Security vulnerabilities analysis of improved user authentication techniques for electronic medical record systems in aging society

G. Eom, H. Byeon, Y. Choi

Purpose The electronic medical record is the sets of individual patient health information stored in a digital format. This format can be shared across medical networks. This system enables the efficient transfer of medical records between institutions, patients and staff. The EMR contains personal health information; therefore, network access to patient-related data must be monitored and controlled to ensure that unlawful parties do not misuse personal information. Han et al. proposed several biometric-based authentication methods. However, Madhusudan et al. revealed that the biometric-based authentication method proposed by Han et al. had various weaknesses and proposed an authentication scheme with improved security suitable for the EMR system. In this paper, through a security analysis, we analyse the operation process of the scheme by Madhusudhan et al. and reveal problems, including H(B_i) recognition errors, no perfect forward secrecy, insider attacks (user identification guessing attacks), insider attacks (forgery attacks) and denial-of-service attacks. **Method** In Madhusudhan et al. scheme, a general hash function is used to use biometric information. If a general hash function is used, there is a problem that an error occurs even if biometric information is input slightly differently. The user enters biometric information in the login phase to log in to the server becomes the value of using for encryption. The login step proceeds only when the value is equal to, is, and is to input as Since is biometric information, it shows a little difference each time you enter a value. Since the combination of comes out differently depending on the input value, even if is input slightly differently, the value of may be output differently from the existing value. The fact that Perfect Forward Secrecy is satisfied means that even if one of the important master keys of the scheme is exposed, the previous session key cannot be found. However, in this scheme, if the value of one of the unchanging long-term keys, is exposed, not only the future session key but also the previously used session key can be found, which does not satisfy Perfect Forward Secrecy. And if the attacker acquires the user's smart card and knows the inside information, he can also find out the user's previous session key. **Results and Discussion** In this paper, after explaining the operation process of the authentication scheme with improved security for the EMR proposed by Madhusudhan et al., a security analysis was conducted. The scheme proposed by Madhusudhan et al. has security problems, such as H(B_i) recognition errors, no perfect forward secrecy, insider attacks (user identification guessing attacks and forgery attacks), and DoS attacks.

Keywords: electronic medical record, security vulnerabilities analysis
Address: Inje University, Republic of Korea
Email: bhwpuma@naver.com

Acknowledgement: The National Research Foundation of Korea (NRF) funded by the Ministry of Education, grant number “2018R1D1A1B07041091, 2021S1A5A8062526”, and “2022 Development of Open-Lab based on 4P in the Southeast Zone”