Security vulnerability analysis for an improved anonymous authentication protocol for wearable health monitoring system in an aging society

G. Eom, H. Byeon, Y. Choi

Purpose The wearable health monitoring system (WHMS) plays a significant role in medical experts collecting and using patient medical data. The WHMS is becoming more popular than in the past through mobile devices due to meaningful progress in wireless sensor networks. However, because the data about health used by the WHMS is related to privacy, it has to be protected from malicious access when wirelessly transmitted. Jiang et al. proposed a two-factor suitable for WHMSs using a fuzzy verifier. However, Jiaqing Mo et al. revealed that the protocol proposed by Jiang et al. had various security vulnerabilities and proposed an authentication protocol with improved security and guaranteed anonymity for WHMSs. In this paper, we analyse the authentication protocol proposed by Jiaqing Mo et al. and determine problems with the offline identification, password guessing attacks, operation process bit mismatch, no perfect forward secrecy, no mutual authentication and insider attacks. **Method** This paper analyzed the operation process of Jiang et al.'s protocol and found various vulnerability as off-line ID, PW guessing attack, operation process bit mismatch, no perfect forward secrecy, no mutual authentication and insider attack. According to Jiaqing Mo et al.'s proposed protocol, when an adversary acquires a MD, the adversary can extract information stored in the MD and then find out the user's ID and PW. The information of {Reg_i, A_i, C_i, m, n, h()} is sent to the MD through the GWN security channel. Thereafter, the MD calculates and updates A_i^*=A_i⊕h(ID_i‖r_i) and D_i=r_i⊕h(h(ID_i‖PW_i) mod m). Finally, information of {Reg_i, A_i^*, C_i, D_i, m, n, h()} is stored in the MD. Assuming that an adversary found out this through a physical analysis method, an ID and password can be derived through the formula of 〖Reg_i〗 ^*=h(h(ID_i‖R_i^*‖HPW_i^*) mod m).

$$
\begin{aligned}
\mathrm{Reg}_i{}^* &= h(h(\mathrm{ID}_i \parallel R_i^* \parallel \mathrm{HPW}_i^*) \bmod m) \\
&= h(h(\mathrm{ID}_i \parallel A_i \oplus \mathrm{HPW}_i{}^* \parallel h(r_i \oplus \mathrm{PW}_i)) \bmod m) \\
&= h(h(\mathrm{ID}_i \parallel A_i^* \oplus h(\mathrm{ID}_i \parallel r_i), \oplus \mathrm{HPW}_i{}^* \parallel h(r_i \oplus \mathrm{PW}_i)) \bmod m) \\
&= h(h(\mathrm{ID}_i \parallel A_i^* \oplus h(\mathrm{ID}_i \parallel D_i \oplus h(h(\mathrm{ID}_i \parallel \mathrm{PW}_i) \bmod m)) \oplus h(r_i \oplus \mathrm{PW}_i) \parallel h(r_i \oplus \mathrm{PW}_i)) \bmod m) \\
&= h(h(\mathrm{ID}_i \parallel A_i^* \oplus h(\mathrm{ID}_i \parallel D_i \oplus h(h(\mathrm{ID}_i \parallel \mathrm{PW}_i) \bmod m)) \oplus h(D_i \oplus h(h(\mathrm{ID}_i \parallel \mathrm{PW}_i) \bmod m) \oplus \mathrm{PW}_i) \\
&\qquad\qquad \parallel h(D_i \oplus h(h(\mathrm{ID}_i \parallel \mathrm{PW}_i) \bmod m) \oplus \mathrm{PW}_i)) \bmod m)
\end{aligned}
$$

Summarizing the above formula, the adversary will be aware of the information {A_i*, D_i, m, h()} except for the ID and PW. The adversary repeatedly performs verification while continuing to change until the user's ID and PW are found. Ultimately, the user's exact ID and PW can be found. **Results and Discussion** In this paper, a security analysis was conducted after explaining the operation process of an authentication protocol with improved security and guaranteed anonymity for the WHMS proposed by Jiaqing Mo et al. The protocols proposed by Jiaqing Mo et al. have vulnerabilities in offline identification, password guessing attacks, operation process bit mismatch, no perfect forward secrecy, no mutual authentication and insider attack problems.

Keywords: wearable health monitoring system, fuzzy verifier, place, authentication protocol, Security vulnerability analysis

Address: Inje University, Republic of Korea
Email: bhwpuma@naver.com

Acknowledgement: This research was funded by Basic Science Research Program through 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”.