

그림 1. 인증 단계.

2.3 Rahaman 등이 제안한 프로토콜의 보안 취약점

본 논문에서는 비정형 보안 분석을 통해 Rahaman 등이 제안한 인증 프로토콜의 취약점을 보인다. Rahaman 등이 제안한 프로토콜은 사용자 사칭 공격, 내부자 공격, 임시 키 유출 공격에 취약하고, 사용자의 추적 가능성을 보장하지 않음을 증명한다.

2.3.1 사용자 사칭 공격

공격자는 사용자의 모바일 기기를 탈취하여 power analysis attack을 통해 기기에 저장된 $\{UID_i, Uinf_i, Encpw, H(*), H(S_k)\}$ 를 획득한다. 공격자는 인증 요청 메시지를 만드는 데에 필요한 값인 $\{Uinf_i, H(S_k)\}$ 를 알게 되므로, 공격자의 난수 n_A 와 타임스탬프 t_A 를 생성하고, 인증 요청 메시지 $\{C_A, VerU_A, t_A, UID_i\}$ 를 생성하여 센서에게 전송할 수 있다. 인증 단계에서 센서와 중앙 서버는 공격자를 합법적인 사용자로 판단하고 인증을 진행하게 된다. 따라서 Rahaman 등의 프로토콜은 사용자 사칭 공격을 방어하지 못한다.

2.3.2 내부자 공격

공격자는 서버에 합법적인 사용자로 등록하여 인증을 수행할 수 있다고 가정한다. 등록 후 공격자는 중앙 서버 마스터키의 해시값 $H(S_k)$ 을 획득하게 된다. $H(S_k)$ 은 중앙 서버에 등록하는 모든 사용자가 공통으로 가지게 되므로, 공격자는 이 값을 활용하여 다른 사용자의 세션 키를 계산할 수 있다. 공격자는 공개 채널을 통해 전송되는 C_i 를 가로채 $H(C_i||H(S_k))$ 를 계산할 수 있다. 그 후 UID_i, L_i 를 통해 세 개의 난수 n_{i1}, n_{i2}, n_{i3} 를 얻을 수 있고, 따라서 공격자는 다른 사용자가 공유하는 세션키 $SK = H(C_i||H(S_k)) \oplus H(n_{i1} \oplus n_{i2} \oplus n_{i3})$ 를 계산할 수 있다.

2.3.3 임시 키 유출 공격

세션 상의 임시 비밀 값인 세 개의 난수 $\{n_{i1}, n_{i2}, n_{i3}\}$ 가 유출된다면, 공격자는 세션키를 계산할 수 있다. 공격자는 중앙서버가 센서에게 전송하는 메시지인 $\{E_i, F_i, L_i, t_s\}$ 를 가로챈다. 공격자는 n_{i1}, n_{i3}, E_i 를 통해 $H(SID_j \oplus n_{i2})$ 를 알아내고, 이 값과 F_i 를 통해 $H(C_i||H(S_k))$ 를 알아낼 수 있다. 그 후 유출된 세 개의 난수와 알아낸 값을 통해 세션키 $SK = H(C_i||H(S_k)) \oplus H(n_{i1} \oplus n_{i2} \oplus n_{i3})$ 를 계산할 수 있다.

2.3.4 사용자의 불추적성

Rahaman 등의 프로토콜에서 사용자는 임시 아이디인 UID_i 를 사용한다. 이 임시 아이디는 인증 단계에서 공개 채널로 전송된다. 하지만 인증 단계에서 사용자의 임시 아이디를 업데이트하지 않기 때문에, 공격자는 사용자의 연속적인 인증을 추적할 수 있게 된다. 따라서 Rahaman 등의 프로토콜은 사용자의 불추적성을 보장하지 못한다.

2.4 대응 방안

Rahaman 등이 제안한 프로토콜은 사용자 사칭 공격, 내부자 공격, 임시 키 유출 공격에 취약하며 사용자 불추적성을 보장하지 않는다. Rahaman 등의 프로토콜에서는 사용자의 모바일 기기가 도난당할 경우 공격자가 사용자를 사칭할 수 있을 뿐만 아니라 세션 키를 계산할 수 있게 된다. 이는 사용자가 인증에 필요한 파라미터를 저장하는 데에 사용한 비밀 값이 부족했음을 나타낸다. 따라서 등록 단계에서 사용자는 난수를 생성하여 해시 함수를 사용함으로써 인증 파라미터의 보안성을 높일 필요가 있다. 또

한 세션 키를 계산할 때 사용되는 SID_j, C_i 는 공개 채널을 통해 얻을 수 있는 값이다. 따라서 세션 키를 사용할 때 공개 채널로 전송되는 값의 사용을 줄이고, 센서와 사용자만이 알 수 있는 값으로 계산한다. 사용자의 불추적성을 보장하기 위해, 인증 단계의 마지막에 사용자의 임시 아이디를 업데이트하는 과정 또한 필요하다.

III. 결론

본 논문에서는 Rahaman 등이 제안한 스마트 파밍 환경에서 사용자, 센서, 중앙 서버 간의 인증 프로토콜을 분석하였다. 보안 분석을 통해 Rahaman 등이 프로토콜이 사용자 사칭 공격, 임시 키 유출 공격에 취약하고, 사용자 불추적성을 보장하지 못한다는 것을 입증하였다. 이러한 취약점을 보완하기 위해 난수와 해시값을 사용해 사전에 공유한 파라미터를 안전하게 저장함으로써 세션 키의 보안성을 높일 수 있었다. 본 논문에서 제시한 대응 방안을 통해 IoT 기반 스마트 파밍 환경에서 사용자와 센서 간의 세션 키 공유를 위한 구체적인 인증 프로토콜을 제안할 수 있다.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. RS-2024-00396797, Development of core technology for intelligent O-RAN security platform)

참 고 문 헌

- [1] Farooq, M. S., Riaz, S., Abid, A., Abid, K., and Naeem, M. A. "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming," *Ieee Access*, pp. 156237-156271. Oct. 2019
- [2] Son, S., Park, Y., and Park, Y. "A secure, lightweight, and anonymous user authentication protocol for IoT environments," *Sustainability*, pp. 9241. Aug. 2021
- [3] Yu, S., Jho, N., and Park, Y. "Lightweight three-factor-based privacy-preserving authentication scheme for iot-enabled smart home," *IEEE Access*, pp. 126186-126197. Sep. 2021
- [4] Kwon, D. K., Yu, S. J., Lee, J. Y., Son, S. H., and Park, Y. H. "WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor network," *Sensors*, pp. 936. Jan. 2021
- [5] Rahaman, M., Lin, C. Y., Pappachan, P., Gupta, B. B., and Hsu, C. H. "Privacy-centric AI and IoT solutions for smart rural farm monitoring and contro," *Sensors*, pp. 4157. Jun. 2024