IoT 환경에서 물리적 복제 방지 기술 기반 인증 프로토콜 취약점 분석 및 개선방안 제안1)

최재현*, 정익래*, 변진욱**
*고려대학교 정보보호대학원 정보보호학과
**평택대학교 정보통신학과
93jamie@korea.ac.kr, irjeong@korea.ac.kr, jwbyun@ptu.ac.kr

A proposal of countermeasure and security analysis on the PUF based authentication protocol in IoT network

Jae Hyun Choi*, Ik Rae Jeong*, Jin Wook Byun**
*Graduate School of Information Security, Korea University
**Dept. of Information and Communication, Pyeongtaek University

요 약

사물인터넷의 사용이 급격히 증가함에 따라 관련 보안 기술의 개발이 매우 중요하게 되었다. 사물인터넷이 지니는 근본적인 자원 제한 요소 환경을 극복하기 위해, 최근 Chatterjee 기타 등은 경량화된 질의 응답 기반의 PUF를 활용한 인증 프로토콜을 최근 IEEE Transactions on Dependable and Secure Computing 저널에 제안하였다. 그러나 장치 간 세션 키를 주고받는 과정에서 공개된 채널에서 값을 한번 획득한 공격자는 누구나 세션 키를 만들 수 있는 치명적인 취약점이 존재한다. 본 논문에서는 이러한 취약점을 설명하고 정당한 장치만 세션 키를 만들 수 있는 방법을 제시한다.

1. 서론

최근 사물인터넷(IoT)의 활용도와 접근성이 증가함에 따라 IoT 기기들은 일상생활에서 다양한 영역에서 사용되고 있다. IoT 환경에서 보안 프로토콜을 설계할 때 가장 큰 이슈는 낮은 계산 능력과 적은 메모리를 고려하여 인증 및 보안 프로토콜을 설계해야 한다는 점이다. 이로 인해, 물리적인 복제 기능을 갖춘 PUF(Physical Unclonable Function) 기술에 주목하게 되었다. PUF는 제조 시 동일한 과정을 거치더라도 반도체의 미세한 구조 차이를 이용하여 물리적으로 복제 불가능한 기능으로 보안키를 생성하는 기술이다. 마치 사람의 지문과 같이 장치의 고유한 정보를 갖고 있고, 이 고유한 값은 외부로 유출되지 않는 특징을 갖고 있다[1]. PUF를 사용하면 질의 응답 기반의 경량화된 인증 설계가 가능하여 IoT 장비의 보안 요구사항에 대한 부담을 줄일 수 있다[2][3][4].

2018년에 Chatterjee 기타 등[5]은 IoT 환경에서 PUF를 사용하여 장치 간 비밀 통신을 위한 프로토콜을 제시했다. 그런데 세션 키를 생성하는데 사용될 값을 공유할 때, 정당하지 않은 장치가 임의의 값으로 세션키를 형성할 때 필요한 값을 만들 수 있는 문제점이 존재한다. 본 논문에서는 Chatterjee 기타 등에서 장치 간 세션 키 형성에 있어서 정당한 장치임을 인증하는 개선방안을 제안한다.

1) 이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. 2017R1D1A1B03032424)

2. 암호 프리미티브

• 타원 곡선 암호 (Elliptic Curve Cryptography)

공개키 암호 시스템으로 타원 곡선 이론에 기반한 이론이다. 타원 곡선은 유한체 $E: y^2 = x^3 + ax + b$ 상의 정수로 이뤄진 점들의 집합이다. 타원 곡선에서의 곱셈은 타원곡선 상에서의 정의된 덧셈 연산의 반복 수행하는 것이다.

• Bilinear paring operation

큰 소수 q에 대해 타원 곡선과 군 G_1, G_2, G_3가 있다. Bilinear paring operation은 bilinear map $e : G_1 \times G_2 \rightarrow G_3$ 이고 다음을 만족한다.

(1) Bilinearity : $\forall a, b \in F_q^*, \forall PING_1, \forall Q \in G_2$: $e(aP, bQ) = e(P, Q)^{ab}$.

(2) Non-degeneracy : $e(P,Q) \neq 1$.

(3) Computability : e를 계산하는데 효율적인 알고리즘이 존재한다.

• Elliptic curve discrete logarithm problem

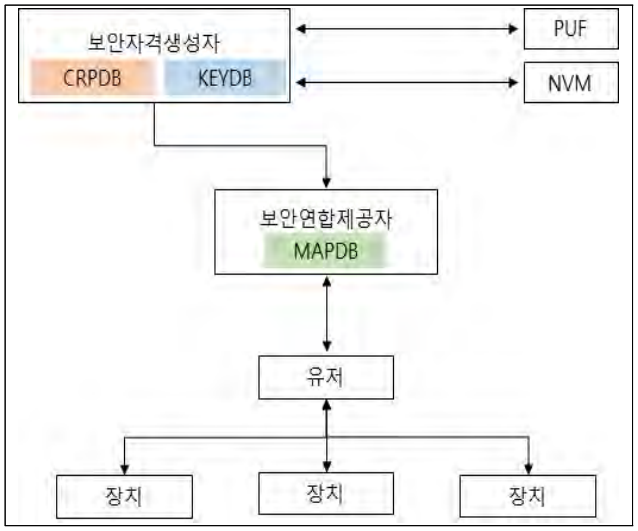
타원곡선 위의 점 P와 생성원 Q가 존재할 때, $P = t \cdot Q$를 만족하는 스칼라 t를 다항 시간 내에 구하는 것은 어렵다.

3. Chatterjee 기타 등의 프로토콜 분석

인증프로토콜은 일반적으로 등록 단계와 인증 및 키 교환 단계로 나뉜다. 등록단계는 안전한 채널을 가정하고 인증 및 키교환 단계는 공개된 채널에서 수행됨을 가정한다. 전체적인 프로토콜에서 사용되는 표기와 그에 대한 설명은 <표 1>, 시스템 구조는 <그림 1>에서 정리하였다. <그림 2>, <그림 3>는 Chatterjee 기타 등[5]의 프로토콜을 직접 이미지화 시켜서 표현한 것이다.

표기	설명
C_A, R_A	PUF의 질의, 응답 값
HLP_A	PUF값의 헬퍼데이터
C_S, K_S	유저의 질의 값, 비밀 값
H_1, H_2, H_3	암호학적으로 안전한 해시 함수단, H_2는 키를 이용한 해시 함수
e	타원곡선 paring 연산
BCH_{Enc}, BCH_{Dec}	헬퍼데이터 값을 위한 인,디코딩
a, x, t	임의의 수
KA_{PUB}, KA_{PRV}	장치 간 사용되는 A의 공개,개인키

<표 1> 표기 및 설명에 대한 소개



<그림 1> 시스템 구조

1) 등록 단계

• 보안 자격 생성자는 IoT 장치 A에 PUF 입력값에 해당하는 질의 값 C_A를 전송하고 장치 A는 $R_A = PUF_A(C_A)$를 계산하여 응답한다. 보안 자격 생성자는 받은 R_A로부터 인코딩을 통해 HLP_A를 생성하고 이 값을 저장한다.

• 보안 자격 생성자는 유저 S에게 비밀 값 K_S를 전달한다.

• 보안 자격 생성자는 유저 S와 장치 A를 연결하는 프로세스를 실행한다. 이때 C_S를 생성하고, $P_A = H_1(R_A), P_S = H_{2_{K_s}}(C_S)$, $aIN_R Z_q^*, B = P_A - aP_S$, $d = H_3(H_1(C_A \| C_S \| HLP_A \| a \| H_3(P_S)) + B)$를 계산 후 보안 연합 제공자에게 $C_A, C_S, a, HLP_A, B, d_1$ 을 건네주고 보안 연합 제공자는 이를 저장한다.

2) 인증 및 키 교환 단계

장치 A는 장치 B와 비밀통신하기 위해 유저와 상호 인증 과정을 마치고 유저에게 받은 값들을 활용하여 장치 간 통신을 위한 세션키를 생성한다.

• 장치 A가 유저에게 장치 A, B의 ID를 보낸 후 유저는 각 장치가 본인의 것인지 확인을 위해 보안 연합 제공자에게 유저와 장치의 ID를 보낸다. 보안 연합 제공자는 저장된 값을 확인 후 유저에게 C_A, C_S, HLP_A, a, B, d를 전송한다.

• <그림 2>에서는 유저가 보안 연합 제공자로부터 값을 전달받은 이후 장치 A와 유저간의 인증 과정을 나타낸다. 장치 B 역시 유저와 같은 과정을 동일하게 수행하므로 장치 A에 대한 프로토콜만 표기하였다.

(1) 유저의 질의값을 키를 사용한 해시함수로 P_S를 생성하고, 해시함수를 통해 보안 연합 제공자로부터 전달받은 값의 무결성을 검증한다. P_A를 계산 후 난수 x와 함께 Q_A값을 생성하고, 나중에 검증값으로 사용될 V_A를 계산한다.

(2) 유저는 ID_B, 장치 A의 질의 값, A의 헬퍼데이터와 자신이 생성한 Q_A값을 장치 A에게 전달한다.

(3) 장치 A는 유저로부터 받은 질의 값에 대한 PUF를 이용한 응답 값에 헬퍼데이터를 디코딩하여

R값을 구한다. R값을 해시한 후 인증에 사용될 값을 생성하고 난수 t와 임의의 생성원 Y_A를 만든다. 난수와 생성원을 기반으로 공개키와 개인키를 생성한다.

(4) 장치 A는 인증하기 위해 생성한 값들을 유저에게 전송한다,

(5) 유저는 장치 A에게 받은 값을 이용하여 장치 A가 정당한지 여부를 확인한다.

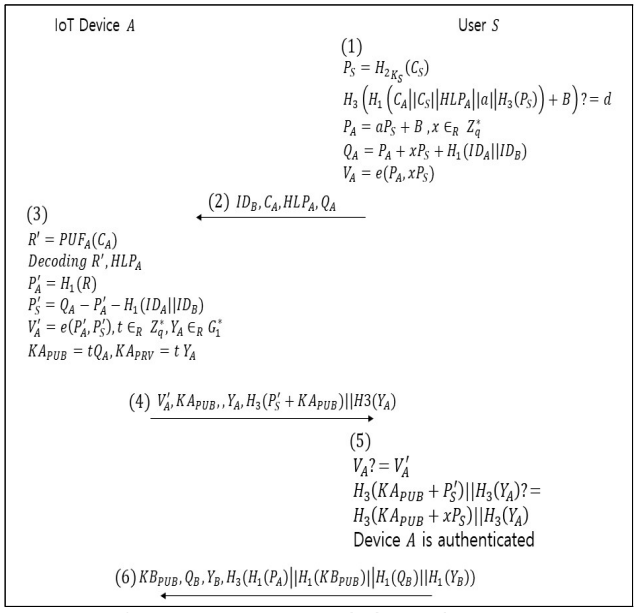
(6) 유저는 장치 A와 동일한 과정을 거친 인증된 장치 B로부터 받은 값을 장치 A에게 전달한다. 이때 정당한 유저라고 인증할 값으로 해시된 P_A값을 해시하여 함께 보낸다.

• 장치 간 세션키를 형성하는 과정은 <그림 3>과 같다.

(1) 장치 A는 유저로부터 받은 장치 B에 대한 값인 KB_{PUB}, Y_B와 임의로 생성한 난수 w를 사용하여 세션키로 사용될 λ를 계산한다.

(2) 장치 A는 장치 B가 λ를 생성할 수 있도록 $w \cdot Q_B$를 건네준다.

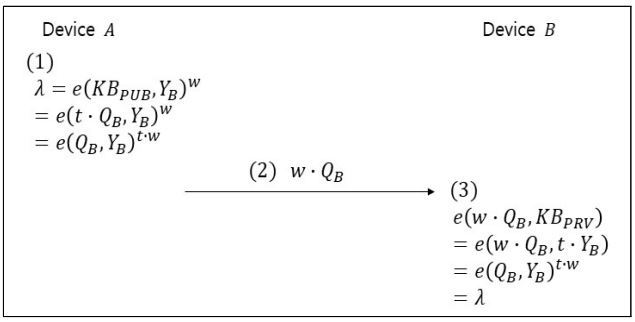
(3) 장치 B는 장치 A에게 받은 값 $w \cdot Q_B$와 자신의 비밀정보 KB_{PRV}를 사용하여 세션키로 사용할 λ를 생성한다.



<그림 2> Chatterjee 기타 등의 프로토콜

3) Chatterjee 기타 등의 프로토콜 취약점

Chatterjee 기타 등의 프로토콜에서 장치간 세션키 λ를 생성할 때 사용되는 인자들이 공개된 채널을 통해 건네주게 된다. 장치 A뿐 아니라 악의적인 사용자가 $KB_{PUB,}Q_B, Y_B$를 얻을 수 있음을 의미한다. 악의적인 사용자가 얻은 값과 임의의 값 w'을 생성하여 세션키 λ'을 생성할 수 있다.



<그림 3> 장치 간 세션키 형성 과정

4. 해결 방안

본 논문에서 $KB_{PUB,}Q_B, Y_B$를 얻은 임의의 장치가 세션키 λ를 생성하는 문제를 해결하고자 한다. 제안하는 해결 방안은 세션키 λ를 생성할 때, 유저와 상호 인증을 마친 정당한 장치 A가 가진 개인키 값 KA_{PRV}를 활용하여 세션키를 만들도록 설계하는 것이다.

1) 세션키 형성 과정

제안하는 장치 간 세션키 형성 과정은 <그림 4>와 같다.

(1) 장치 A는 자신이 생성한 KA_{PRV}, 유저로 부터 건네 받은 KB_{PUB}, 난수 w를 활용하여 타원곡선 paring 연산을 통해 세션키 λ $(= e(KA_{PRV,}KB_{PUB})^w)$를 생성한다.

(2) 장치 A는 장치 B에게 세션키 λ를 만들기 위해 사용될 $w \cdot t_a \cdot Q_B$을 건네준다.

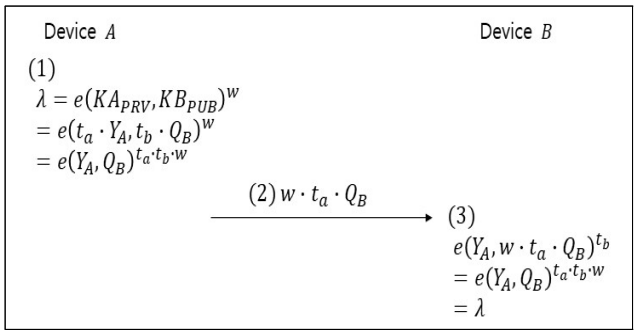
(3) 장치 B는 유저에게 받은 Y_A, 자신이 가진 비밀값 t_b과 장치 A에게 받은 값 $w \cdot t_a \cdot Q_B$을 사용한다. $e(Y_{A,}w \cdot t_a \cdot Q_B)$에 t_b를 거듭제곱 한 후 paring 연산 방법에 따른 계산을 완료하면 λ를 생성할 수 있다.

2) 안전성 분석

본 논문에서 제안한 프로토콜에서는 세션키를 만들 때 장치 A의 개인키 KA_{PRV}와 장치 B의 공개키 KB_{PUB}와 임의의 난수 w가 사용된다. 이때, 개인키는 장치 A가 임의로 생성한 난수 t_a와 임의의 생성

원 Y_A를 사용하여 만든다. 이전의 장치 및 유저 간 인증 과정에서 유저를 통해 Y_A, KA_{PUB}, Q_A가 전달되어 노출되더라도 타원 곡선 이산대수 문제의 어려움에 따르면, 공격자는 $KA_{PUB}(=t_a \cdot Q_A)$와 Q_A 값을 통해서 t_a를 다항 시간 내에 계산하는 것이 어렵다. 마찬가지로 타원 곡선 이산대수 문제에 따라 Q_B를 알고 있더라도, 세션키 형성 중 건네주는 $w \cdot t_a \cdot Q_B$의 값을 통해서도 t_a뿐 아니라 w값도 얻어 낼 수 없다. 따라서 t_a를 모르는 공격자는 장치 A의 개인키 값인 KA_{PRV}를 만들 수 없다. 장치 B는 이를 근거로 오로지 t_a값을 알고있는 장치 A가 세션키를 만들었음을 알 수 있다.

또한 공격자가 장치 B인척 $w \cdot t_a \cdot Q_B$를 탈취하여 장치 A와 세션키를 공유하려고 할지라도 마찬가지의 이유로 장치 B의 비밀 값인 t_b를 알지 못하므로 세션키 λ를 생성할 수 없다. 따라서 정당한 장치 A와 정당한 장치 B만 안전하게 세션키를 주고 받을 수 있게 된다.



<그림 4> 제안하는 세션키 형성 과정

5. 결론

사물인터넷(IoT)의 사용의 증가에 따라 보안 문제도 함께 해결되어야 함에 있어서 자원 문제 등 많은 제한사항이 있는 환경에서 Chatteerjee 기타 등은 PUF를 활용하여 보안성을 높이고 보안 요구사항에 적합한 프로토콜을 제시했다. 그러나 장치 간 세션키 형성 과정에서 사용되는 값이 공개된 채널에서 전달되고 이를 탈취한 공격자가 정당한 장치인 척 세션키를 만들 수 있는 문제점이 발견되었다. 본 논문에서는 이를 해결하고자 세션키를 생성할 때, 타원 곡선 이산대수 문제의 어려움에 기반한 유저와 상호 인증을 마친 정당한 장치만 갖고있는 개인키를 사용함으로써 장치 간 상호 인증을 가능하도록 방법을 제안하였다.

참고문헌

[1] M. Potkonjak and V. Goudar, "Public Physical Unclonable Functions," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1142-1156, Aug. 2014.

[2] K. Zhao and L. Ge, "A Survey on the Internet of Things Security," 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, 2013, pp. 663-667.

[3] A. P. Johnson, R. S. Chakraborty and D. Mukhopadhyay, "A PUF-Enabled Secure Architecture for FPGA-Based IoT Applications," in IEEE Transactions on Multi-Scale Computing Systems, vol. 1, no. 2, pp. 110-122, 1 April-June 2015.

[4] Y. Yilmaz, S. R. Gunn and B. Halak, "Lightweight PUF-Based Authentication Protocol for IoT Devices," 2018 IEEE 3rd International Verification and Security Workshop (IVSW), Costa Brava, 2018, pp. 38-43.

[5] U. Chatterjee et al., "Building PUF Based Authentication and Key Exchange Protocol for IoT Without Explicit CRPs in Verifier Database," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 3, pp. 424-437, 1 May-June 2019.