IoT 환경에서 양자 내성 암호 기반 인증 프로토콜 보안 분석 및 해결 방안

이준영, 유성진, 김태성, 정보흥, 김건우

한국전자통신연구원

ljy@etri.re.kr, sj.yu@etri.re.kr, taesung@etri.re.kr, bhjung@etri.re.kr, wootopian@etri.re.kr

Security Analysis and Countermeasure of Post Quantum based Authentication Protocol in IoT Environment

Lee JoonYoung, Yu SungJin, Kim TaeSung, Chung BoHeung, Kim KewonWoo

Electronics and Telecommunications Research Institute

요 약

최근 양자컴퓨팅에 관한 기술 개발이 발전함에 따라 기존 암호의 취약점을 보안한 양자 내성 암호를 이용한 보안 연구가 진행되고 있다. 또한 IoT 환경에서는 데이터의 안전한 송·수신을 위해 인증 프로토콜의 연구가 필요하다. 2022년 Alawi 등은 IoT 환경에서 양자 내성 암호 기반 인증 프로토콜을 제안하였다. Alawi 등은 제안하는 프로토콜이 양자 컴퓨팅에 대한 내성을 가지며 이와 동시에 내부자 공격, 스마트 카드 도난 공격 및 중간자 공격에 안전하다고 주장하였다. 본 논문에서는 Alawi 등이 제안한 프로토콜이 스마트 카드 도난 공격 및 서버 위장 공격에 취약함을 분석하고 이에 대한 해결 방안을 제시한다.

Ⅰ. 서 론

최근 양자 컴퓨팅의 기술 발전이 급속도로 이루어짐에 따라 기존 암호인 RAS 및 AES 등의 암호 알고리즘들은 보안에 취약해질 것으로 전망하고 있다. 이에 따라 양자 컴퓨팅 기술에도 보안성을 가질 수 있는 양자 내성 암호 기술 개발이 활발히 이루어지고 있다 [1]. IoT 환경에서는 무선 채널을 통해 데이터 등을 실시간으로 수집 및 공유되고 있으나 공개 채널을 통한 데이터 송·수신은 다양한 공격에 취약하다 [2,3]. 이러한 문제점들을 해결하기 위해 양자 내성 암호 및 인증 기술을 활용하여 보안 프로토콜 연구가 활발히 진행되고 있다.

2022년 Alawi 등은 [4] IoT 환경에서 환자의 정보를 수집 및 공유하기 위하여 양자 내성 암호를 이용한 인증 프로토콜을 제안하였다. Alawi 등은 제안하는 프로토콜이 양자 내성을 가지며 스마트 카드 도난 공격, 내부자 공격 및 중간자 공격 등에 안전하다고 주장하였다. 그러나 본 논문에서는 Alawi 등이 제안한 프로토콜이 스마트 카드 도난 공격 및 서버 위장 공격 등에 취약함을 보임을 증명한다. 또한 본 논문에서는 보안 취약점을 개선하기 위한 대응 방안을 제시한다.

Ⅱ. 본론

본 장에서는 Alawi 등이 제안한 인증 프로토콜에 대해 간략히 소개하며 보안 취약점을 분석한다.

2.1 Alawi 등의 인증 프로토콜

IoT 환경에서 헬스케어 시스템을 위해 Alawi 등이 제안한 인증 프로토콜은 간략하게 등록 단계, 로그인 및 인증 단계 및 생체정보 폐지 단계로 이루어진다. 먼저 초기화 단계에서 의료 서버 (MS)는 소수 p와 두 개의 양수 m과 n을 생성한다. 그 후, MS는 매트릭스 $A \in Z_p^{m \times n}$를 생성하며 해시 함수 $h: 0,1^* \rightarrow 0,1^k$를 생성한다. MS는 마스터 키 벡터 $mk \in Z_p^{1 \times n}$와 공개키 $pk = A.mk^T (\mathrm{mod}\, p) \in Z_p^{1 \times m}$를 계산하여 공개 파라미터 $m, n, p, A, pk, h(\bullet)$를 배포한다.

2.1.1 사용자 등록 단계

사용자 등록 단계에서 사용자는 의료 서버에 자신의 정보를 등록하며 스마트 카드를 전달 받는다. 등록 단계의 상세 절차는 그림 1과 같다.

User Registration Phase	
User (U_i)	Medical Server (MS)
Selects unique identity ID_i	
Generates cryptographic key $k_i \in Z_2^l$	
random number N	
Computes $c_i = h(k_i \| N)$	
Inputs a biometric data B_i	
Biometric reference template extracts $x_r \in Z_2^t$	
,where $m = t + l$	
Computes $\beta_r = A \times_q v_i +_{q,2} (x_r \| k_i)$	
$r_i = h(c_i \| \beta_i)$, $w_I = A \times_q v_i$,	
$Z_i = w_i \times_q pk^T$, $\delta_i = h(w_i) \oplus h(ID_i \| r_i)$.	Computes $e_i = h(ID_i \| mk) \oplus r_i$
$\langle ID_i, r_i, Z_i, \delta_i \rangle \rightarrow$	Stores $\{s, e_i, \delta_i, Z_i, r_i\}$
	$\leftarrow \langle Smartcard \rangle$
Stores N and β_r in the smart card	

그림 1. 사용자 등록 단계

2.1.2 로그인 및 인증 단계

사용자는 환자의 건강 정보를 얻기 위해 MS에 로그인하며 MS와 사용자는 안전한 통신을 위하여 인증을 수행하며 이를 통해 세션키를 계산한다. Alawi 등이 제안한 인증 프로토콜의 로그인 및 인증 단계는 그림 2와 같다.

2.2 Alawi 등의 인증 프로토콜의 보안 취약점 분석

본 논문에서는 Alawi 등이 제안한 인증 프로토콜의 보안 분석을 위하여 공격자가 무선 채널로 송·수신되는 메시지를 도청하여 삽입, 삭제 및 수정 등을 할 수 있는 가정을 지닌 Dolev-Yao (DY) 모델을 [5] 이용하여

분석한다. 이에 따라 본 논문에서는 Alawi 등이 제안한 프로토콜이 스마트 카드 도난 공격 및 서버 위장 공격에 취약함을 분석하고 이에 대한 해결 방안을 제시한다.

Login and Authentication Phase	
User (U_i)	Medical Server (MS)
Inserts his/her smart card, keys and ID_i smart card sends the login request message $\{r_i, Z_i, \delta_i\}$ →	
	Computes $w_i' = (Z_i \cdot A) \cdot mk^T (modp)$ $\{w_i'\}$ ←
Presents his/her biomertics B_i	
Extracts biometric template x_q Computes $\beta_q = w_i' +_{q,2} (x_q \| 0)$ and Verifies $dist(\beta_q, \beta_r) \leq d_{th}$ If it corrects, extracts $k_i' = \beta_r \oplus \beta_q$ Computes $r_i' = h(h(k_i' \| N) \| \beta_q)$ verifies $r_i = r_i'$	
If it corrects, computes $\theta_1 = e_i \oplus r_i'$	Computes $\theta_7 = \theta_1 \oplus \theta_1$
$\theta_2 = \theta_1 \oplus R_u$, $\theta_3 = h(s \| R_u)$	$ID_i' = \theta_6 \oplus h(s \| \theta_1 \oplus \theta_2)$
$\theta_4 = c_i \oplus \theta_3$, $\theta_5 = h(\theta_2 \| \theta_3 \| \theta_4)$	Checks the format ID_i', If it is valid
$\theta_6 = \theta_3 \oplus ID_i$	Computes $\theta_8 = h(s \| \theta_1 \oplus \theta_2)$
$\{\theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6\}$ →	$\theta_5' = h(\theta_2 \| \theta_8 \| \theta_4)$
	Checks $\theta_5' = \theta_5$. If it corrects, Stores ID_i, θ_7 in the server Computes $\theta_9 = \theta_4 \oplus \theta_8$ $\theta_{10} = h(\theta_9 \| ID_s \| s) \oplus \theta_8 \oplus R_s$
Computes $\theta_{12} = h(c_i \| ID_s \| s) \oplus R_u$	$\theta_{11} = h(\theta_1 \| \theta_9 \| s \| R_s)$
$\theta_{11}' = h(\theta_1 \| c_i \| s \| \theta_{12})$	$\{\theta_{10}, \theta_{11}\}$ ←
Checks $\theta_{11}' = \theta_{11}$. If it valids, Computes $SK_{sess} = h(c_i \| \theta_3 \| \theta_{12} \| ID_s)$	Computes $SK_{sess} = h(\theta_9 \| \theta_8 \| R_s \| ID_s)$

그림 2. 로그인 및 인증 단계

2.2.1 스마트 카드 도난 공격

DY 모델에 따라 로그인 및 인증 단계에서 공개 채널로 송·수신되는 메시지들을 도청하여도 공격자는 세션 키를 계산할 수 없어야만 한다. 그러나 Alawi 등이 제안한 프로토콜에서 스마트 카드 도난 공격을 통해 스마트 카드에 저장된 값과 공개 채널로 전송되는 메시지들을 도청하여 얻은 값들을 이용하면 아래와 같은 단계를 통하여 세션 키를 계산할 수 있다.

• 1단계 : 공격자는 사용자의 스마트 카드 도난 공격을 통해 스마트 카드에 저장된 $\{N, \beta_r, s, e_i, \delta_i, Z_i, r_i\}$ 값을 획득할 수 있으며 공개 채널을 통해 송신하는 메시지 $\{\theta_1, \theta_2, \theta_4, \theta_5, \theta_6\}$ 값을 획득할 수 있다.

• 2단계 : 공격자는 획득한 값을 통해 $R_u = \theta_1 \oplus \theta_2$, $\theta_3 = h(s \| R_u)$ $= \theta_8$, $c_i = \theta_4 \oplus \theta_3$ 및 $\theta_{12} = h(c_i \| ID_s \| s) \oplus R_u$ 값을 계산할 수 있다.

• 3단계 : 따라서 공격자는 인증 단계에서 세션 키인 $SK_{sess} = h(c_i \| \theta_3 \| \theta_{12} \| ID_s)$를 계산할 수 있다.

따라서 Alawi 등이 제안한 인증 프로토콜은 스마트 카드 도난 공격에 취약하며 세션 키의 안전성을 보장할 수 없다.

2.2.2. 의료 서버 위장 공격

공격자는 스마트 카드 도난 공격을 이용하여 의료 서버를 위장한 공격 역시 가능하다. Alawi 등의 인증 프로토콜에서 공격자는 인증 단계에서 다음과 같은 단계를 통하여 의료 서버로 위장할 수 있다.

• 1단계 : 공격자는 스마트 카드 도난 공격 및 탈취한 메시지 값을 통해 $R_u = \theta_1 \oplus \theta_2$, $\theta_8 = h(s \| R_u)$ 및 $\theta_9 = \theta_4 \oplus \theta_8$를 계산할 수 있다.

• 2단계 : 공격자는 랜덤 넘버 R_A를 생성하여 $\theta_{10A} = h(\theta_9 \| ID_s \| s)$ $\oplus \theta_8 \oplus R_A$ 및 $\theta_{11A} = h(\theta_1 \| c_i \| s \| R_A)$를 계산하여 사용자에게 $\{\theta_{10A}, \theta_{11A}\}$를 전송하여 서버로 위장할 수 있다.

Ⅲ. 해결 방안

Alawi 등의 인증 프로토콜은 스마트 카드 도난 공격 및 의료 서버 위장 공격에 취약하며 세션 키의 안전성을 보장할 수 없다. 따라서 사용자의 안전한 서비스 제공 및 세션 키의 안전성을 보장하기 위하여 다음과 같은 해결 방안을 제시한다.

• Alawi 등이 제안하는 인증 프로토콜에서 전송되는 메시지는 단순한 XOR 계산을 통해 생성되므로 공격에 취약하다. 이를 방지 하기 위해서 전송되는 메시지 값에 장기 비밀 키를 생성하고 이를 사용하여 메시지를 암호화하여 메시지의 안전성을 보장하여야 한다.

• 공격자가 스마트 카드를 도난하여 스마트 카드 값에 저장되어 있는 값을 획득하더라도 세션 키를 계산할 수 없도록 장기 비밀 키 값 및 새로운 랜덤 넘버를 XOR 및 hash 연산을 하여 세션키를 생성하여야 한다.

Ⅳ. 결론

본 논문에서 Alawi 등의 IoT 환경을 위한 인증 프로토콜이 스마트 카드 도난 공격 및 서버 위장 공격 등에 취약하며 이를 통해 세션 키의 안전성이 보장 받지 못함을 증명하였다. 이와 같은 보안 취약점들을 해결하기 위하여 세션 키 및 전송되는 메시지에 장기 비밀 키 및 랜덤 넘버 값을 추가하여 계산하는 해결 방안을 제시하였다. 따라서 공격자는 세션 키를 계산할 수 없다. 따라서 제안하는 해결 방안을 통해 보안 공격에 안전함을 보임과 동시에 양자 내성 암호를 활용하여 안전한 프로토콜을 설계할 수 있다. 위와 같은 해결 방안을 통해 IoT 환경에서 양자 내성 암호 기반 인증 프로토콜을 설계한다면 실제 IoT 환경에 적응하여 안전한 IoT 데이터 수집 및 공유가 가능할 것이다.

ACKNOWLEDGMENT

This research was supported by the Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by the Korean government (MSIT) (No. 2022-0-01019, Development of eSIM security platform technology for edge devices to expand the eSIM ecosystem)

참 고 문 헌

[1] Shor P. W. “Polynomial time algorithms for discrete logarithms and factoring on a quantum computer,” In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformactics), 1994.

[2] Yu S. and Park K., “Puf-based robust and anonymous authentication and key establishment scheme for v2g networks,” IEEE Internet of Things Journal, vol. 11, no. 9, pp. 15450-15464 2024.

[3] Lee, J., Oh, J., Kwon, D., Kim, M., Kim, K., and Park, Y. “Blockchain-enabled key aggregate searchable encryption scheme for personal health record sharing with multi-delegation,” IEEE Internet of Things Journal, early access, 2024.

[4] Al-Saggaf, A. A., Sheltami, T., Alkhzaimi, H., and Ahmed, G. “Lightweight two-factor-based user authentication protocol for iot-enabled healthcare ecosystem in quantum computing,” Arabian Journal for Science and Engineering, vol. 48, no. 2, pp. 2347-2357, 2022.

[5] Dolev V., and Yao A. C. “On the security of public key protocols,” IEEE Trans. Inf. Theory vol. 29, pp. 198-208, 1983.