그림자 패스워드를 사용한 IoT 홈 디바이스 사이의 세션키 공유 프로토콜

정석원*
목포대학교 정보보호학과 교수

Session Key Agreement Protocol for IoT Home Devices using Shadow Passwords

Seok Won Jung*
Professor, Department of Information Security Engineering, Mokpo National University

요 약 유·무선 연결이 가능한 홈 디바이스의 증가로 다양한 홈 서비스가 나타나고 있으나, 인가 없는 원격 접속으로 사생활 침해와 개인정보의 유출이 발생하고 있다. 이는 디바이스의 인증 부재와 전송 데이터의 보호가 없는 것에 대부분 기인한다. 본 논문에서는 스마트폰을 사용하여 디바이스의 비밀 정보를 안전한 메모리에 저장하고 디바이스의 인증을 수행한다. 패스워드에 디바이스 개인키를 곱한 그림자 패스워드를 디바이스에 저장하여 디바이스 패스워드의 직접적인 유출을 막는다. 또한, Lamport의 일회용 패스워드 기법으로 스마트폰과 디바이스를 상호인증하고, SRP 프로토콜을 이용하여 패스워드를 복구하여 디바이스 사이의 세션키를 공유하는 방법을 제안한다. 본 논문에서 제안하는 프로토콜은 도청, 재전송, 위장 공격 등에 안전하다.

주제어 : 사물인터넷, 홈 네트워크, 패스워드 기반, 디바이스 인증, 세션키 공유

Abstract Although various home services are developed as increasing the number of home devices with wire and wireless connection, privacy infringement and private information leakage are occurred by unauthorized remote connection. It is almost caused by without of device authentication and protection of transmission data. In this paper, the devices' secret value are stored in a safe memory of a smartphone. A smartphone processes device authentication. In order to prevent leakage of a device's password, a shadow password multiplied a password by the private key is stored in a device. It is proposed mutual authentication between a smartphone and a device, and session key agreement for devices using recovered passwords on SRP. The proposed protocol is resistant to eavesdropping, a reply attack, impersonation attack.

Key Words : IoT, Home Network, Password Base, Device Authentication, Session Key Agreement

1. 서론

최근 연결형(connected) 가전, 에너지 가전, 실감 미디어 가전, 웰니스 케어 가전 등 다양한 홈 디바이스의 개발과 원격제어 감시, 홈에너지 최적화, 맞춤형 웰니스 서비스 등 홈 서비스의 발전으로 인간 중심의 스마트 홈

본 논문은 2016년도 목포대학교 해외 장기연수 지원으로 수행되었음.
*교신저자 : 정석원(jsw@mokpo.ac.kr)
접수일 2020년 3월 12일 수정일 2020년 4월 21일 심사완료일 2020년 5월 12일

이 점차 활성화되고 있다[1]. 시스코에 따르면 2018년 총 184억 대였던 IP 네트워크 디바이스 수가 2023년에 293억대로 증가할 것으로 예측했다[2].

반면, 인터넷과 연결되는 IoT 디바이스의 증가에 따라 보안 취약성도 지속적으로 나타나고 있다. 한국인터넷진흥원은 IoT의 유형별 주요 보안 위협으로 멀티미디어, 생활가전, 제어 제품에 인증 메커니즘 부재와 네트워크, 모바일 앱, 센서 제품에 전송 데이터 보호의 부재를 주요 원인으로 꼽고 있다[3]. OWASP의 첫 번째 IoT 보안 취약점으로 취약 또는 추측할 수 있거나 하드코드 된 패스워드 사용이 올랐고, 두 번째로 인증받지 않은 원격 접속을 허용하여 기밀성, 무결성/인증, 가용성이 침해되는 것이 뽑혔다[4].

IoT 디바이스 사이의 상호인증은 경량화 프로토콜인 MQTT(Message Queuing Telemetry Transport) 위에 TLS(Transport Layer Security) 또는 CoAP (Constrained Application Protocol) 위에 DTLS (Datagram TLS)를 구현하고 디바이스 인증서를 사용하는 방법이 보편적이다[5-7].

그러나 인증서 기반의 상호인증은 어느 정도 컴퓨팅 파워가 필요하고 통신부하를 견딜 수 있어야 한다. 이를 보완하기 위해 보다 제약적인 환경의 홈 디바이스에 적합한 패스워드 기반의 프로토콜, 하드웨어 장치인 PUF(Physical Unclonable Function)을 사용한 IoT 디바이스의 상호인증 프로토콜, CoAP 위 클라이언트와 서버 사이에서 패이로드 암호화 스킴 상호인증 프로토콜, 블록체인을 이용한 인증 등이 제안되고 있다[8-12].

본 논문에서는 패스워드를 사용하는 스마트 홈 환경에서 디바이스의 인증과 디바이스 사이의 비밀 통신을 위한 세션키 공유 프로토콜을 소개한다. 스마트 폰과 홈 디바이스 사의의 상호인증을 위해 Lamport의 일회용 패스워드를 사용한다. 또한 SRP(Secure Remote Password Protocol) 프로토콜을 변형한 패스워드 복구 절차를 마련하고 복구된 패스워드와 Diffie-Hellman 키 공유 프로토콜을 이용하여 디바이스 사이의 세션키를 공유하는 방법을 제안한다. 본 논문에서 제안하는 프로토콜에서는 디바이스에 패스워드를 그대로 저장하는 대신, 패스워드에 디바이스의 개인키를 곱하여 패스워드를 숨긴 그림자 패스워드를 홈 디바이스에 저장한다. 이를 통해 패스워드 자체의 외부노출을 막는다. 또한, 디바이스와 스마트폰의 위장공격과 재전송 공격을 방어한다.

본 논문의 구성은 다음과 같다. 2장에서 본 논문에서 사용하는 기존 프로토콜들을 살펴보고, 3장에서 제안 프로토콜의 세부 절차를 살펴본다. 또한, 3장에서 프로토콜의 정당성을 검증하고, 몇 가지 안전성에 대해 살펴본다. 4장 결론에서 향후 연구에 대한 검토를 다룬다.

2. 기존 프로토콜

이 장에서는 본 논문에서 제안하는 프로토콜에서 활용하는 기존의 인증 프로토콜과 세션키 공유 프로토콜을 소개한다.

2.1 Lamport의 일회용 패스워드 프로토콜

Lamport는 일방향 함수 F를 사용하여 일회용 패스워드를 사용하는 프로토콜을 제안하였다[13].

〈등록 절차〉
1) 사용자:
 1-1) 패스워드 l_0로부터 N개의 해시 체인을 만든다.
 $$l_0, l_1 = F(l_0), l_2 = F^2(l_0), \cdots, l_N = F^N(l_0)$$
 1-2) DB에 $(l_1, l_2, \cdots . l_{n-1})$ 저장
2) 사용자 → 호스트:
 2-1) 아이디와 패스워드 (I, l_N) 전송
3) 호스트:
 3-1) DB에 (I, l_N)를 저장

〈인증 절차〉
1) 사용자:
 1-1) DB에 저장된 마지막 값 l_{N-1} 검색
 1-2) DB를 $(l_1, l_2, \cdots . l_{n-2})$로 갱신
2) 사용자 → 호스트:
 2-1) (I, l_{N-1}) 전송
3) 호스트:
 3-1) 아이디 I에 해당하는 l_N 검색
 3-2) $l_N' = F(l_{N-1})$ 계산
 3-3) 계산한 l_N'과 저장된 l_N 비교
 3-4) DB에 (I, l_{N-1})을 저장

Lamport의 일회용 패스워드 프로토콜은 일방향 함수 F를 사용하여 〈인증 절차〉의 단계 2-2)에서 $F(l_{N-1})$을 계산한다. 호스트는 l_N 값을 저장하고 있지만, 역 해시함수 값인 l_{N-1}을 계산할 수는 없다. 따라서 l_N을 계산할

수 있는 l_{N-1} 값을 보낸 쪽이 정당한 사용자가 되는 것이다. 도청을 통해 공격자가 l_{N-1}을 수집해도 일방향 함수의 성질 때문에 다음 번에 사용할 l_{N-2}의 값을 찾을 수는 없다.

2.2 Diffie-Hellman 키 공유 프로토콜

1976년 Diffie와 Hellman은 이산대수 문제의 어려움에 근거한 공개키 알고리즘을 사용한 키 공유 프로토콜을 제안하였다[14]. 먼저 두 명의 통신 당사자가 키를 공유할 수 있도록 소수 p에 대한 유한체 $\mathbb{Z}_p^*$의 생성원 g를 공개한다. 그리고 두 사람 A와 B가 키를 공유하기 위해 다음 절차를 따른다.

〈Diffie-Hellman 키 공유 절차〉
1) 사용자 A:
 1-1) 난수 a를 선택
 1-2) $u = g^a \bmod p$ 계산
2) 사용자 A → 사용자 B
 2-1) u 전송
3) 사용자 B:
 3-1) 난수 b를 선택
 3-2) $v = g^b \bmod p$ 계산
4) 사용자 B → 사용자 A
 4-1) v 전송
5) 사용자 A:
 5-1) 공유키 $K = v^a \bmod p$ 계산
6) 사용자 B:
 6-1) 공유키 $K = u^b \bmod p$ 계산

사용자 A는 〈Diffie-Hellman 키 공유 절차〉 단계 5-1)에서

$$v^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p$$

을 얻고, 사용자 B는 단계 6-1)에서

$$u^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p$$

를 얻으므로 두 사용자가 같은 공유키를 가짐을 알 수 있다.

2.3 SRP 프로토콜

먼저 SRP(Secure Remote Password Protocol)에서 사용하는 시스템 파라미터를 〈Table 1〉에 소개한다[15- 16]. 다음은 사용자와 호스트 사이의 세션키 공유 프로토콜이다.

〈등록 절차〉
1) 사용자 → 호스트
 1-1) (I, p) 전송
2) 호스트:
 2-1) 소금값 s 생성
 2-2) 개인키 $x = H(s, p)$ 계산
 2-3) 패스워드 검증자 $v = g^x \bmod N$ 계산
 2-4) (I, s, p) 저장

〈Table 1〉 Definition of System parameters

Parameter	Description
q	a large prime number
N	a prime number, $N = 2q+1$
g	a generator of $\mathbb{Z}_N^*$
$H()$	a hash function such as SHA-3
k	a multiplier, $k = H(N, g)$ or $k = 3$
s	a user's salt
I	the username
p	a cleartext password
u	a random scrambling parameter
a, b	secret ephemeral values
A, B	public ephemeral values
x	the private key, $x = H(s, p)$
v	the password verifier, $v = g^x \bmod N$

〈세션키 공유 절차〉
1) 사용자:
 1-1) 난수 a에 대해 $A = g^a \bmod N$ 계산
2) 사용자 → 호스트:
 2-1) (I, A) 전송
3) 호스트:
 3-1) 난수 b에 대해 $B = kv + g^b \bmod N$ 계산
 3-2) $u = H(A, B)$ 계산
 3-3) $S = (Av^u)^b$ 계산
 3-4) 세션키 $K = H(S)$ 계산
4) 호스트 → 사용자
 4-1) (s, B) 전송
5) 사용자:
 5-1) $x = H(s, p)$ 계산
 5-2) $S = (B - kg^x)^{a+ux} \bmod N$ 계산
 5-3) 세션키 $K = H(S)$ 계산

〈인증 절차〉
1) 사용자 → 호스트:
 1-1) $M = H(H(N) \text{ xor } H(g) | H(I) | s | A | B | K)$ 전송

2) 호스트 → 사용자

2-1) $N = H(A|M|K)$ 전송

사용자와 호스트는 〈세션키 공유 절차〉의 단계 3-3)과 단계 5-2)에서 같은 값을 만들어 세션키를 공유한다. 즉, 사용자는

$$(B-kg^x)^{a+ux} \equiv (kv+g^b-kg^x)^{a+ux} \equiv (g^b)^{a+ux} \equiv g^{ab+bux} \pmod N$$

를 얻고, 호스트는

$$(Av^u)^b \equiv (g^a(g^x)^u)^b \equiv g^{ab+bux} \pmod N$$

으로 사용자와 같은 값을 가진다.

호스트는 〈인증 절차〉 단계 1-1)에서 사용자로부터 받은 M값을 자신이 가지고 있는 N, g, I, s, A, B, K를 해시한 값과 비교하여 사용자를 인증한다.

사용자는 〈인증 절차〉 단계 2-1)에서 호스트로부터 받은 N값을 자신이 가지고 있는 A, M, K를 해시한 값과 비교하여 호스트를 인증한다.

3. 제안 프로토콜

3.1 프로토콜 설계

먼저 본 논문에서 제안하는 프로토콜에서 사용하는 시스템 파라미터를 〈Table 2〉에 소개한다.

〈Table 2〉 Definition of System parameters

Parameter	Description
q	a large prime number
N	a prime number, $N=2q+1$
g	a generator of $\mathbb{Z}_N^*$
$H()$	a hash function such as SHA-3
z	a multiplier, $z=H(N,g)$
M	a smartphone'name
D	a home device' name
md	a session key between M and D
$E_{md}()$	encryption with Session Key md
$D_{md}()$	decryption with Session Key md
s_D	a salt for a Device D
i_D	an identification of a Device D
p_D	a password for a Device D
x_D	device's private key, $x_D=H(s_D,p_D)$
v_D	the verifier, $v_D=g^{x_D} \bmod N$
$\bar{p}_D$	the shadow password, $\bar{p}_D=p_D \cdot x_D \bmod N$
l_{Dn}	nth Lamport's Password for D

사용자는 새로운 홈 디바이스를 구입하고 홈 네트워크 상에 설치할 때, 스마트폰을 이용하여 홈 디바이스의 패스워드를 설정하고 다음의 〈등록 절차〉에 따라 시스템 환경을 설정한다. 스마트폰과의 인증을 위해 Lamport의 일회용 패스워드를 설정하고, 홈 디바이스 사이의 세션키 공유를 위해 SRP 프로토콜과 유사한 시스템 파라미터를 설정한다. 여기에서 홈 디바이스에 패스워드를 그대로 저장하지 않고, 패스워드에 개인 키를 곱한 값인 그림자 패스워드를 저장하여 홈 디바이스의 패스워드가 노출되지 않도록 한다. 즉, SRP 프로토콜과 달리 홈 디바이스에는 그림자 패스워드$\bar{p}_D$ $(=p_D \cdot x_D \bmod N)$을 저장한다.

〈등록 절차〉

1) 스마트폰 M:

1-1) 홈 디바이스 용 아이디, 패스워드 (i_D, p_D)생성

1-2) 소금 값 s_D 생성,

1-3) 개인 키 $x_D=H(s_D,p_D)$ 생성,

1-4) 검증자 $v_D=g^{x_D} \bmod N$ 계산

1-5) 그림자 패스워드 $\bar{p}_D=p_D \cdot x_D \bmod N$ 계산

1-6) t번째 Lamport 패스워드 l_{Dt} 계산

1-7) DB에 (i_D, v_D) 쌍 저장

1-8) 안전한 장소에 (i_D, l_{Dt}, t, x_D) 쌍 저장

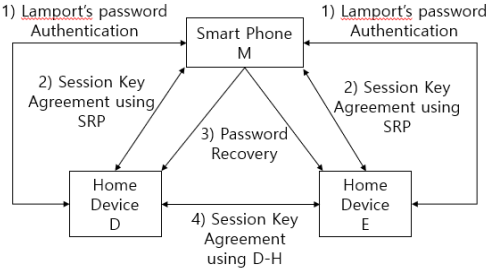
2) 스마트폰 M → 홈 디바이스 D:

2-1) $(i_D, v_D, l_{Dt}, \bar{p}_D)$ 쌍 전송

3) 홈 디바이스 D:

3-1) DB에 $(i_D, v_D, l_{Dt}, \bar{p}_D)$ 쌍 저장

등록된 홈 디바이스 D와 홈 디바이스 E가 세션 키를 공유하는 방법은 [Fig 1]과 같다.



[Fig. 1] Process for session key agreement

홈 디바이스와 스마트폰은 Lamport의 패스워드 프로토콜을 이용하여 상호인증을 한다. 그리고 SRP 프로토콜을 이용하여 세션키를 생성하고, 세션키를 이용하여 홈 디바이스에 패스워드를 복구한다. 홈 디바이스 D와 홈 디바이스 E는 복구된 패스워드를 가지고 Diffie-Hellman(D-H) 프로토콜을 이용하여 세션키를 공유한다. 상세한 절차는 다음과 같다.

홈 네트워크 상에 등록된 홈 디바이스와 스마트폰 사이의 인증 절차는 Lamport의 일회용 패스워드를 사용한다. 홈 디바이스가 등록된 이후 여러 번 인증을 거친 후 홈 디바이스가 저장하고 있는 Lamport 패스워드를 l_{Dn}이라고 가정하자.

〈홈 디바이스 인증 절차〉
1) 홈 디바이스 D → 스마트폰 M:
1-1) (i_D, l_{Dn}) 쌍 전송
2) 스마트폰 M:
2-1) DB에서 i_D에 해당하는 (l_{D0}, n) 검색
2-2) l_{D0}를 n번 해시한 $l_{Dn}' = H^n(l_{D0})$ 계산
2-3) l_{Dn}과 l_{Dn}'을 비교하여 인증

스마트폰 인증과 홈 디바이스의 패스워드를 복구하기 위해 먼저 SRP의 세션키 공유 절차를 따라 세션키를 만든다. 스마트폰은 세션키로 Lamport의 패스워드와 홈 디바이스의 개인키를 암호화하여 보내고, 홈 디바이스는 이를 복호화하여 스마트폰을 인증한다. 통신하고자 하는 홈 디바이스와의 세션키를 만들기 위해 자신의 패스워드를 복구한다.

〈스마트폰 인증 및 홈 디바이스 D의 패스워드 복구〉
1) 홈 디바이스 D → 스마트폰 M:
1-1) (i_D, 패스워드 복구 요청) 전송
2) 스마트폰 M:
2-1) 난수 a로 $A = g^a \bmod N$ 계산
3) 스마트폰 M → 홈 디바이스 D:
3-1) A 전송
4) 홈 디바이스 D:
4-1) 난수 b로 $B = zv_D + g^b \bmod N$ 계산
4-2) $u = H(A, B)$ 계산
4-3) 세션키 $md = (Av^u)^b \bmod N$ 계산
5) 홈 디바이스 D → 스마트폰 M:
5-1) B 전송
6) 스마트폰 M:
6-1) $u = H(A, B)$ 계산
6-2) 안전한 DB에서 x_D 검색
6-3) 세션키 $md = (B - zg^{x_D})^{a+ux_D}$ 계산
6-4) $L = E_{md}(l_{Dn-1}, x_D)$ 암호화
6-5) DB를 $(l_{D0}, n-1)$로 갱신
7) 스마트폰 M → 홈 디바이스 D:
7-1) L 전송
8) 홈 디바이스 D:
8-1) $(l_{Dn-1}, x_D) = D_{md}(L)$ 복호화
8-2) $H(l_{Dn-1})$과 l_{Dn} 비교
8-3) l_{Dn} 대신 l_{Dn-1} 저장
8-4) $p_D = \bar{p}_D \cdot x_D^{-1} \bmod N$ 복구

홈 디바이스 D와 홈 디바이스 E 사이의 세션키 공유는 Diffie-Hellman 키 공유 프로토콜을 이용한다. 〈디바이스 사이의 세션키 공유 절차〉에서는 Diffie-Hellman 프로토콜과는 달리 난수 대신 패스워드와 난수를 곱한 값을 사용한다.

〈디바이스 사이의 세션키 공유 절차〉
1) 홈 디바이스 D:
1-1) 난수 i로 $U = g^{ip_D} \bmod N$ 계산
2) 홈 디바이스 D → 홈 디바이스 E:
2-1) U 전송
3) 홈 디바이스 E:
3-1) 난수 j로 $V = g^{jp_E} \bmod N$ 계산
3-2) 세션키 $de = U^{jp_E} \bmod N$ 계산
4) 홈 디바이스 E → 홈 디바이스 D:
4-1) V 전송
5) 홈 디바이스 D:
5-1) 세션키 $de = V^{ip_D} \bmod N$ 계산

3.2 프로토콜 검증

3.2.1 스마트폰과 디바이스 상호인증

스마트폰이 홈디바이스를 인증하는 방법은 3.1절 〈홈 디바이스 인증 절차〉로 Lamport의 방법을 사용한다. 홈 디바이스가 보낸 n번째 l_{Dn}과 스마트폰에 저장된 초기 패스워드 값 l_{D0}를 n번 해시한 값을 비교하여 같으면 홈

디바이스를 인증한다. 해시값이 일치하는 l_{Dn}을 가진 것은 홈디바이스 D 밖에 없으며, 이 값은 통신로에 노출된 적이 없는 값으로 한 번 사용 후 폐기되는 패스워드이다.

홈 디바이스가 스마트폰을 인증하는 절차는 3.1절 〈스마트폰 인증 및 홈 디바이스 D의 패스워드 복구〉의 절차를 따른다. 단계 2-1)부터 단계 6-3)를 거쳐 세션키 md를 설정한 후 단계 7)에서 스마트폰이 홈 디바이스 D로 암호화하여 보낸 $L(=E_{md}(l_{Dn-1}, x_D))$를 단계 8-1)에서 복호화한다. 복호화 값에 포함된 $n-1$번째 Lamport 패스워드 l_{Dn-1}를 단계 8-2)와 같이 홈 디바이스가 해시한 값이 저장된 값인 l_{Dn}과 같으면 스마트폰을 인증한다. 즉, 스마트폰으로부터 받은 값을 복호화 값 X를 해시한 값이 l_{Dn}과 같을 확률은

$$H(X) = l_{Dn}$$

을 만족하는 X를 찾는 것과 같은데, 해시함수의 역상 저항성 성질에 의해 이런 X를 찾을 확률은 매우 희박하다. 따라서 단계 8-2)에서 비교하는 값이 같다면 정당한 스마트폰임을 확인하게 된다.

3.2.2 스마트폰과 디바이스의 세션키 공유

세션키는 3.1절 〈스마트폰 인증 및 홈 디바이스 D의 패스워드 복구〉의 단계 4-3)에서

$$md \equiv (Av^u)^b \equiv (g^a g^{x_D u})^b \equiv g^{ab+bux_D} \pmod N$$

이고, 단계 6-3)에서

$$\begin{aligned} md &\equiv (B - zg^{x_D})^{a+ux_D} \equiv (zv_D + g^{x_D} - zg^{x_D})^{a+ux_D} \\ &\equiv (zg^{x_D} + g^{x_D} - zg^{x_D})^{a+ux_D} \equiv (g^{x_D})^{a+ux_D} \\ &\equiv g^{ab+bux_D} \pmod N \end{aligned}$$

로 같은 값임을 알 수 있다. 그런데 스마트폰에 저장된 패스워드 검증값 v_D를 획득한 공격자는 단계 4)를 수행할 수 있어 공유 세션키를 만들 수 있다(v_D는 안전하지 않은 DB에 저장되어 있다). 그러나 스마트폰을 위장한 공격자는 안전한 DB에 저장되어 있는 l_{D0}와 x_D 값을 모르기 때문에 단계 6-4)의 L 값을 만들 수 없으며, 홈 디바이스는 위장 스마트폰을 알아낼 수 있어 스마트폰을 위장한 공격은 발각된다.

3.2.3 디바이스 사이의 세션키 공유

디바이스 사이의 세션키는 3.1절 〈디바이스 사이의 세션키 공유 절차〉의 단계 3-2에서

$$de \equiv U^{jp_E} \equiv (g^{ip_D})^{jp_E} \equiv g^{ijp_Dp_E} \pmod N$$

이고, 단계 5-1)에서

$$de \equiv V^{ip_D} \equiv (g^{jp_E})^{ip_D} \equiv g^{ijp_Dp_E} \pmod N$$

으로 같은 값을 갖는다. 공유 세션키를 만들기 위해서는 3.1절 〈스마트폰 인증 및 홈 디바이스 D의 패스워드 복구〉 절차를 통해 인증을 받고, 스마트폰으로부터 받은 암호화된 x_D을 복호화한 후 단계 8-4)와 같이 패스워드를 복구해야만 한다. 또한, 디바이스 사이의 세션키를 공유할 때마다 새로운 난수를 사용하므로 매번 다른 세션키를 공유할 수 있다.

3.3 프로토콜의 안전성

공격자가 3.1절 〈홈 디바이스 인증 절차〉의 단계 1)을 도청한 후 수집한 정보 (i_D, l_{Dn})쌍을 재전송 할 수 있다. 그러나 l_{Dn}은 이전 통신 시 사용된 것으로 스마트폰의 DB에는 $(l_{D0}, n-1)$이 저장되어 있다. 따라서 스마트폰은 단계 2-2)에 따라서 $l_{Dn-1} = H^{n-1}(l_{D0})$를 계산한다. 그 결과 공격자가 보낸 l_{Dn}과 스마트폰이 계산한 l_{Dn-1}이 같지 않으므로 홈 디바이스의 인증요청은 거절된다.

공격자가 3.1절 〈홈 디바이스 인증 절차〉에서 스마트폰을 가장하면 홈 디바이스의 l_{Dn}을 얻을 수 있다. 그러나 〈스마트폰 인증 및 홈 디바이스 D의 패스워드 복구〉에서 홈 디바이스가 스마트폰의 인증을 요구한다. 스마트폰을 위장한 공격자가 위장에 성공하기 위해서는 〈스마트폰 인증 및 홈 디바이스 D의 패스워드 복구〉의 단계 6-4)와 같이 (l_{Dn-1}, x_D) 쌍을 암호화할 수 있어야 한다. 이를 위해서는 획득한 l_{Dn}의 값으로부터 l_{Dn-1}을 찾을 수 있어야 한다. 그런데 이 둘은 해시함수에 대해

$$H(l_{Dn-1}) = l_{Dn}$$

인 관계에 있으며, l_{Dn-1}를 찾는 것은 l_{Dn}에 대한 역상을 찾는 것과 같은 문제이다. 그런데 역상 저항성 성질을 갖는 해시함수를 사용하면 역상을 찾는 것은 매우 어렵다. 확률적으로 희박한 역상을 찾았다고 하더라도 단계 6-4)와 같이 암호화를 하려면 홈 디바이스의 개인키 x_D를 알아야만 한다. 그러나 이 값은 스마트폰의 안전한 장소에 저장되어 있고, 네트워크 상에 노출되지 않으므로 스마트폰을 위장한 공격자는 단계 6-4)를 올바르게 수행할 수 없다.

스마트폰을 위장한 공격자는 〈스마트폰 인증 및 홈 디바이스 D의 패스워드 복구〉의 단계 3-1)과 단계 7-1)을 도청할 수 있다. 도청한 정보인 A와 L을 홈 디바이스로

재전송 할 수 있다. 그러나 매번 홈 디바이스는 단계 4-1)에서 난수 b'에 대해 세션키 $md' = (Av^{u'})^{b'} \bmod N$을 만든다. 매번 난수 b와 b'이 다르므로 세션키 md와 md'은 다르다. 홈 디바이스는 단계 8-1)에서 스마트폰으로부터 받은 L을 세션키 md'로 복호화하여 $D_{md'}(L) = (X, Y)$를 얻을 때, X와 l_{Dn-1} 값이 같을 확률은 매우 희박하다. 따라서 스마트폰을 위장한 재전송 공격은 실패한다.

공격자가 홈 디바이스 D의 메모리에 저장되어 있는 그림자 패스워드 $\bar{p}_D (= p_D \cdot x_D \bmod N)$의 값을 알아냈다고 하더라도 개인키 x_D를 알 수 없으므로 패스워드 p_D를 알 수 없다. 디바이스 사이의 세션키 공유는 홈 디바이스의 패스워드 p_D를 기반으로 만들므로 p_D를 알 수 없는 공격자는 디바이스 사이의 세션키를 만들 수 없다.

4. 결론

유·무선 통신 기능을 가진 홈 디바이스의 증가로 인해 홈 네트워트가 복잡해지고 있으며, 홈 네트워트의 진화에 따라 다양한 서비스 제공을 위해 홈 디바이스 사의의 통신이 증가하고 있다. 반면, 홈 디바이스의 지능화와 유·무선 통신 지원에 대한 역기능으로 불법적인 홈 디바이스 제어, 위장 홈 디바이스 설치, 백도어를 통한 개인정보 유출 등이 발생하는 상황이다. 이러한 역기능을 막고 신뢰성 있는 홈네트워크 구축을 위해서는 홈 디바이스의 인증은 필수적인 요소이며, 통신 상에서 정보를 보호하기 위한 세션키 공유도 필요하다.

본 논문에서는 Lamport의 일회용 패스워드를 사용하여 홈 디바이스를 인증한다. 또한, 패스워드에 디바이스의 개인키를 곱한 그림자 패스워드와 SRP를 이용하여 홈 디바이스 사이의 세션키를 공유하는 방법을 제안하였다. 홈 디바이스에 그림자 패스워드를 저장하므로 공격자에게 그림자 패스워드가 유출되어도 홈 디바이스의 패스워드 유출을 막을 수 있다. 그리고 홈 디바이스는 인증된 절차로 그림자 패스워드로부터 패스워드를 복구한 후 세션 키를 만들므로 세션키에 홈 디바이스만의 고유값이 포함된다. 이는 일반적인 Diffie-Hellman 프로토콜이 공개된 생성원과 임의의 난수를 사용하는 것과 달리 홈 디바이스의 고유값으로 세션키를 만드는 장점이 있다.

본 논문에서 제안된 방법은 스마트폰을 이용하여 홈 디바이스의 Lamport 패스워드와 개인키를 안전하게 저장하고, 이를 통하여 홈 디바이스의 인증을 제공한다. 그리고 홈 디바이스 사이는 그림자 패스워드로부터 세션키를 공유하도록 하여 홈 디바이스 사이의 기밀성고 무결성 등의 정보보호 서비스를 제공할 수 있다. 따라서 본 논문에서 제한한 그림자 패스워드를 사용한 디바이스 사이의 인증과 세션키 공유 프로토콜을 위장 홈 디바이스 또는 백도어 프로그램의 사용을 차단하여 홈 네트워크 내의 정보를 보호할 수 있다.

향후 홈 디바이스의 Lamport 패스워드 갱신, 그림자 패스워드 갱신 등의 기능 추가 및 안전성 분석과 연산의 효율성에 대한 연구가 필요하다. 또한, 홈 게이트웨이를 포함한 네트워크 구축을 통한 제안 프로토콜의 실증이 필요하다.

REFERENCES

[1] KATS, *Smart home industry and standardization trend*, KATS Technical Report, Vol.74, 2015.

[2] CISCO, *CISCO Annual Internet Report(2018-2023)*, 2020.

[3] KISA, *IoT Security Guide for Household Appliances*, 2017.

[4] https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

[5] MQTT 3.1.1 specification. OASIS. 2015.

[6] Z.Shelby, K.Hartke and C.Bormann, "Constrained Application Protocol (CoAP)," RFC 7252, 2014.

[7] E.Rescorla and N.Modadugu, "Datagram Transport Layer Security Version 1.2," RFC 6347, 2012.

[8] X.Sun, S.Men, C.Zhao and Z.Zhou, "A security authentication scheme in machine-to-machine home network service." Secur. Comm.. Netw., Vol.8, pp.2678-2686, 2012.

[9] M.Zhao, X.Yao, H.Liu and H.Ning, "Physical Unclonable Function Based Authentication Protocol for Unit IoT and Ubiquitous IoT." In Proceedings of the 2016 International Conference on Identification, IIIKI, pp.179-184, 2016.

[10] M.A.Muhal, X.Luo, Z.Mahmood and A.Ullah, "Physical Unclonable Function Based Authentication Scheme for Smart Devices in Internet of Things." In Proceedings of the 2018 IEEE International Conference on Smart Internet of Things(SmartIoT), pp.160-165, 2018.

[11] M.A.Jan, F.Khan, M.Alam and M.Usman, "A payload-based mutual authentication scheme for Internet of Things." Future Gen. Comput. Syst., Vol.92, pp.1028-1039, 2019.

[12] K.Lee, "A Scheme for Information Protection using Blockchain in IoT Environment," Jour. of The Korea Internet of Things Society, Vol.5, No.2, pp.33-39, 2019.

[13] L.Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, Vol.24, No.11, pp.770-772, 1981.

[14] W.Diffie and M.E.Hellman, "New Directions in Cryptography," IEEE Trans. on Information Theory, Vol.IT-22, No.6, pp.644-654, 1976.

[15] T.Wu, "The Secure Remote Password Protocol," Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, pp.97-111, 1998.

[16] T.Wu, "SRP-6: Improvements and Refinements to the Secure Remote Password Protocol," Submission to the IEEE P1363 Working Group, 2002.

정 석 원(Seok Won Jung) [종신회원]

■ 1993년 2월 : 고려대학교 일반대학원 수학과 (이학석사)
■ 1997년 2월 : 고려대학교 일반대학원 수학과 (이학박사)
■ 1999년 2월 ~ 2001년 2월 : ㈜ 텔리맨 책임연구원
■ 2004년 4월 ~ 현재 : 목포대학교 정보보호학과 교수

〈관심분야〉
암호알고리즘 구현, 암호프로토콜 설계, 부채널공격법