The Journal of Digital Policy & Management 2013 Jul; 11(7): 141-148

스마트카드 및 동적 ID 기반 전기 자동차 사용자 인증 스킴

정수영*, 곽진**
순천향대학교 정보보호학과 정보보호응용 및 보증연구실*, 순천향대학교 정보보호학과**

Smart Card and Dynamic ID Based Electric Vehicle User Authentication Scheme

Su-Young Jung*, Jin Kwak**
ISAA Lab, Dept of Information Security Engineering, Soonchunhyang University*
Dept of Information Security Engineering, Soonchunhyang University**

요 약 스마트그리드는 정보통신기술을 이용하여 전력공급자와 소비자의 양방향통신을 가능하게 한다. 또한 동적인 전력 공급이 가능하기 때문에 전기 자동차 기술과 접목시킬 경우 전기 자동차 충전 인프라를 활성화시키고 전기 자동차의 배터리를 가정용 축전지로 활용하여 재판매할 수도 있다. 이러한 전기 자동차 충전 인프라는 가정, 아파트, 건물, 기타 충전소 등에 고정적으로 위치하여 있고 사용자만 유동적으로 서비스를 이용한다. 만약 유동적으로 서비스를 이용하는 사용자에 대해 인증이 이루어지지 않을 경우 전력 서비스의 불법적인 사용, 전력 정보 유출, 불법적인 전력 요금 변경 등의 피해가 발생할 수 있다. 본 논문에서는 스마트그리드 환경에서 안전하게 전기 자동차 관련 서비스를 이용하기 위해 스마트카드 및 동적 ID 기반 사용자 인증 스킴을 제안한다.

주제어 : 스마트카드 및 동적 ID 기반, 전기 자동차 사용자 인증, 사용자 인증, 스마트그리드, 전기 자동차 보안

Abstract Smart grid can two-way communication using ICT(Information & Communication Technology). Also, smart grid can supply to dynamic power that grafted to electric vehicle can activate to electric vehicle charging infrastructure and used to storage battery of home. Storage battery of home can resale to power provider. These electric vehicle charging infrastructure locate fixed on home, apartment, building, etc charging infrastructure that used fluid on user. If don't authentication for user of fluid user use to charging infrastructure, electric charging service can occurred to illegal use, electric charges and leakgage of electric information. In this paper, we propose smartcard and dynamic ID based user authentication scheme for used secure to electric vehicle service in smart grid environment.

Key Words : Smart Card and Dynamic ID Based, Electric Vehicle User Authentication, User Authentication, Smart grid, Electric Vehicle Security

Received 31 May 2013, Revised 28 June 2013
Accepted 20 July 2013
Corresponding Author: Jin Kwak(Soonchunhyang University)
Email: jkwak@sch.ac.kr

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.otg/licenses/by-nc/3.0), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. 서론

스마트그리드는 현대화된 정보통신기술을 이용하여 전력공급자와 소비자의 양방향 통신을 할 수 있도록 하는 전력시스템으로서 단방향 통신을 하는 기존의 전력망의 전력 시스템 노후화, 늘어나는 전력 수요로 인해 전력 공급 불안정, 신재생 에너지 활용의 낮은 비율 등의 문제점을 해결할 수 있다. 스마트그리드 기술을 통해 공급자와 소비자는 양방향 통신을 이용하며 전력 사용에 대한 모니터링, 신재생 에너지에 대한 효율적인 활용, 안정적인 전력 공급, 전력 공급자와 소비자 간의 다양한 서비스 제공 등이 가능하다. 또한 스마트그리드의 핵심 개념 중 하나인 동적인 전력 공급을 전기 자동차 기술에 접목할 경우 전기 자동차의 충전 인프라를 활성화시킬 수 있고 전기 자동차의 배터리를 가정용 축전지로 활용하여 전력을 재판매할 수도 있다[1,2].

스마트그리드는 공급자를 최상단으로 두고 소비자가 최하위 단에 위치하는 계층적구조로 이루어져 있다. 최하위단에 위치한 스마트미터는 가정, 건물, 마트, 기타 충전소 등의 충전 인프라에 고정적으로 위치하고 사용자들이 유동적으로 이용하게 된다. 이와 같이 전기 자동차 전력 서비스를 이용하는 사용자가 유동적인 이러한 구조에서 정당한 사용자만 전력 서비스를 이용할 수 있도록 하는 사용자 인증절차가 필요하다. 인증이 이루어지지 않을 경우 전력 서비스의 불법적인 사용, 전력 정보 유출 등의 피해가 발생할 수 있다[3-5].

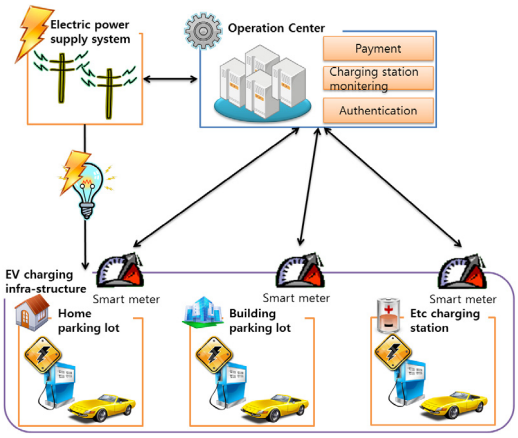
본 논문에서는 스마트그리드 환경의 전기 자동차 전력 서비스를 정당한 사용자만이 이용할 수 있도록 하는 사용자 인증 스킴을 제안한다.

2. 관련연구

2.1 스마트그리드 환경의 전기 자동차 개요

스마트그리드 환경을 통해 전기 자동차에 대한 전력 소비량 예측을 용이하게 해주고 충전 인프라를 최적화시킬 수 있다. 또한 전기 자동차를 가정용 축전지로 활용하여 전력 요금이 저렴한 시간에 충전을 하고 전력 요금이 비싼 시간에는 재판매 할 수 있다. 이를 통해 가정에서까지도 전력 공급자와 양방향 전력거래를 가능하게 해준다[6-8].

다음 그림[Fig. 1]은 스마트그리드환경에서 전기 자동차 충전 인프라에대한 구조를 나타낸다.



[Fig. 1] Electric vehicle infrastructure in smartgrid

2.2 전기 자동차의 사용자 인증 필요성

스마트그리드 환경에서 각 가정의 전력 사용이나 전기 자동차를 이용할 때 사용자 인증이 필요한 부분이 존재한다. 스마트미터는 각 가정, 건물, 기타 충전소 등의 충전 인프라에 고정되어 있고 사용자가 유동적으로 변하기 때문에 사용자를 안전하게 인증할 수 있는 방법이 필요하다. 또한 전기 자동차를 이용하기 위해 충전을 하거나 이미 충전되어 있는 전력을 축전지로 활용하여 요금이 비싼 시간에 재판매를 하는 등의 활동을 할 수 있다. 전력을 충전/판매할 때는 불법적인 사용자에 의해 전기 자동차 전력 서비스가 이용될 수 있고 충전/판매한 전력에 대한 요금 등을 처리하기 위해 사용자를 판별할 수 있어야 한다.

이러한 기능을 제공하기 위해서는 사용자를 식별할 수 있고 정당한 사용자만이 이용할 수 있도록 하는 사용자 인증이 필요하다.

2.3 스마트카드 및 동적 ID 기반 사용자 인증 기법

스마트카드 및 동적 ID를 기반으로 사용자가 서버에 인증하는 방식을 제안하였다. 사용자, 서버 및 등록 센터

로 구성되어 있으며, 사용자는 등록 센터와 안전한 채널을 통해 인증에 필요한 값을 전송받아 스마트카드에 저장한다. 이렇게 저장된 값을 서버에 로그인할 때 사용자 인증에 필요한 값으로 활용한다[9,10].

3. 사용자 인증을 위한 보안 요구사항

3.1 재전송 공격(Replay attack)

사용자를 인증할 때 사용되는 값은 재전송공격으로부터 안전해야한다. 사용자를 인증할 수 있는 값이 매번 같거나 공격자가 그 값을 재전송하면, 악의적으로 인증하는데 활용될 수 있다. 만약 악의적인 인증이 이루어질 경우 공격자가 다른 사용자로 로그인하여 사용자의 정보 및 전력 사용 정보 등을 유출, 조작할 수 있다.

3.2 스마트카드 절취를 통한 공격(Stolen smart card attack)

사용자가 스마트카드를 이용하여 사용자 인증을 수행할 때 스마트카드에 저장되어 있는 정보만으로는 인증을 완료할 수 없어야한다. 스마트카드는 사용자가 휴대하고 다니므로 분실의 위험성이 존재하기 때문에 스마트카드에 저장되어있는 정보로만 인증을 완료할 수 있으면 공격자들이 쉽게 악의적인 목적으로 스마트카드를 사용할 수 있게 된다.

3.3 상호인증(Mutual authentication)

전기 자동차에 대한 충전 인프라를 이용하는 사용자는 자신이 정상적인 사용자라는 것을 인증한 후 전력 서비스를 이용하게 된다. 만약 전력서비스를 이용할 때 인증이 이루어지지 않을 경우 악의적으로 전력 서비스를 이용하는 사용자가 증가할 수 있다. 또한 사용자 인증이 완료되어도 사용자와 통신을 주고받는 스마트미터가 정당하지 않을 경우 사용자의 정보가 유출 및 조작될 수 있으므로 사용자와 스마트미터 간의 상호 인증이 필요하다[11].

3.4 세션키 안전성(Security of session key)

공격자가 이전의 세션에서 사용한 세션키를 알아도 다른 세션에서 사용되는 세션키를 만들어 낼 수 없어야 한다. 만약 한 세션에서 사용된 세션키를 통해 다른 세션에서 사용하는 세션키를 만들어낼 수 있다면 사용자와 스마트미터 간의 통신에서 주고받는 정보들이 전부 노출되기 때문에 한 세션키를 이용하여 다른 세션키를 만들어 낼 수 없도록 해야 한다.

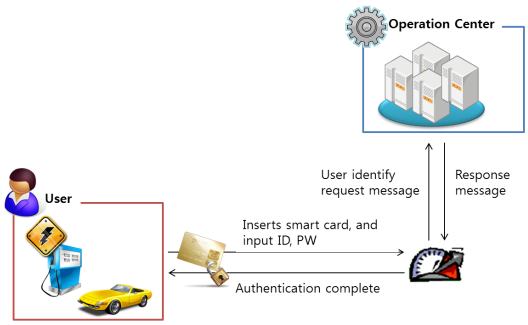
4. 전기 자동차 사용자 인증 스킴

스마트그리드 환경에서 전기 자동차는 충전을 위해 상황에 따라 각기 다른 곳에 위치해 있는 스마트미터에 접속하여 인증을 수행한 후 전력 서비스를 이용하는 구조로 되어있다. 본 논문은 스마트카드 및 동적 ID를 기반으로 한 인증 방식을 활용하였다.

본 논문에서 제안하는 방법은 각 가정에서 스마트미터에 사용자를 등록하거나 전기 충전 인프라를 이용할 때 사용자를 인증하기 위해 스마트카드를 활용한다. 또한 통신 과정에서 사용자 정보 노출을 방지하기 위해 동적 ID를 활용한다.

사용자는 전기 자동차 인프라 운영서버에서 등록절차를 통해 자신의 ID, PW를 등록하고 사용자 인증에 필요한 값을 저장한 스마트카드를 발급받는다. 이후 사용자가 전력 서비스를 이용하기 위해 가정, 마트, 기타 충전소 등의 충전 인프라에 있는 스마트미터에 접속한 후 자신의 ID, PW, 스마트카드를 이용하여 인증을 요청한다. 스마트 미터나 충전 인프라는 요청에 대한 정당성을 인증서버를 통해 확인하고 해당 사용자에 대한 인증을 완료한다.

다음 [Fig. 2]는 본 논문에서 제안하는 사용자 인증 방법에 대한 개념도를 나타낸다.



[Fig. 2] Overview of the proposed scheme

4.1 사용자 파라미터

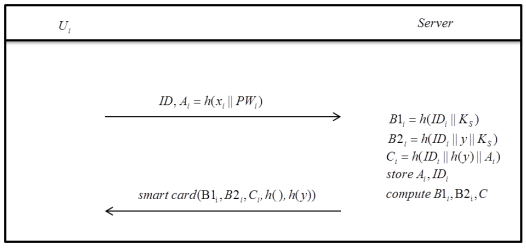
다음 <Table 1>은 본 논문에서 제안한 스킴에서 사용되는 파라미터에 대해 정리한 것이다.

〈Table 1〉 System parameter

Notation	Description
ID_i/PW_i	The ID/PW of electric vehicle user
y	The secret number of server
x_i	The secret number of user
K_S	The master key of server
$N_{i/j}$	The Nonce value of user/smart meter
T_i	The timestamp value of user
$SMID_i$	The Smart meter ID
CID_i	The dynamic ID of user
$h(\cdot)$	A one-way hash function
$\oplus$	Exclusive-or operation
$E_{P_S}(\cdot)/D_{R_S}(\cdot)$	
Encryption/decryption function of public key cryptosystem using key server's PU/PR	
$E_{P_{SM}}(\cdot)/D_{R_{SM}}(\cdot)$	
Encryption/decryption function of public key cryptosystem using key smart meter's PU/PR	

4.2 등록과정

등록과정은 전력을 이용하는 사용자가 사용자 인증을 위해 진행하는 절차이다. 사용자는 인증서버에게 안전한 경로를 통해서 스마트카드를 발급받는다. 이후 사용자는 인증서버로부터 발급받은 스마트카드를 이용하여 사용자 인증과정에 활용한다.



[Fig. 3] User registration phase

- Step 1. 사용자는 자신의 ID와 패스워드를 이용하여 A_i를 생성한다. 생성한 후 자신의 ID와 함께A_i를 서버에 전송한다.

$$A_i = h(x_i \| PW_i)$$

- Step 2. 서버는 사용자로부터 전송받은 A_i를 저장한다. 이후 사용자의 ID, A_i 이용하여 $B1_i$, $B2_i$, C_i를 생성한다. 생성된 값은 로그인 단계와 인증단계에서 사용자를 식별하기 위한 값으로 활용된다.

$$B1_i = h(ID_i \| K_S)$$
$$B2_i = h(ID_i \| y \| K_S)$$
$$C_i = h(ID_i \| h(y) \| A_i)$$

4.3 로그인 단계

사용자가 전기 자동차 충전 서비스를 이용하기 위해서는 사용자 인증을 거쳐야한다. 인증을 거치기 위해 사용자가 자신의 ID, PW, 스마트카드를 이용하여 로그인하는 단계이다.

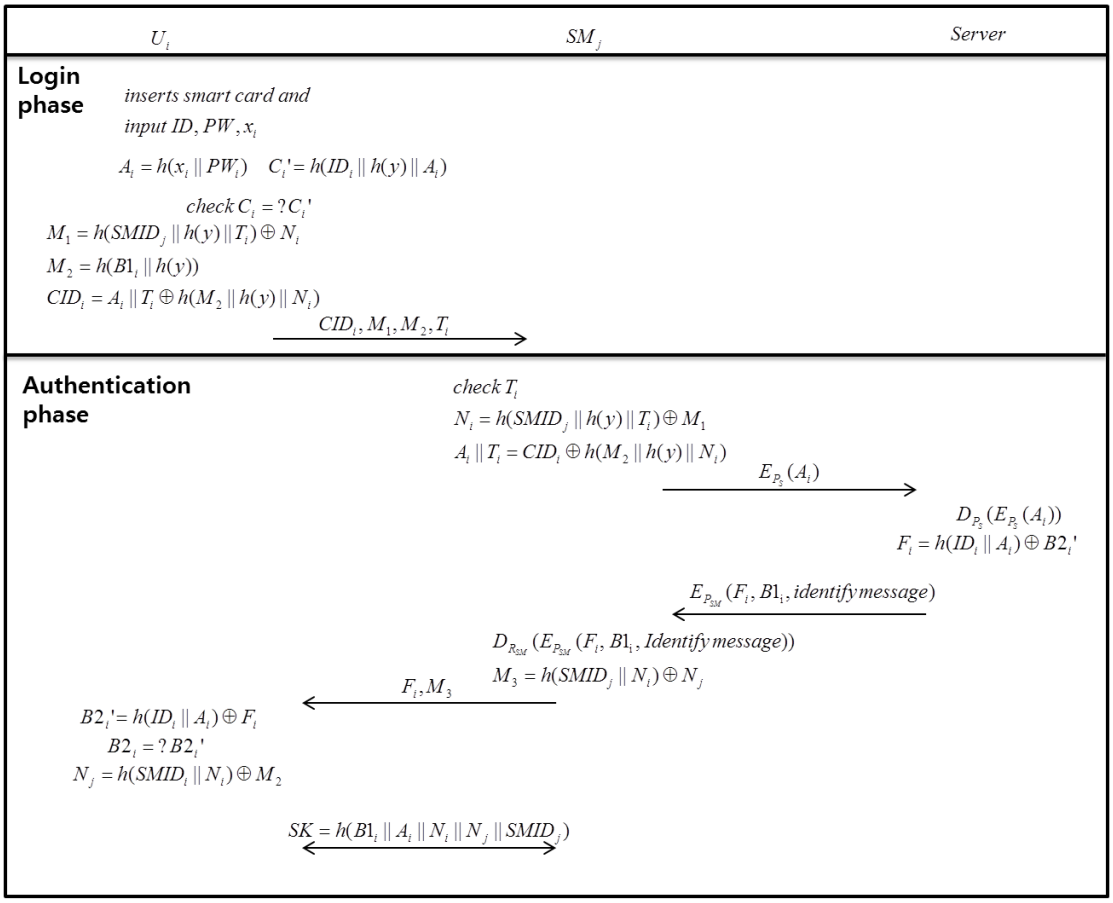
- Step 1. 사용자는 스마트카드를 삽입하고 자신의 ID_i, PW_i, x_i를 입력한다.

- Step 2. 사용자가 로그인하기 위해 사용자는 ID, PW를 입력한다. 사용자가 입력한 ID, PW를 이용하여 C_i'를 생성하고 스마트카드에 저장된 C_i와 비교하여 정상적인 사용자의 로그인 시도 여부를 확인한다.

$$A_i' = h(x_i \| PW_i)$$
$$C_i' = h(ID_i \| h(y) \| A_i)$$

- Step 3. Step 2에서 사용자가 정상적으로 로그인하게 되면 스마트미터에 자신을 인증하기 위한 값을 생성한다. 동적 ID인 CID_i와 M_1, M_2, T_i를 생성한다. M_1은 스마트미터가 CID_i에서 사용자를 판별 할 수 있는 값 A_i를 얻기 위해 필요한 값 N_i를 전송하는 목적으로 활용한다.

$$M_1 = h(SMID_j \| h(y) \| T_i) \oplus N_i$$
$$M_2 = h(B1_i \| h(y))$$
$$CID_i = A_i \| T_i \oplus h(M_2 \| h(y) \| N_i)$$



[Fig. 4] Login and authentication phase

4.4 사용자 인증 및 키 동의 단계

사용자가 로그인과정을 거친 후 자신이 정당한 사용자임을 인증하기 위해 수행하는 단계이다. 사용자가 동적 ID를 이용하여 자신을 인증하기 위한 값을 전송하면 스마트미터는 운영서버를 통해서 값을 인증하고 사용자에 대한 인증을 한다. 사용자 인증이 정상적으로 되면 스마트미터는 자신을 인증하기 위한 값을 전송한다. 인증이 정상적으로 이루어지면 사용자와 스마트미터는 세션키를 공유할 수 있다.

- Step 1. 사용자는 로그인후 생성한 CID_i, M_1, M_2, T_i를 스마트미터에게 전송한다.
- Step 2. 스마트미터는 사용자로부터 전송받은 CID_i, M_1, M_2, T_i를 이용하여 사용자를 인증한다. 스마트미터는 전송받은 타임스탬프 값 T_i를 확인한다. 이상이 없을 경우 스마트미터가 갖고 있는 정보인 $SMID_j$, $h(y)$와 T_i를 이용하여 M_1로부터 N_i를 얻는다. 얻은 N_i와 사용자로부터 전송받은 M_2를 이용하여 CID_i에서 사용자를 판별 할 수 있는 값인 $A_i \| T_i$를 얻는다. 스마트미터는 먼저 타임스탬프 값 T_i를 확인하고 이상이 없을 경우 A_i에 대해 정당한 사용자 여부를 검증하기 위해 A_i를 서버의 공개키로 암호화하여 서버로 확인을 요청한다.

$N_i = M_1 \oplus h(SMID_j || h(y) || T_i)$
$A_i || T_i = CID_i \oplus h(M_2 || h(y) || N_i)$
$E_{P_S}(A_i)$

· Step 3. 서버는 스마트미터로부터 전송받은 값 $E_{P_S}(A_i)$를 자신의 개인키로 복호화하여 A_i를 얻는다. 서버는 A_i를 검증하고 정상적인 사용자인지 여부를 판별해준다. 이후 등록 단계에서 해당 A_i를 갖는 사용자에게 발급해줬던 $B2_i = h(ID_i || y || K_{AS})$를 해당 사용자만 풀어 볼 수 있도록 하여 F_i를 생성한다.
$F_i = h(ID_i || A_i) \oplus B2_i'$

· Step 4. 서버는 사용자에게 스마트미터를 인증하기 위해 생성한 값 F_i와 세션키를 생성할 때 해당 사용자 고유의 값을 만들기 위한 $B1_i$, 사용자 판별 결과를 스마트미터의 공개키로 암호화하여 전송한다.
$E_{P_{SM_i}} = (F_i, B1_i, Identyfy\ message)$

· Step 5. 스마트미터는 서버로부터 전송받은 값을 개인키로 복호화화여 F_i, $B1_i$을 얻고 판별 결과를 확인한다. 이후 스마트미터는 세션키를 생성하기 위해 해당 세션에서만 사용하는 nonce 값 N_j을 생성한다. 스마트미터는 N_j을 안전하게 전송하기 위해 생성한 M_3와 F_i를 사용자에게 전송한다.
$M_3 = h(SMID_i || N_i) \oplus N_j$

· Step 6. 사용자는 스마트미터로부터 전송받은 F_i에서 $B2_i'$를 얻고 자신의 스마트카드에 저장되어 있는 $B2_i$ 값과 비교를 하여 스마트미터 인증을 완료한다. 인증 후 M_2 값에서 N_j을 얻어 세션키를 생성하고 스마트미터와의 통신에 이용한다,
$B2_i' = F_i \oplus h(ID_i || PW_i)$
$N_j = M_2 \oplus h(SMID_i || N_i)$
$SK = h(B1_i || A_i || N_i || N_j || SMID_i)$

〈Table 2〉 Security Analysis

	Security requirements	The proposed scheme
Replay attack	The value used to user authentication must be protected from replay attack.	Every time user connect to the session, CID_i is different. If attacker re-transmit CID_i and N_i, server can prevent to replay attack. Because user transmit timestamp to server($A_i \| T_i$).
Stolen smart card attack	The attacker can never complete authentication from stolen smart card.	If attacker steal smart card , attacker can't generate C_i. Because stolen smart card don't contain user's input value(ID, PW, x). Therefore, attacker can't start authentication phase.
Mutual authentication	Electric power service of electric vehicle required mutual authentication.	When user transmit CID_i to smart meter, smart meter get user authentication value A_i. Because A_i contain in dynamic ID value(CID_i). And smart meter use A for user authentication. If user authentication complete, smart meter transmit $B2_i$ of that user to user for smart meter authentication. Thus, the proposed scheme provide mutual authentication.
Security of session key	If attacker get previous session key, attacker can never generate next session key.	Session key SK_j generate using one-way hash function. Thus, attacker can't inference to session key SK. Also, the SK_j value changed every session by nonce value N_j. Therefore, attacker can never generate session key.

5. 안전성 분석

5.1 재전송 공격(Replay attack)

사용자를 스마트미터에 인증하기 위해 전송하는 값인 CID_i는 동적 ID로서 사용자가 세션에 연결할 때마다 랜덤 값인 N_i이 달라지기 때문에 같은 사용자라고 하여도 값이 달라진다. 또한 스마트미터가 CID_i로부터 사용자를 식별할 수 있는 값 A_i를 얻기위해 필요한 N_i는 M_1을 통해 얻기 때문에 직접적으로 노출되지 않는다.

만약 공격자가 CID_i, N_i를 얻어 다음 세션에 그대로 전송해도 사용자를 식별하는 값 A_i에 타임스탬프 값이 연접되어 있기 때문에 재전송 공격을 방지할 수 있다.

5.2 스마트카드 절취를 통한 공격(Stolen smart card attack)

사용자가 스마트카드를 분실한 후 공격자가 스마트카드에 저장되어 있는 값들을 얻을 수 있어도 인증에 필요한 값을 만들어 낼 수 없다. 공격자가 분실된 스마트카드에 저장되어 있는 값에서 사용자의 ID, PW, x를 알 수 없기 때문에 A_i를 만들 수 없다. A_i를 모르기 때문에 공격자는 결국 C_i를 만들 수 없어서 로그인을 할 수 없기 때문에 인증절차를 수행할 수 없다.

5.3 상호인증(Mutual authentication)

본 논문에서는 전기 자동차를 이용하는 사용자를 인증하기 위해 스마트카드와 동적 ID를 이용한다. 스마트미터는 디바이스의 계산능력상 모든 사용자의 정보를 담고 있을 수 없다. 이를 해결하기 위해 스마트미터와 서버가 통신하며 사용자에 대한 정당성을 판단한다.

스마트미터에 사용자를 인증할 때는 동적 ID인 CID_i를 이용하여 사용자 인증 값 A_i를 노출시키지 않기 때문에 안전하게 사용자 인증을 수행할 수 있다, 또한 사용자와 서버의 등록단계를 통해 서로 저장한 $B2_i$값으로 사용자에게 스마트미터에 대한 인증도 수행하기 때문에 상호인증이 수행된다.

5.4 세션키 안전성(Security of session key)

본 논문에서 제안한 스킴에서 생성되는 세션키 SK는 사용자의 정보 A_i와 인증단계에서 생성한 서버의 nonce 값 N_j를 이용하여 생성한다. 또한 세션키 SK는 $B1_i$, A_i, N_j, $SMID_j$를 연접하고 해쉬연산을 수행하여 생성하기 때문에 해쉬함수의 일방향성으로 인해 공격자가 역으로 값을 유추할 수 없다. 또한 세션마다 nonce 값 N_j가 달라진다. 따라서 공격자가 이전의 세션키를 알고 있어도 다음 세션에서 사용되는 키는 생성할 수 없다.

6. 결론

스마트그리드 환경에서 전기 자동차는 가정, 마트, 건물, 기타 충전소 등에서 충전을 할 수 있고 전기 자동차를 가정용 축전지로 활용하여 전력을 재판매 할 수 도 있다. 이와 같은 서비스가 이루어지기 위해서는 전기 자동차를 이용하는 사용자에 대한 사용자 인증이 이루어져야 한다. 사용자가 여러 장소에서 전기 자동차를 충전하기 위해 스마트미터에 연결할 때 사용자 인증이 이루어지지 않으면 악의적인 사용자에 의해 제3자가 충전서비스를 이용한 것처럼 사용되거나 전력 서비스 사용 요금의 불법적인 과금 등의 문제가 발생할 수 있다.

따라서 본 논문에서는 정당한 사용자만이 전기 자동차의 전력 서비스를 이용할 수 있게 하기 위해 스마트카드와 동적 ID를 기반으로 사용자 인증 방법을 제안했다. 스마트카드의 정보와 사용자의 ID, PW가 있어야만 로그인 단계를 거쳐야 인증을 요청할 수 있고 사용자와 스마트미터의 통신과정에서 동적 ID를 사용자를 인증할 수 있는 값을 안전하게 전송한다. 이로 인해 정당한 사용자만이 스마트미터에 인증을 할 수 있고 서비스를 이용할 수 있다.

REFERENCES

[1] NIST, Smart grid cyber security strategy and requirements. Aug. 2010. [Online]. Available: http://csrc.nist.gov/publications/nistir/ir7628/nistir-

7628_vol1.pdf
[2] NIST, Draft NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 2.0., 2011.
[3] Jaeduck Choi, Jungtaek Seo, Separate Networks and an Authentication Framwork in AMI for Secure Smart Grid, Journal of The Korea Institute of Information Security & Cryptology, Vol. 22, No. 3, 2012.
[4] J. Naruchiptparames, M.H Gunes, and C.Y Evrenosoglu, Secure Communications in the Smart Grid, IEEE Consumer Communications and Networking Conference (CCNC) 2011, pp. 1171-1175, 2011.
[5] NIST, Guidelines for Smart Grid Cyber Security, NISTIR 7628, 2010
[6] Jongmin Lee, Woohyuk Chang, Bang Chul Jung, Magnetic Induction Communication System for Electric Vehicle on Smart Grid, The Journal of Korea Information and Communications Society, Vol. 35, No. 9, 2010.
[7] Seong-ku Kang, Jung-taek Seo, An Analysis of the Security Threats and Security Requirements for Electric Vehicle Charging Infrastructure, Journal of The Korea Institute of Information Security & Cryptology, Vol. 22, No. 5, 2012.
[8] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, and Tadayoshi Kohno, Experimental Security Analysisof a Modern Automobile, IEEE Symposium on Security and Privacy, Oakland, CA, 2010.
[9] Xiong Li, Jian Ma, Wendong Wang, Yongping Xiong, Junsong Zhang, A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments, Mathematical and Computer Modelling, In Press, Corrected Proof, Available online 2012.
[10] R. Madhusudhan, R.C. Mittal, “Dynamic ID-based remote user password authentication schemes using smart cards: A review”, Journal of Network and Computer Applications, Vol. 35, Issue 4, pp. 1235-1248, 2012,
[11] Open Smart Grid Users Group, AMI System Security Requirements v1.01 2008. [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/14-AMI_System_Security_Requirements.pdf

정 수 영(Jung, Su-Young)

- 2012년 2월 : 순천향대학교 정보보호학과(공학사)
- 2012년 2월 ~ 현재 : 순천향대학교 정보보호학과 석사과정
- 관심분야 : 스마트그리드 보안, SNS 보안, 클라우드 컴퓨팅 보안
- E-Mail : syjung@sch.ac.kr

곽 진(Kwak, Jin)

- 2000년 8월 : 성균관대학교 생물기전공학과(공학사)
- 2003년 2월 : 성균관대학교 컴퓨터공학과(공학석사)
- 2006년 2월 : 성균관대학교 컴퓨터공학과(공학박사)
- 2007년 3월 ~ 현재 : 순천향대학교 정보보호학과 교수
- 관심분야 : 자동차 보안, 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안
- E-Mail : jkwak@sch.ac.kr