Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.6, Dec. 2016 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2016.26.6.1471

스마트홈 환경에서 패스워드 추측 공격에 안전한 개선된 3PAKE 기법에 대한 연구*

이 대 휘,† 이 임 영‡
순천향대학교 컴퓨터학과

A Study on Enhanced 3PAKE Scheme against Password Guessing Attack in Smart Home Environment*

Dae-Hwi Lee,† Im-Yeong Lee‡
Department of Computer Science and Engineering, Soonchunhyang University

요 약

최근 IoT에 대한 관심이 급증함에 따라 다양한 IoT 서비스들이 출시되고 있다. 그 중 스마트홈은 사용자의 주거공간에 IoT를 접목함으로써 우리의 생활과 매우 밀접하게 연관되어 있다. 그렇기 때문에, 정당하지 않은 사용자가 스마트홈 내부의 디바이스에 접근한다면, 일상생활과 매우 밀접한 만큼 사용자에게 더 큰 피해를 입힐 수 있다. 예를 들어 스마트홈 내부의 도어락에 인증되지 않은 공격자가 접근하여 명령을 수행할 수 있게 된다면, 주거 침입의 형태로 큰 재산 피해를 입을 수도 있다. 이를 방지하기 위해 본 논문에서는 패스워드 기반의 인증 및 키 교환(PAKE)을 이용하여 사용자와 디바이스가 홈 게이트웨이를 통해 인증과 키 교환을 할 수 있는 3자간 PAKE(3PAKE) 기법을 제안한다.

ABSTRACT

As concern about IoT is increasing recently, various IoT services are being launched. Smart home is closely related to our daily life by combining IoT with user's residential space. Therefore, if an unauthorized user accesses a device inside a Smart home, it can cause more serious damage to user as it is related with daily lives. For instance executing the command allowing unauthenticated access for the internal locking device can be a real harm to user's property like a home invasion. To prevent this problem, this paper introduces 3PAKE Techniques, which provides authenticated Key exchange through Home gateway using Password-based Authenticated Key Exchange(PAKE).

Keywords: Smart Home, Password-based Authentication, 3PAKE

I. 서 론

IoT(Internet of Things) 시대를 맞아 센서와 컨트롤 기술이 발달하고, 이에 따라 다양한 서비스들이 출시되고 있다. 스마트폰이나 태블릿을 통해 사람들은 언제나 인터넷에 연결된 생활을 하고 있으며, IoT에 대한 관심도 증가되면서 사람과 사물, 공간을 연결하는 초연결사회가 도래하고 있다. IoT는 우리의 일상생활뿐만 아니라 다양한 분야에 적용되고 있으며, 우리나라를 비롯한 세계 주요국과 글로벌 기업들도 적극적으로 투자하여 개발하고 있다[1]. 이에 따라 IoT를 활용하는 다양한 서비스가 개발되고 있는데, 스마트홈 서비스도 이 중 하나이다. 스마트홈은 우리의 주거환경에 IoT를 적용한 서비스로, 가정

Received(11. 15. 2016), Modified(12. 08. 2016), Accepted(12. 08. 2016)
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2016-R0992-16-1006)
† 주저자, leedh527@sch.ac.kr
‡ 교신저자, imylee@sch.ac.kr(Corresponding author)

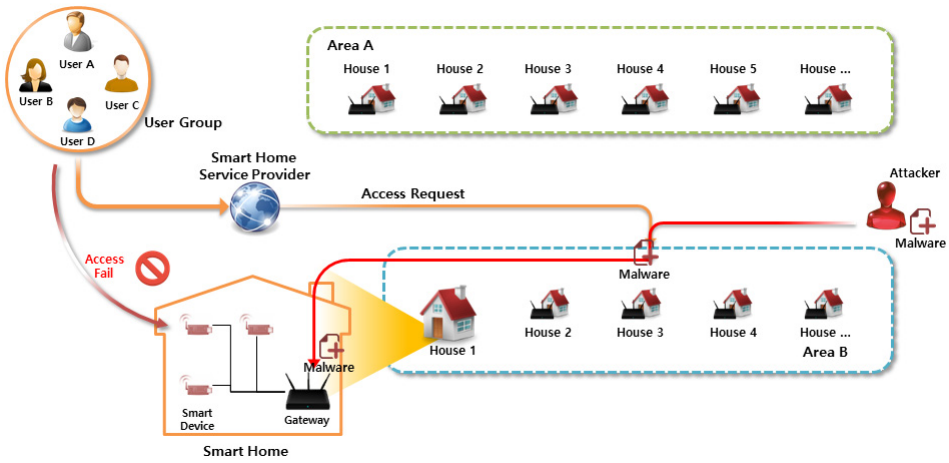

Fig. 1. Structure of Smart Home and Security Threat

내의 가전기기들이 인터넷에 연결된다. 외부에서 사용자가 원격으로 집 안의 에어컨 등의 가전제품의 전원을 제어하거나, 보일러에 접근하여 온도를 알맞게 조절하는 등의 편리한 생활을 위한 서비스를 제공한다. 최근에는 국내에서 SKT와 KT, LG와 같은 대형 통신사도 각각 스마트홈 서비스를 출시했으며, 이를 위한 스마트 디바이스들을 판매하기 시작했다.

스마트홈 환경에서는 어플리케이션을 조작하는 사용자, 스마트홈 내부에서 인터넷과 연결되는 홈 게이트웨이, 그리고 스마트홈을 구성하는 스마트 디바이스가 각각 통신하여 서비스를 제공한다. 사용자가 홈 게이트웨이를 통해 스마트홈 내부의 스마트 디바이스에게 명령을 내리는 구조이다. 이러한 구조에서는 사용자와 디바이스의 인증 및 통신에 있어서 안전성이 고려되어야 한다. 만약 인가되지 않은 공격자나 공격자의 디바이스가 전송되는 데이터를 가로채어 홈 게이트웨이를 통해 스마트홈 네트워크의 접근 권한을 얻게 된다면, 도어락을 열어 주거 침입을 허용하거나 가스밸브를 여는 등의 큰 사고를 일으킬 수 있다. 이외에도 데이터 위·변조, 프라이버시 유출, DDoS 공격 등에 대한 취약점이 발생할 수 있으므로 이를 고려한 보안 프로토콜이 필요하다[2,3].

이에 본 논문에서는 스마트홈 환경에서 3PAKE (Three-party Password-based Authenticated Key Exchange)을 이용하여 사용자 및 디바이스에 대한 인증을 제공하기 위한 기법을 제안한다. 3PAKE는 두 객체 사이에 서버가 인증 및 키 교환을 중재하는 기법으로, 스마트홈 환경에서 홈 게이트웨이가 중재역할을 하여 사용자와 디바이스 간의 인증과 키 교환을 할 수 있도록 설계한다.

본 논문의 구성은 2장에서는 스마트홈 환경에서의 보안위협에 대해 살펴보고, 3PAKE 기술에 대해 분석한다. 3장에서는 패스워드 추측 공격에 안전하면서도 효율성을 제공하기 위한 방식과, 홈 게이트웨이에게 인증 값을 남기지 않는 방식의 보안요구사항에 대해 분석하고, 4장에서는 제안방식에 대해 기술한다. 5장에서는 기존방식과 제안방식을 비교하여 분석하고, 6장에서 결론을 맺는다.

II. 관련연구

본 장에서는 스마트홈에서의 보안위협과 3PAKE 기술에 대해 분석한다.

2.1 스마트홈 보안위협

스마트홈 환경은 가정 내부의 기기들을 제어할 수 있는 정당한 사용자와 스마트홈 내부의 홈 게이트웨이, 그리고 스마트 디바이스의 3종류의 객체로 이루어진다. 스마트홈 서비스를 위해서는 사용자가 네트워크 통신망을 통해 스마트홈 네트워크에 연결된 환경이 기반이 되므로 다양한 보안 위협이 발생할 수 있다. 통신상의 데이터를 가로채어 데이터를 위·변조하거나, DDoS, 시스템 해킹과 스마트폰 분실로 인한 개인정보 유출 등이 대표적이라고 할 수 있다[2,3,4].

데이터 위·변조 공격은 공격자가 스마트홈 환경에서의 통신 데이터를 가로채고 위·변조를 수행하여

재전송한다. 서비스 사용자에게는 정상적인 처리 데이터를 보내지만, 실제로 스마트홈에서는 오작동을 유발하게 하여 피해를 입힐 수 있다.

DDoS 공격은 공격자가 홈 게이트웨이에게 패킷을 대량으로 요청하거나 필요한 시스템 자원을 고갈시켜 서비스 이용자에게 정상적인 서비스를 제공할 수 없게 한다. 또한, 스마트홈 네트워크에 침입하여 스마트 디바이스들을 악성코드에 감염시킬 경우 DDoS 공격의 주체인 좀비PC로 이용하여 다른 네트워크를 공격하도록 명령할 수 있게 된다.

시스템 해킹은 정당하지 않은 사용자나 디바이스가 홈 네트워크에 접근할 경우, 악의적인 목적으로 바이러스와 악성코드 등을 침투시킬 수 있다. 이러한 경우는 홈 네트워크 전체가 감염된다면 도어락을 악의적인 목적으로 열어 외부의 침입을 허용하여 금전 피해를 입히거나, 가스락 또는 온도조절기를 조작하여 더욱 큰 사고로 이어지게 할 수도 있다.

개인정보 유출은 스마트홈에서 고정형 스마트 디바이스가 항상 집안의 개인정보를 수집하기 때문에 발생할 수 있다. 스마트홈 서비스의 보급이 확산되며 스마트홈 영역까지 사이버공격의 대상이 된다면, 사용자들에게 사이버공격에 따른 사회적, 경제적인 불안 요소로 작용할 수 있을 것이다.

2.2 3PAKE(Three-Party Password-based Authenticated Key Exchange)

PAKE(Password-based Authenticated Key Exchange) 프로토콜은 서버와 클라이언트 사이에서 안전한 통신을 하기 위해 상호 인증을 실시한 후 통신에 사용될 세션키를 안전하게 교환할 수 있는 기술이다. PAKE가 제안되기 이전에는 1992년에 Bellovin과 Merritt가 공개키 방식을 이용해 대칭키를 교환하는 EKE(Encrypted Key Exchange) 프로토콜을 제안하였다[5]. 그 후로부터 EKE로부터 변형된 다양한 프로토콜들이 제안되었으며, 2000년대에는 Bellare와 Rogaway가 사전공격에 안전한 AKE(Authenticated Key Exchange) 프로토콜을 제안하였다[6]. 이후 AKE의 응용으로 패스워드를 기반으로 한 PAKE가 제안되었다. PAKE는 서버와 클라이언트가 인증을 위해 사전에 공유한 패스워드를 사용하고 이후의 통신에 사용될 세션키를 동의하는 것이 목적인 프로토콜이다. 서버는 패스워드에 의해 만들어진 검증자만을 갖고 세션키에 대한 동의가 이루어진다[7].

3PAKE는 3자간의 키 교환 및 인증을 위한 PAKE 프로토콜의 한 종류이다. 3PAKE는 상호 인증 및 키 교환을 하고자 하는 두 사용자 사이에 서버 역할을 하는 객체가 존재한다. 일반적으로 서버와 각 사용자는 각각 패스워드를 공유하여 패스워드를 이용해 두 사용자 사이의 상호 인증과 키 교환에 대한 중재역할을 해준다. 패스워드를 사용하는 이유는 인증서, 생체정보와 같은 다른 인증 방식에 비해 사용자가 상대적으로 기억하기 쉬우며, 설계에 따라 매우 간단한 동작만으로 구현이 가능하기 때문이다. 하지만, 패스워드는 편리한 만큼 낮은 엔트로피를 가지기 때문에 공격자가 추측을 하기 쉽다. 따라서 안전한 3PAKE 설계를 위해서는 패스워드 추측 공격에 대해 꼭 고려되어야 한다. 패스워드 추측 공격은 통신에 직접 참여하여 서버의 응답값을 통해 패스워드를 유추하는 온라인 패스워드 추측 공격과 통신상의 데이터를 도청·수집하고 이를 이용해 패스워드를 추측하는 오프라인 추측 공격이 있다.

2.3 기존 3PAKE 기술 연구

2.3.1 C.Lee 등의 방식

C.Lee 등은 Wu[8] 등의 방식을 분석하고, 오프라인 패스워드 추측 공격에 안전하지 않음을 밝혀 개선 방안을 제시하였다[9]. 본 방식에서는 일반적인 이산대수 문제를 이용한 Diffie-Hellman 키 교환 방식을 응용하여 타원곡선 이산대수 문제를 이용한 프로토콜을 설계하였으며, 오프라인 패스워드 추측 공격을 탐지할 수 있는 3PAKE 기법을 제안하였다. 하지만, 통신하고자 하는 객체 A와 B 사이의 서버는 통신을 요청하는 A와 상호 인증할 수는 있지만 B에 대해서는 상호 인증을 제공하지 않아 온라인 패스워드 추측 공격의 가능성이 존재한다.

2.3.2 T.Lee 등의 방식

T.Lee는 Abdalla[10] 등이 제안한 SPAKE(Simple PAKE)를 응용하여 서버의 명시적 인증을 제공하는 S-EA-3PAKE와 묵시적 인증을 제공하는 S-IA-3PAKE를 제안하였다[11]. 하지만 두 방식 모두 패스워드 기반이기 보다는 대칭키 기반의 키 교환 구조와 같은 형태이다. 통신하고자 하는 각 객체

A와 B 사이의 키 교환 이전에 A와 B가 각각 패스워드를 기반으로 한 서버와의 대칭키를 생성하고, 이 대칭키를 이용해 A와 B 사이의 세션키를 생성한다. 이 때문에 다른 기존방식에 비해 A와 B에서의 연산에 대한 오버헤드가 증가하게 되며, 경량화를 요구하는 IoT 환경에서는 비효율적이라고 할 수 있다.

2.3.3 Farash 등의 방식

Farash는 Tallapally[12]의 3PAKE 프로토콜을 분석하고, 온라인 및 오프라인 패스워드 추측 공격에 대한 취약점을 제시하여 이를 보완한 프로토콜을 제안하였다[13]. 또한 인증 및 키 교환의 중재 역할을 하는 서버의 공개키가 필요 없이 서버를 명시적으로 인증할 수 있게 도와준다. 하지만 본 방식에서는 다른 제안방식들에 비해 통신량이 많은 편이며, 세션키가 설립되기 전까지 통신하고자 하는 객체 A, B는 서로를 인증할 수 없도록 설계되어 공격자에게 온라인 패스워드 공격의 위험성이 존재하는 문제가 있다.

III. 보안요구사항

스마트홈 보안에서의 핵심은 사용자와 스마트 디바이스의 인증이다. 패스워드 추측 공격 등을 행하여 공격자가 인증에 성공하거나 세션키를 알아낼 수 있게 된다면, 악의적인 공격자에 의해 보안 취약점이 발생할 수 있다[2,3,4]. 따라서 본 논문에서 제안하는 스마트홈에서 인증과 기밀성을 제공하기 위한 보안 요구사항은 다음과 같다.

- 상호 인증 : 홈 게이트웨이는 사용자의 스마트폰을 통해 스마트홈에 접근하려는 사용자와 스마트 홈 내부의 스마트 디바이스의 상호 인증을 중재한다.
- 접근제어 : 상호 인증을 통해 정당한 권한을 획득한 사용자와 스마트 디바이스만이 스마트홈 네트워크에 접근할 수 있어야 한다.
- 효율성 : 스마트홈 환경에서 연산량이 낮은 기기를 위해 연산적으로 효율성을 제공해야 한다.
- 신분 위장 방지 : 정당한 사용자의 스마트폰과 스마트 디바이스만이 스마트홈 서비스를 이용할 수 있어야 한다.
- 재전송 공격 방지 : 통신 시 전송되는 메시지를 공격자가 획득하여도 정당한 사용자로 위장할 수 없어야 한다.
- 패스워드 추측 공격 방지 : 통신 시 전송되는 정보가 노출되어도 사용자의 패스워드를 추측할 수 없어야 한다.

IV. 제안방식

본 장에서는 3장에서의 보안요구사항을 만족하는 스마트홈 서비스를 위한 경량화된 XOR 기반의 3PAKE 기법과 Diffie-Hellman 키 교환을 응용한 3PAKE 기법을 제안한다.

4.1 XOR 기반의 3PAKE 기법(제안방식 1)

본 제안방식에서는 XOR 연산과 해시연산을 기반으로 효율성을 높인 3PAKE 기법을 제안한다. 사용자와 스마트 디바이스는 각 등록 단계를 통해 안전하게 홈 게이트웨이와의 패스워드를 주고받아 저장한다. 이후 인증 및 키 교환 단계에서 단계적인 정보 전송을 통해 사용자와 홈 게이트웨이, 스마트 디바이스간의 상호 인증이 이루어진다.

4.1.1 시스템 계수

본 제안방식에서 사용되는 시스템 계수는 다음과 같다.

- $*$: 참여 객체(U: $User$, GW: $Gateway$, D: $Device$)
- ID_* : 참여 객체 $*$의 식별자
- PW_U : 사용자의 패스워드
- DID_* : $*$가 생성한 동적 파라미터
- $h(\bullet)$: 일방향 해쉬함수
- R_* : $*$가 생성한 비밀 값
- S_U : 사용자와 홈 게이트웨이가 공유한 비밀 값
- S_{GW} : 홈 게이트웨이와 스마트 디바이스가 공유한 비밀 값
- K : 스마트 디바이스에서 생성한 세션키 생성에 사용되는 값
- T_i : i 번째 타임스탬프
- C_i : i 단계의 인증 값
- V_D : 스마트 디바이스의 검증에 사용되는 값
- V_{GW} : 홈 게이트웨이의 검증에 사용되는 값

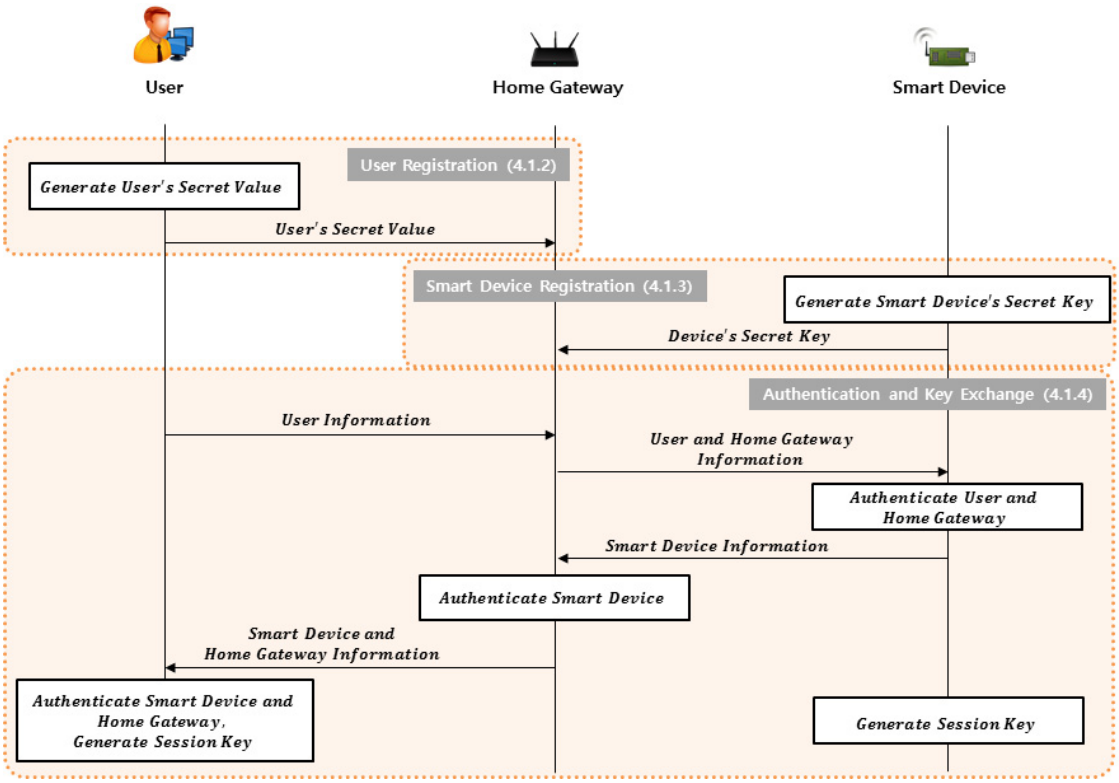

Fig. 2. Structure of Proposed Scheme 1

4.1.2 사용자 등록 단계

Step 1. 사용자는 자신의 스마트폰을 통해 ID_U와 PW_U를 연접하여 해쉬 연산 후, 비밀 값 R_U를 선택하여 다음과 같이 홈 게이트웨이와 공유할 비밀 값 S_U를 계산한다.

$$S_U = R_U \oplus h(ID_U \| PW_U)$$

Step 2. 사용자는 생성한 S_U와 ID_U를 안전한 채널을 통해 홈 게이트웨이에게 전송한다.

Step 3. 홈 게이트웨이는 사용자로부터 수신한 ID_U와 S_U를 저장한다.

4.1.3 스마트 디바이스 등록 단계

Step 1. 홈 게이트웨이는 ID_{GW}와 임의의 수 x를 연접하여 해쉬한 값과 자신의 비밀 값인 R_{GW}를 통해 스마트 디바이스와 공유할 비밀 값 S_{GW}를 계산한다.

$$S_{GW} = R_{GW} \oplus h(ID_{GW} \| x)$$

Step 2. 홈 게이트웨이는 등록하고자 하는 스마트 디바이스에게 안전한 채널을 통해 ID_{GW}와 S_{GW}를 전송한다.

Step 3. 스마트 디바이스는 홈 게이트웨이로부터 수신한 ID_{GW}와 S_{GW}를 저장하고, ID_D를 홈 게이트웨이에게 전송한다.

Step 4. 홈 게이트웨이는 스마트 디바이스로부터 전송받은 ID_D와 함께 R_{GW}와 S_{GW}를 저장한다.

4.1.4 인증 및 키 교환 단계

Step 1. 사용자는 상호 인증을 위해 자신의 비밀 값 R_U와 홈 게이트웨이와 공유한 값 S_U를 이용하여 DID_U, C_1, C_2를 다음과 같이 계산한다.

$DID_U = R_U \oplus h(S_U \| ID_U \| T_1)$
$C_1 = h(DID_U \oplus S_U)$
$C_2 = h(R_U \| C_1 \| S_U \| T_1)$

Step 2. 사용자는 현재의 타임스탬프와 함께 홈 게이트웨이에게 $ID_U, ID_D, DID_U, C_2, T_1$를 전송한다.

Step 3. 홈 게이트웨이는 $|T^* - T_1| \le \Delta T$를 계산한다. ΔT는 전송에 발생할 수 있는 예상 전송 지연 값이다. 만약 T_1이 유효하다면 홈 게이트웨이는 사용자를 인증하기 위해 다음을 계산해 C_2와 C_2'를 비교하여 검증한다.

$C_1' = h(DID_U \oplus S_U)$
$R_U = DID_U \oplus h(S_U \| ID_U \| T_1)$
$C_2' = h(R_U \| C_1' \| S_U \| T_1)$
$Home\ Gateway\ check\ C_2 ? = C_2'$

Step 4. 홈 게이트웨이는 C_2를 검증하여 사용자를 확인한 후, 자신의 비밀 값 R_{GW}와 스마트 디바이스와 공유한 값 S_{GW}를 이용하여 DID_{GW}, C_3, C_4를 다음과 같이 계산한다.

$DID_{GW} = R_{GW} \oplus h(S_{GW} \| ID_{GW} \| T_2)$
$C_3 = h(DID_{GW} \oplus S_{GW})$
$C_4 = h(R_{GW} \| C_3 \| S_{GW} \| T_2)$

Step 5. 홈 게이트웨이는 현재의 타임스탬프와 함께 스마트 디바이스에게 ID_U, DID_{GW}, C_4, T_2를 전송한다. 여기서 사용자의 ID_U는 사용자에게 스마트홈 서비스를 제공하기 위해 전송한다.

Step 6. 스마트 디바이스는 $|T^* - T_2| \le \Delta T$를 계산하여 시간 유효성을 확인한다. T_2가 유효하다면 스마트 디바이스는 홈 게이트웨이를 인증하기 위해 다음과 같이 C_4와 C_4'를 비교하여 검증한다.

$C_3' = h(DID_{GW} \oplus S_{GW})$
$R_{GW} = DID_{GW} \oplus h(S_{GW} \| ID_{GW} \| T_2)$
$C_4' = h(R_{GW} \| C_3' \| S_{GW} \| T_2)$
$Smart\ Device\ check\ C_4 ? = C_4'$

Step 7. 스마트 디바이스는 C_4를 검증하여 홈 게이트웨이를 확인한 후, 상호 인증을 위해 검증 값 V_D을 다음과 같이 계산하고, 세션키 생성에 사용될 K를 생성하여 C_5를 계산한다.

$V_D = h(DID_{GW} \| T_3 \| C_3)$
$D: C_5 = K \oplus h(S_{GW} \| T_3)$

Step 8. 스마트 디바이스는 현재의 타임스탬프와 함께 홈 게이트웨이에게 V_D, C_5, T_3를 전송한다.

Step 9. 홈 게이트웨이는 $|T^* - T_3| \le \Delta T$를 계산하여 시간 유효성을 확인한다. T_3이 유효하다면 홈 게이트웨이는 스마트 디바이스와의 상호 인증을 위해 V_D'를 계산하여 인증한다. 그리고, S_{GW}와 T_3를 이용해 K를 다음과 같이 계산하여 획득한다.

$V_D' = h(DID_{GW} \| T_3 \| C_3)$
$Smart\ Device\ check\ V_D ? = V_D'$
$K = C_5 \oplus h(S_{GW} \| T_3)$

Step 10. 홈 게이트웨이는 V_D을 확인하여 스마트 디바이스와 상호 인증 후, 사용자와의 상호 인증을 위해 자신의 검증 값 V_{GW}를 다음과 같이 계산하며, 세션키 생성에 사용될 K를 이용하여 C_6을 계산한다.

$V_{GW} = h(DID_U \| T_4 \| C_1)$
$C_6 = K \oplus h(S_U \| T_4)$

Step 11. 홈 게이트웨이는 현재의 타임스탬프와 함께 사용자에게 V_{GW}, C_6, T_4를 전송한다.

Step 12. 사용자는 $|T^* - T_4| \le \Delta T$를 계산하여 시간 유효성을 확인한다. T_4가 유효하다면 사용자는 홈 게이트웨이와의 상호 인증을 위해 V_{GW}'를 계산하여 인증한다. 또한 S_U와 T_4를 통해 K를 획득한다.

$V_{GW}' = h(DID_U \| T_4 \| C_1)$
$User\ check\ V_{GW} ? = V_{GW}'$
$K = C_6 \oplus h(S_U \| T_4)$

Step 13. 사용자와 스마트 디바이스는 K를 해쉬하여 세션키 $SK = h(K)$를 계산한다.

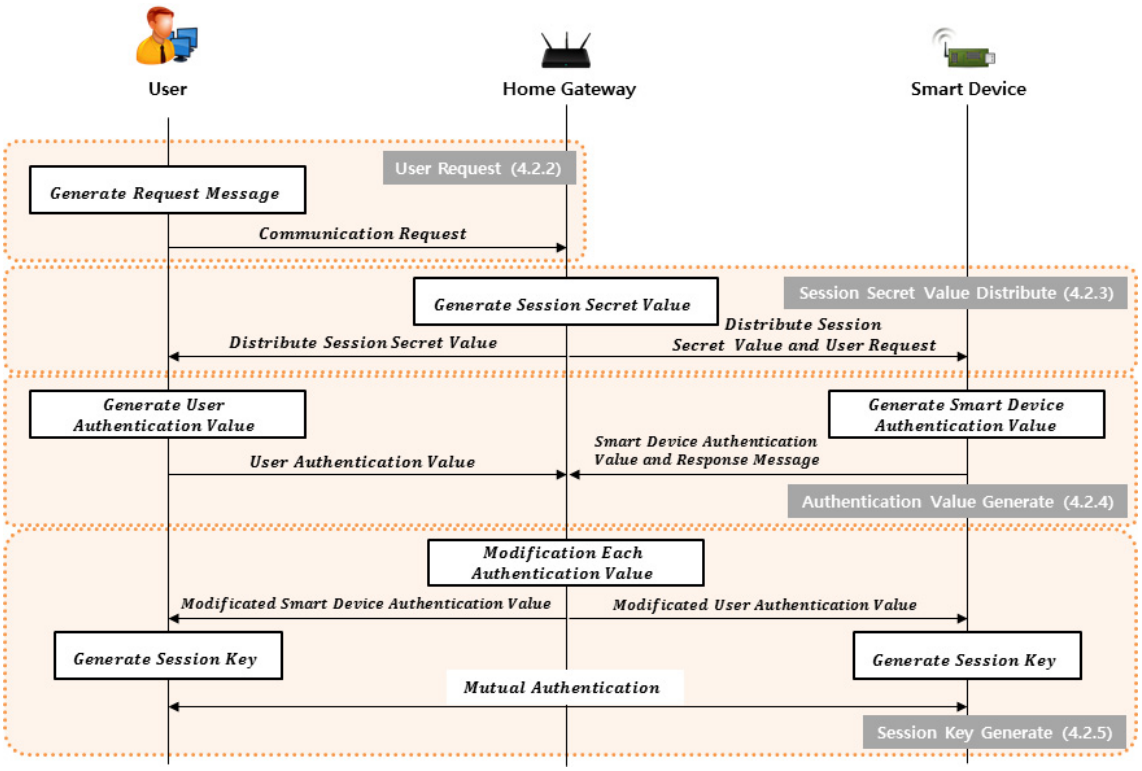

Fig. 3. Structure of Proposed Scheme 2

4.2 Diffie-Hellman 기반의 3PAKE 기법(제안방식 2)

본 제안방식에서는 Diffie-Hellman 키 교환 프로토콜을 응용하여 사용자와 스마트 디바이스 사이의 인증과 키 교환을 이룬다. 사용자와 디바이스는 홈 게이트웨이에게 사전에 안전한 채널을 통해 패스워드 기반의 검증 값을 저장한다. 이후 사용자 통신 요청 단계에서 홈 게이트웨이에게 스마트 디바이스와의 통신을 요청하고, 홈 게이트웨이는 세션 비밀 값 분배 단계에서 사용자와 스마트 디바이스에게 세션의 새로운 비밀 값을 전송한다. 사용자와 스마트 디바이스는 홈 게이트웨이는 인증 값 생성 단계에서 자신들의 인증 값을 생성하여 홈 게이트웨이에게 전송한다. 세션키 생성 단계에서 홈 게이트웨이는 인증 값을 수정하여 사용자와 스마트 디바이스에게 분배하고, 세션키를 생성하여 상호 인증을 완료한다.

4.2.1 시스템 계수

본 제안방식에서 사용되는 시스템 계수는 다음과 같다.

- $*$: 참여 객체(U: $User$, GW: $Gateway$, D: $Device$)
- ID_* : 참여 객체 $*$의 식별자
- p : 큰 소수
- g : 곱셈군 Z_p^*의 생성자
- $h(\bullet)$: 일방향 해쉬함수
- PW_* : $*$와 GW가 공유하고 있는 패스워드
- V_* : $*$의 패스워드 기반 검증 값 ($V_* = h(PW_* \| ID_* \| ID_{GW})$)
- r_{Uold} : 이전 세션에 생성된 U와 GW의 비밀 값
- r_U : 현재 세션에 생성되어 업데이트된 U와 GW의 비밀 값
- SK : 사용자 A와 B 사이의 세션키

4.2.2 사용자 통신 요청 단계

Step 1. 사용자는 스마트 디바이스와 통신하기 위해 임의의 a를 선택한 후 다음과 같이 요청 메시지 Req_U를 생성하여 Req_U, ID_U, ID_D를 홈 게이트웨이

에게 전송한다.

$$Req_U = a \bmod p \oplus h(V_U \| r_{Uold} \| ID_U)$$

Step 2. 홈 게이트웨이는 임의의 수 z를 선택하고 $g^z \bmod p$를 계산한 후 현재 세션에 사용될 r_U를 생성한다. 그리고, 사용자로부터 전송받은 값 Req_U를 통해 $a = Req_U \oplus h(V_U \| r_{Uold} \| ID_U)$를 계산한다.

4.2.3 세션 비밀 값 분배 단계

Step 1. 홈 게이트웨이는 다음과 같이 $Req_{GW}, R_U, R_D, RV_U, RV_D$를 생성한다.

$$Req_{GW} = a \oplus h(V_D \| r_U \| ID_U)$$
$$R_U = r_U \oplus V_U$$
$$R_D = r_U \oplus V_D$$
$$RV_U = h(r_U \| V_U)$$
$$RV_D = h(r_U \| V_D)$$

Step 2. 홈 게이트웨이는 사용자에게 R_U, RV_U, g^z를, 스마트 디바이스에게 $Req_{GW}, ID_U, R_D, RV_D, g^z$를 각각 전송한다.

4.2.4 인증 값 생성 단계

Step 1. 사용자와 스마트 디바이스는 각각의 패스워드 기반 검증 값 V_U와 V_D를 이용해 새로운 비밀 값 r_U', r_U''을 구하고, RV_U', RV_D'를 다음과 같이 계산하여 비교를 통해 홈 게이트웨이로부터 수신한 RV_U와 RV_D를 검증한다.

$$r_U' = R_U \oplus V_U$$
$$RV_U' = h(r_U' \| V_U)$$
$$User\ check\ RV_U' ? = RV_U$$
$$r_U'' = R_D \oplus V_D$$
$$RV_D' = h(r_U'' \| V_D)$$
$$Smart\ Device\ check\ RV_D' ? = RV_D$$

Step 2. 사용자는 RV_U를 검증 후 임의의 x를 선택하고 g^{xz}를 계산해 사용자의 인증 값 A_U를 다음과 같이 생성하여 홈 게이트웨이에 전송한다.

$$A_U = (g^{xz} \bmod p) \oplus h(r_U \| ID_U \| ID_D)$$

Step 3. 스마트 디바이스는 RV_D를 검증 후 Req_{GW}에서 x를 다음과 같이 계산하여 획득한다. 그리고, 임의의 b,y를 선택하고 다음과 같이 스마트 디바이스의 인증 값 A_D와 Res_D를 계산하여 홈 게이트웨이에게 전송한다.

$$x = Req_{GW} \oplus h(V_D \| r_U \| ID_U)$$
$$A_D = (g^{yz} \bmod p) \oplus h(r_D \| ID_U \| ID_D)$$
$$Res_D = b \oplus h(V_D \| r_U \| ID_D)$$

4.2.5 세션키 생성 단계

Step 1. 홈 게이트웨이는 사용자와 스마트 디바이스로부터 받은 정보를 이용하여 Res_{GW}를 계산 후, 사용자에게 A_D, Res_{GW}를 전송하고 스마트 디바이스에게 A_U를 전송한다.

$$Res_{GW} = Res_D \oplus h(V_D \| r_U \| ID_D) \oplus h(V_U \| r_U \| ID_D)$$

Step 2. 사용자는 Res_{GW}에서 b를 획득하고, A_D에서 g^{yz}를 획득하여 세션키 SK를 생성한다. 그리고 세션키의 인증 값 A_{UD}를 생성한다.

$$b = Res_{GW} \oplus h(V_U \| r_U \| ID_D)$$
$$g^{yz} \bmod p = A_D \oplus h(r_U \| ID_D \| ID_U)$$
$$SK = g^{xyz} \bmod p$$
$$A_{UD} = h(b \| r_U \| SK \| ID_U \| ID_D)$$

Step 3. 스마트 디바이스는 A_U에서 g^{xz}를 획득하여 세션키 SK를 생성한다. 그리고 세션키의 인증 값 A_{DU}를 생성한다.

$$g^{xz} \bmod p = A_U \oplus h(r_U \| ID_U \| ID_D)$$
$$SK = g^{xyz} \bmod p$$
$$A_{DU} = h(a \| r_U \| SK \| ID_U \| ID_D)$$

Step 4. 사용자와 스마트 디바이스는 각각 생성한 A_{UD}, A_{DU}를 홈 게이트웨이를 통해 교환하여 자신이 가진 정보를 통해 검증한다.

$$A_{DU}' = h(a \| r_U \| SK \| ID_U \| ID_D)$$
$$Smart\ Device\ check\ A_{DU}' ? = A_{DU}$$
$$A_{UD}' = h(b \| r_U \| SK \| ID_U \| ID_D)$$
$$User\ check\ A_{UD}' ? = A_{UD}$$

V. 제안방식 분석

5.1 XOR 기반의 3PAKE 기법(제안방식 1)

제안방식 1의 경우 XOR 기반의 3PAKE 기법으로 경량화에 초점을 맞추어 제안된 방식이다. 기존 방식들의 경우 대부분이 이산대수 문제를 기반으로 한 Diffie-Hellman 키 교환 방식을 사용하지만, 본 제안방식에서는 XOR 연산과 해쉬연산을 이용하여 패스워드 추측 공격을 방지하였다. 특히나 경량화를 요구하는 IoT와 스마트홈 환경에서 연산에 부담을 주지 않으며, 통신에 참여한 사용자와 홈 게이트웨이, 스마트 디바이스 간의 3자간 인증을 제공하도록 설계되었다. 패스워드 PW_U를 알고 있는 사용자만이 스마트홈 네트워크에 접근할 수 있으며, 통신상에 공개되는 동적 파라미터 DID나 단계별 인증 값 C를 공격자가 수집하여 재전송 하더라도 패스워드와 세션키를 유도해낼 수 없다. 또한 홈 게이트웨이에서 식별자를 확인하여 신분 위장 공격을 방지하고 타임스탬프를 추가하여 재전송 공격을 방지하였다. 하지만, Diffie-Hellman 키 교환 방식을 이용하지 않아 키를 분배하기 위한 정보를 홈 게이트웨이가 확인 후 사용자와 스마트 디바이스에게 분배해야 하기 때문에 홈 게이트웨이에 키가 노출된다. 엄격한 의미에서의 3PAKE에서는 키 교환과 인증의 중재역할을 하는 서버에서는 생성되는 키 값을 알 수 없어야 한다. 생성되는 키들을 저장해두고 있다면, 외부의 공격자로부터 공격의 대상이 될 수도 있으므로, 본 논문에서 제안하는 환경인 스마트홈에서의 홈 게이트웨이에서도 안전한 키의 관리가 필요하다. 따라서 대칭키 기반의 상호 인증 및 세션키 분배보다는 안전성이 떨어진다고 판단된다.

5.2 Diffie-Hellman 기반의 3PAKE 기법(제안방식 2)

제안방식 2의 경우 Farash의 방식을 응용하여 사용자와 스마트 디바이스의 검증 정보를 홈 게이트웨이와 공유시켜 검증을 할 수 있도록 한다. 추가로 공개되어 전송되는 값을 공격자가 수집하더라도, 세션마다 사용자, 홈 게이트웨이, 스마트 디바이스가 생성하는 임의의 수 a, b, x, y, z를 모두 알 수 없기 때문에 세션키와 패스워드를 추측할 수 없다. 즉, 온라인 및 오프라인 패스워드 추측 공격에 안전하도록 업데이트 되는 랜덤 값을 이용하여 이전 세션에서 정상적인 인증 및 키 교환을 받은 사용자나 스마트 디바이스만이 인증 및 키 교환이 가능하도록 설계되었다. 이를 통해 사용자와 스마트 디바이스의 상호 인증이 가능하며 제안방식 1과는 달리 Diffie-Hellman 기반의 키 교환 방식을 사용하므로 서버

Table 1. Analysis of Proposed Schemes

		C.Lee[8]	T.Lee-1[9]	T.Lee-2[9]	Farash[10]	Proposed Scheme 1	Proposed Scheme 2
Integrity		○	○	○	○	○	○
Server Authentication		○	X	○	○	○	○
Traffic		6	8	10	9	8	9
Key Exposure to Home Gateway		○	○	○	○	X	○
Masquerade Attack		△	○	○	○	○	○
Replay Attack		X	○	○	X	○	○
Password Guessing Attack		○	△	△	○	○	○
Computation	User	3E+4H	4E+4H	4E+5H	3E+5H	6H+4X	2E+5H+2X
	Server	4E+4H	6E+2H	6E+6H	3E+4H	10H+6X	E+6H+6X
	Device	3E+4H	4H+4H	4E+5H	3E+5H	5H+2X	2E+6H+5H
	Total	10E+12H	14E+10H	14E+16H	9E+14H	21H+12X	5E+17H+13X

○: Offer, Secure △: Usually-offer X: Non-offer, Insecure
E: Exponentiation H: Hash function X: XOR

에서 키를 확인하거나 계산할 수도 없다. 또한 기존의 Farash 방식에 비해 지수승 연산과 통신 횟수도 줄여 효율성을 향상시켰다. 하지만 만약 한번 키가 노출되면 이후의 세션 정보도 계속 노출되는 형태이기 때문에, 사용자가 스마트홈을 서비스를 이용하면서 주기적으로 패스워드와 키의 업데이트를 할 수 있도록 권장해야 한다. 또한, 8번의 통신 횟수를 가지는데, 이후 효율성을 더욱 증가시키는 방향으로 연구해야할 필요가 있다고 판단된다.

VI. 결 론

IoT의 발달로 각종 서비스들이 출시되고 있으며, 스마트홈은 최근 상용화가 되고 있는 IoT 서비스 중 하나이다. 다양한 스마트홈 서비스가 출시되고 있지만, 인증에 대한 보안 취약점들이 있으며 안전한 스마트홈을 위해 효율적이고 안전한 기술의 개발이 필요하다. 본 논문에서는 안전한 스마트홈 서비스를 위한 3PAKE 기법을 제안하여 재전송 공격을 방지하고 IoT 환경에 적합하도록 효율성을 제공한다. 최근 스마트홈 서비스의 상용화가 진행되고 있지만, 아직까지는 스마트홈 보안에 대한 연구가 많이 부족하다. 스마트홈은 특히 우리의 주거생활에 밀접하게 연관되어있기 때문에, 보안이 취약하다면 주거침입 등의 금전적 손실을 불러올 수 있을 것이다. 따라서 이후에도 스마트홈의 상용화를 위해 안전하고 효율적인 상호 인증 방식에 대해 많은 연구가 진행되어야 한다.

References

[1] Hak-Jun Lee, “Smart Home based on Internet of Things,” Jonornal of the KICS, 32(4), pp. 44-49, Mar. 2015.

[2] Moo-Hwan Kim and Yong-Tae Shin, “A Study on The Smart Home Service Security Threat,” Conference of the KICS, pp. 1069-1070, Jan. 2016.

[3] Ho-Seok Ryu and Jin Kwak, “Analysis of Security Threats and Security Requirements in Smart Home,” Conference of the KSII, pp. 113-114, Oct. 2014.

[4] Jun-Sub Kim, “Authentication and Key Management Technology for Secure Smart Home Service,” Ph.D.Thesis, Soonchunhyang University, Feb. 2015.

[5] S. Bellovin and M. Merritt, “Encrypted Key Exchange: Password-based Protocols Secure against Dictionary Attacks,” IEEE Symposium on Research in Security and Privacy, pp. 72-84, May, 1992.

[6] M. Bellare, D. Pointcheval and P. Rogaway, “Authenticated Key Exchange Secure against Dictionary Attacks,” EUROCRYPT 2000, Lecture Notes in Computer Science, vol. 1807, pp. 139-155, May, 2000.

[7] Choon-Sik Park, “Analysis on Security Vulnerability of Password-based Key Exchange and Authentication Protocols,” Journal of KMMS, 11(10), pp. 1403-1408, Oct. 2008.

[8] S. Wu, Q. Pu, S. Wang and D. He, “Cyptanalysis of a Communication-efficient Three-party Password Authenticated Key Exchange Protocol,” Information Sciences, vol. 215, pp. 83-96, Dec. 2012.

[9] C.C. Lee, S.T. Chiu and C.T. Li, “Improving Security of A Communication-efficient Three-party Password Authentication Key Exchange Protocol,” International Journal of Network Security, vol. 17, no. 1, pp. 1-6, Jan. 2015.

[10] M. Abdalla, O. Chevassut, P.A. Fouque and D. Pointcheval, “A Simple Threshold Authenticated Key Exchange From Short Secrets,” Advances in Cryptology - Proceedings of ASIACRYPT ’05, Lecture Notes in Computer Science, vol. 3788, pp. 566 - 588, Dec. 2005.

[11] T.F. Lee and T. Hwang, “Simple Password-based Three-Party Authenticated Key Exchange without Server Public Keys,” Information Sciences, vol. 180, no. 9, pp. 1702-1714,

May. 2010.
[12] S. Tallapally, "Security Enhancement on Simple Three-Party PAKE Protocol," Information Technology and Control, vol. 41, no. 1, pp. 15-22, 2012.
[13] M.S. Farash and M.A. Attari, "An Enhanced and Secure Three-Party Password-based Authenticated Key Exchange Protocol without Using Server's Public-Keys and Symmetric Cryptosystems," Information Technology and Control, vol. 43, no. 2, Mar. 2014.

〈저자소개〉

이 대 휘 (Dae-Hwi Lee) 학생회원
2015년 2월: 순천향대학교 컴퓨터소프트웨어공학과 졸업
2015년 3월~현재: 순천향대학교 컴퓨터학과 석사과정
〈관심분야〉 암호프로토콜, 인증, IoT, 컴퓨터보안

이 임 영 (Im-Yeong Lee) 종신회원
1981년 2월: 홍익대학교 전자공학과 졸업
1986년 2월: 오사카대학 통신공학전공 석사
1989년 2월: 오사카대학 통신공학전공 박사
1989년~1994년: 한국전자통신연구원 선임연구원
1994년~현재: 순천향대학교 컴퓨터소프트웨어공학과 교수
〈관심분야〉 암호이론, 정보이론, 컴퓨터보안