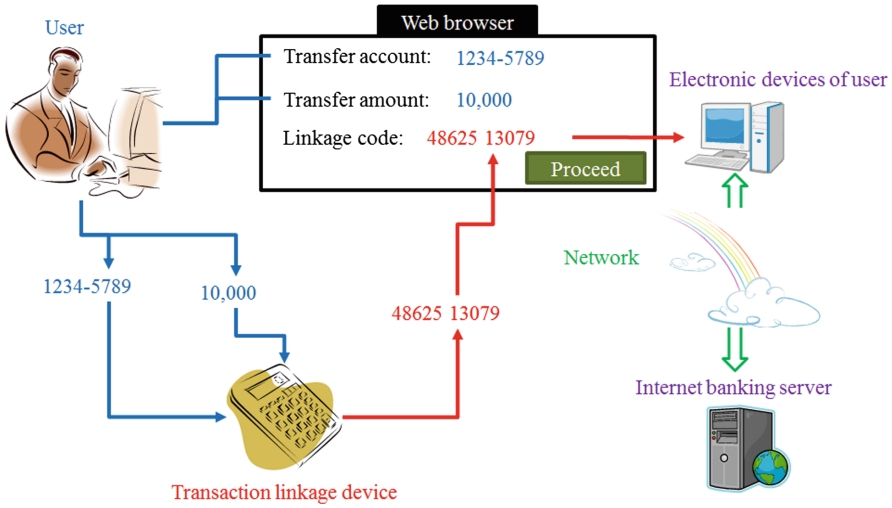

Fig. 1. Operational process of transaction linkage technique

3 Proposed Transaction Linkage Technique Combining a Designated Terminal

In this paper, we propose a transaction-linkage technique combined with a designated terminal to improve the security against the problems described above. The proposed technique is used only with a designated terminal; hence, the technique can counteract when the linkage device is stolen, and mutual authentication is provided between the server and the device. Moreover, a generated linkage code is transferred directly to the server, not inputted from the keyboard, and this technique provides non-repudiation by storing transaction history within the device. The operational process of the proposed technique is shown Fig. 2.

Stage 1. In the registration process, a user applies service of designated terminal device (SDTD) to the financial institutions and registers the hardware unique information (HWUI) of electronic devices that the user wants to register as transaction linkage devices.

Stage 2. After applying SDTD, the user identities himself or herself by offline authentication to visit the financial institutions directly, and he or she obtains the transaction linkage device after the offline authentication. The server and the transaction linkage device share a seed value for generating an encryption/decryption key, and time synchronization is applied in this stage.

Stage 3. The user begins the financial transaction by accessing financial transaction sites in the authentication process.

Stage 4. The user and financial institutions share a session key to establish a secure channel in the network communication.

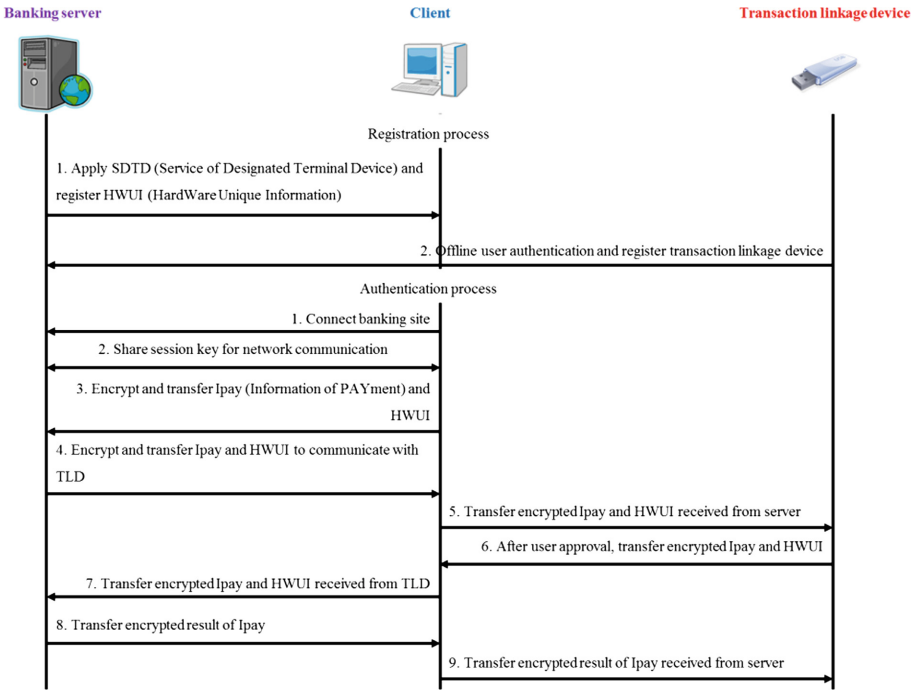

Fig. 2. The operational process of proposed technique

Stage 5. The user sends transfer information, which is encrypted inputted transaction information and hardware unique information of the designated device, to the server.

Stage 6. The server sends encrypted transaction information received and hardware unique information based on the shared encryption key between the server and the transaction linkage device to communicate with the device.

Stage 7. The user authenticates the server based on the received information, and then sends the encrypted transaction information and hardware unique information to the transaction linkage device.

Stage 8. The transaction linkage device displays an extra module such as a LCD (Liquid Crystal Display) panel for user recognition by decrypting the transaction information received, and the user approves the transaction after confirmation that the transaction information is correct. When the transaction is approved, the device sends encrypted transaction information and hardware unique information approved by the user to the server. If the transaction information is not correct, the transaction information mingled with random information is sent to the server in order to disrupt the communication process.

Stage 9. The user sends information received from the device directly to the server.

Stage 10. The server decrypts the transaction information received from the device and detects manipulation by comparing decrypted transaction information with received transaction information from the user. If the compared result is correct, this transaction is approved properly and the server sends the encrypted result, which is the processed transaction result.

Stage 11. The user sends the received transaction result to the transaction linkage device.

Stage 12. The transaction linkage device displays the received decrypted transaction result, and when the user finally confirms a transaction result, the transaction result is stored inside the device for non-repudiation

The server and transaction linkage device generate the encryption/decryption key based on a generated time stamp based on shared seed value and time synchronization. The generated key comprises a hash-chain type application based on time stamping to prevent encryption/decryption of transaction information and hardware unique information based on the same encryption/decryption key. Moreover, the session key for network communication in Stage 4 is changed in every session to prevent a replay attack, and a fixed password method, a one of the knowledge-based identity verification method, is applied to the transaction linkage device to improve transaction security. In addition, the transaction linkage device is flexible and can be applied to a variety of devices by communicating wirelessly or by a connector that can be inserted into the PC or mobile device. In terms of the safety of the proposed technique, the technique is safe from the debugging and reverse engineering attack because the transaction information is encrypted and decrypted in the server and the device inside by generating a key using a hash-chain type application based on shared seed value and time stamp. Therefore, the information is safe during sending and receiving processes between the network,

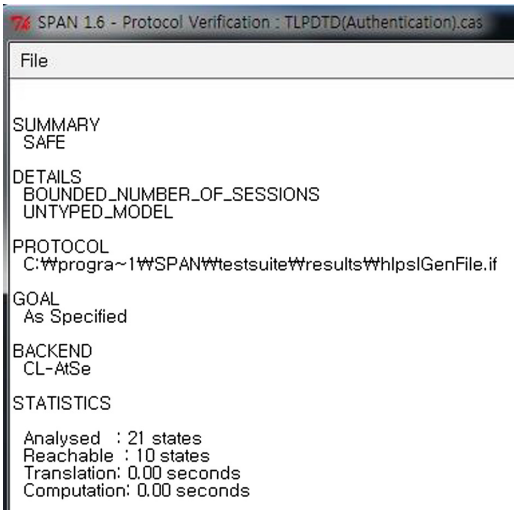

Fig. 3. Assessment result of security for proposed protocol by AVISPA

server, host, and the device. Moreover, a communication process between the host and the device is concealed, not exposed to the attacker; therefore, the proposed technique is safe. As the communication process has a one-sided transfer type, it is not a challenge-response structure.

In the security assessment [4, 5], we assess the security of the proposed protocol by the verification of satisfying security requirements using automated validation of internet security protocols and applications (AVISPA) as a formal verification tool. AVISPA assesses the security by deriving possible security threats. Figure 3 shows the verification result. As a result, in the SUMMARY, SAFE is displayed; this means that the proposed protocol is safe.

4 Conclusions

A designated PC service has been adopted to restrict the use of terminals by security threats of identity verification methods supported from the existing Internet banking service. Nevertheless, the designated PC service applied to a terminal using the service did not verify the security assessment and did not define the evaluation criteria; therefore, the service was exposed to security threats. To address this problem, the transaction linkage technique was proposed such that linkage code is generated by combining transaction information with secret information, but this technique was also exposed to various security threats. For these reasons, the current designated PC service and transaction linkage technique do not ensure security; therefore, we proposed a transaction linkage technique combining a designated terminal to solve these problems. The technique proposed in this paper can counteract and analyze all security threats; thus, the online identity verification method is also improved. We consider that the safety of Internet banking services can be enhanced by applying the proposed protocol.

Acknowledgements. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2015R1A6A3A01019717).

References

1. Hole, K.J., Moen, V., Tjostheim, T.: Case study: Online banking security. IEEE Secur. Priv. **4** (2), 14–20 (2006)
2. Baek, J., Newmarch, J., Safavi-Naini, R., Susilo, W.: A survey of identity-based cryptography. In: Proceedings of Australian UNIX Users Group Annual Conference, pp. 95–102, September 2004
3. Zhou, J., Gollmann, D.: Evidence and non-repudiation. J. Netw. Comput. Appl. **20**(3), 267–281 (1997)
4. Haley, C., Laney, R., Moffett, J., Nuseibeh, B.: Security requirements engineering: A framework for representation and analysis. IEEE Trans. Softw. Eng. **34**(1), 133–153 (2008)
5. Mirkovic, J., Dietrich, S., Dittrich, D., Reiher, P.: Internet Denial of Service: Attack and Defense Mechanisms. Radia Perlman Computer Networking and Security. Pearson Education, London (2004)