Three-factor user authentication method using biometrics challenge response

Haruhiko Fujii, Yukio Tsuruoka
Nippon Telegraph and Telephone Corporation
{fujii.haruhiko, tsuruoka.yukio}@lab.ntt.co.jp

Abstract: We propose a three-factor authentication method by pointing out the weakness in the two-factor authentication method that uses telephony currently used in Internet banking by adding voice verification, creating a three-authentication method (password, possession of phone, and voice printing) .
Keywords: multi-factor authentication, phone as a token, voice verification

The use of the two-factor authentication (two-path authentication) method using telephony has recently spread in terms of user authentication in electronic service applications, such as e-government, Internet banking, Amazon, Google, and Facebook. For example, Internet banking involves the following steps. Terminals such as PCs/smart phones send an ID and password a user enters into a server. The server checks the ID and password (knowledge factor), calls back the user's phone, which was registered beforehand, and finishes authentication when the user answers (possession factor). Since an attacker can remotely change the legitimate user's call-transfer setting to his/her telephone with only a stolen PIN, he/she can pretend to be the legitimate user; therefore, this system is not secure. In contrast, we have proposed a method with which users call the server and the server checks the caller's number (caller ID) [1]. Although this method solves the above-mentioned problem, the caller ID can still be changed in several countries, although not in Japan.

To solve this problem, we add voice verification to this method. The server asks the user a question, which is changed each time to prevent a replay attack in the audio line, receives a response, and uses voice recognition to check if the user has said the correct word, and conducts voiceprint recognition to check if the voice print matches the user. When all of these steps have been completed, user authentication (inherence factor) finishes successfully. This method enables a biometrics challenge response by using voice recognition and voice print recognition to prevent a replay attack. This feature is difficult to realize with other biometric methods such as face and fingerprint authentication. Even though another study argues that the crossover error rate of voiceprint authentication on public networks is 6.47% [2], our method is practical due to the use of multiple authentication factors (knowledge: password, possession: phone, and inherence: voice printing).

References

1. H. Fujii et al. "Telelogin: a two-factor two-path authentication Technique Using Caller ID," NTT Technical review, Vol. 6, No. 8, pp. 1-6 (2008).
2. N. Tsuchiya et al., "Speech Identification in VoIP (Voice over IP) System," Symposium on Mobile Interactions and Navigation, 2004/3/17-18. (2004)