http://dx.doi.org/10.14400/JDC.2015.13.7.197

웹 사용자를 위한 통합 ID 인증 프로토콜에 관한 연구

신승수*, 한군희**
동명대학교 정보보호학과, 백석대학교 정보통신학부

A Study on Integrated ID Authentication Protocol for Web User

Seung-Soo Shin*, Kun-Hee Han**
Dept. of Information Security, Tongmyong University*
Division of Information & Communication Engineering, Baekseok University**

요 약 기존의 웹 인증방식은 주민등록번호를 이용하여 신용평가회사의 실명확인 데이터베이스를 통해서 인증 방식과 주민등록번호를 이용한 인증 방식을 개선한 대체인증 수단인 아이핀 인증방식 등이 있다. 기존 인증 방식을 개선하여 모든 웹에서 이용할 수 있는 통합 ID 인증 프로토콜을 제안한다. 제안한 인증 방식은 안전성을 높이기 위해서 사용자 검증값을 암호화하여 인증기관의 데이터베이스에 고유 식별번호로 저장한다. 그리고 해당 웹에 로그인하기 위해 필요한 패스워드는 일회용 난수를 인증기관으로부터 수신하기 때문에 사용자가 패스워드를 따로 기억할 필요가 없고 스마트폰을 사용하여 난수를 수신한다. 웹은 데이터베이스에 사용자의 개인정보를 저장하지 않기 때문에 개인정보 관리가 용이하며 사용자에게는 통합 ID 하나만 기억하고 매번 일회성 난수를 패스워드로 발급받아 여러 ID와 패스워드를 기억하고 관리하지 않아도 되는 편리성을 제공해 준다.

주제어 : 아이핀, 해시함수, 인증 프로토콜, 통합 아이디, 웹

Abstract Existing Web authentication method utilizes the resident registration number by credit rating agencies separating i-PIN authentication method which has been improved authentication using resident registration number via the real name confirmation database. By improving the existing authentication method, and it provides the available integrated ID authentication on Web. In order to enhance safety, the proposed authentication method by encrypting the user of the verification value, and stores the unique identifier in the database of the certificate authority. Then, the password required to log in to the Web is for receiving a disposable random from the certificate authority, the user does not need to remember a separate password and receives the random number by using the smart phone. It does not save the user's personal information in the database, and it is easy to management of personal information. Only the integration ID needs to be remembered with random number on every time. It doesn't need to use various IDs and passwords if you use this proposed authentication methods.

Key Words : i-PIN, Hash Function, Authentication Protocol, Integrated ID, Web

Received 8 May 2015, Revised 19 June 2015
Accepted 20 July 2015
Corresponding Author: Seung-Soo, Shin
(Dept. of Information Security, Tongmyong University)
Email: shinss@tu.ac.kr

ISSN: 1738-1916

1. 서론

최근에 기업 및 공공기관의 개인정보 대량 유출에 따른 보안사고가 지속적으로 발생하고 있으며 내부 정보 유출 방지를 위한 사용자 인증기술이 주목받고 있다[1]. 때문에 의료정보 보호를 위해 사용자의 의료 건강정보를 제 3자가 불법적으로 접근하는 것을 사전에 예방하기 위한 아이핀 기반의 유헬스케어 사용자 정보보호 프로토콜[2], 클라우드 컴퓨팅 환경에서의 사용자 인증을 위한 혼용 암호화방식을 이용한 사용자 인증 프로토콜[3] 그리고 청소년이 성인용 게임에 쉽게 접근할 수 없도록 PIN(Personal Identification Number)코드를 이용한 사용자 개별인증 프로토콜[4]등이 의료, 클라우드 컴퓨팅 그리고 IoT(Internet of Things) 등의 다양한 분야에서 제안되었다. 이러한 사용자 인증기술이 웹 분야에서도 필요하다.

웹에서는 사용자가 웹사이트를 통해 다양한 서비스를 제공받기 위해서 회원가입을 해야 한다. 즉, 면대면 방식으로 등록하던 오프라인 회원 서비스에서 비대면 방식으로 등록하는 온라인 회원 서비스를 제공하게 되었다. 따라서 회원등록을 위해서 사용자 인증이 필요하다. 주민등록번호를 이용한 기존의 인증방식은 사용자의 성명과 주민등록번호를 제공받아 실명을 확인하는 방식이다. 그러나 해킹 및 내부관리 소홀 등과 같은 다양한 원인으로 인해 주민등록번호가 대량으로 유출되는 사고가 계속 발생하고 있으며, 유출된 주민등록번호를 이용하여 도용과 같은 2차 피해가 발생되고 있다. 이러한 주민등록번호의 문제점으로 인해 대체수단이 필요해졌다[5,6,7]. 많은 웹사이트에서는 주민등록번호 인증방식의 데이터베이스를 사용하고 있다. 그래서 데이터베이스의 변경을 최소한으로 하여 주민등록번호를 이용하지 않고도 본인확인, 성인인증 등의 서비스가 가능한 아이핀을 개발하여 보급했다. 아이핀을 이용한 본인인증을 할 경우, 다른 수단을 통한 본인인증에 비해 주민등록번호의 남용을 줄여 개인정보 유출과 명의도용의 위협을 줄일 수 있다. 하지만 ID, 패스워드에 의존한 본인확인이기 때문에 ID와 패스워드가 탈취될 경우 위험하다[8,9,10].

기존 아이핀 인증방식은 고정된 값인 아이핀 ID와 패스워드로 이루어지므로 키로거, 트로이목마와 같은 악성코드 공격 또는 사회공학공격 등의 기법으로 인해 노출될 경우에 명의 도용과 개인정보유출로 악용될 수 있다. 또한, 아이핀 인증기관의 내부자의 불법유출이나 데이터베이스 해킹을 통해 집약된 개인정보의 유출이 발생할 경우 피해가 크다. 본 논문에서는 이러한 아이핀 인증의 취약점을 개선하기 위해 통합 ID 인증 프로토콜을 제안한다.

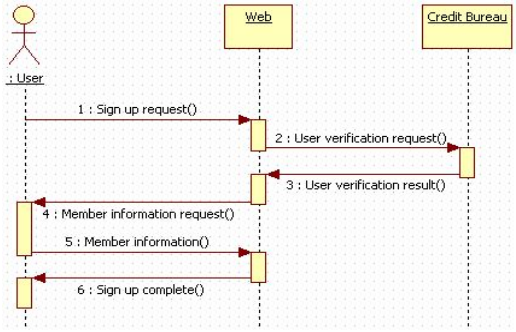
본 논문의 구성은 다음과 같다. 2장에서는 기존 인증방식인 주민등록번호를 이용한 인증방식과 아이핀을 이용한 인증방식에 대하여 알아본다. 3장에서는 기존 방식들을 개선한 통합 ID 인증 프로토콜을 제안한다. 4장에서는 제안한 인증 프로토콜의 정보들이 유출되었다는 가정하에 안전성을 분석하고 5장에서 결론을 맺는다.

2. 관련연구

본 장에서는 기존의 웹 인증방식인 주민등록번호를 이용하여 신용평가회사의 실명확인 데이터베이스를 통해서 인증방식[11]과 주민등록번호를 이용한 인증방식을 개선한 대체인증 수단인 아이핀 인증방식[12]의 절차와 문제점에 대하여 알아본다.

2.1 주민등록번호를 이용한 인증방식

주민등록번호를 이용한 인증방식은 사용자가 이름과 주민등록번호를 웹에 전송하면, 웹은 이를 실명확인 서비스를 제공하는 신용정보회사에 전달한다. 신용정보회사는 실명확인 데이터베이스에서 수신한 이름과 주민등록번호가 일치하는지 조회를 한다. 조회 결과에 따라 'YES' 또는 'NO'의 결과 값만 웹에 전송한다[11]. 이 방식은 [Fig. 1]과 같은 절차로 진행된다.



[Fig. 1] Authentication process using resident registration number

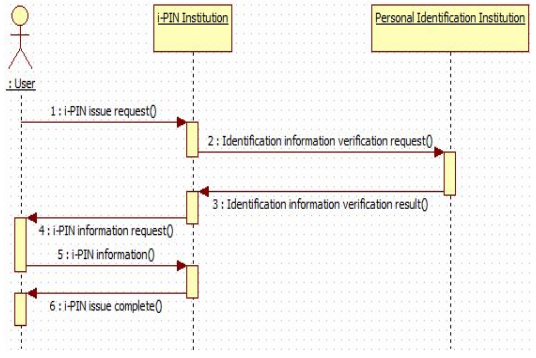
사용자는 회원등록을 하고자 하는 웹에 본인확인을 위해 이름, 주민등록번호를 전송하면 웹은 사용자의 이름과 주민등록번호를 검증하기 위해 신용정보회사에게 전송한다. 신용정보회사는 수신한 이름과 주민등록번호를 데이터베이스에서 조회한 결과를 웹에 전송한다. 그리고 웹은 사용자 확인이 완료되면 회원가입을 위한 회원정보를 사용자에게 요청한다. 사용자는 웹에서 사용할 ID와 패스워드 등을 포함한 회원정보를 전송한다. 웹은 사용자가 보내온 회원정보를 데이터베이스에 저장하고 회원가입을 사용자에게 전송한다.

2.2 아이핀을 이용한 인증방식

개인정보 유출 사고가 잦아지면서 주민등록번호의 문제점이 부각되어 대체수단으로 만들어진 아이핀을 이용한 인증방식을 사용한다. 아이핀을 이용한 인증은 아이핀을 발급하는 과정과 발급된 아이핀을 이용해 웹에서 인증하는 과정으로 이루어진다.

2.2.1 아이핀 발급과정

아이핀 발급과정은 다음 [Fig. 2]와 같은 절차로 진행된다.

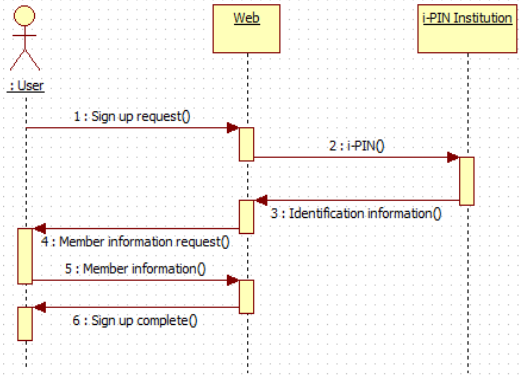


[Fig. 2] i-PIN issue

사용자는 아이핀을 발급 받기 위해 본인확인 정보(공인 인증서, 전화번호, 계좌정보 등) 중 하나를 선택하여 아이핀 인증기관에게 전송한다. 아이핀 인증기관은 수신한 사용자의 본인확인 정보를 확인할 수 있는 본인확인기관에게 사용자의 검증을 요청한다. 본인확인기관은 사용자의 본인확인 정보 조회 결과를 아이핀 인증기관에게 전송하고 본인확인이 완료되면 아이핀 인증기관은 사용자에게 아이핀 계정으로 사용할 ID와 패스워드, E-mail 등의 아이핀 정보를 요청한다. 사용자는 아이핀 인증기관에게 아이핀 정보를 전송한다. 아이핀 인증기관은 사용자로부터 수신한 아이핀 정보를 데이터베이스에 저장하고 아이핀 발급이 완료됨을 사용자에게 알린다.

2.2.2 아이핀 인증과정

아이핀 인증과정은 다음 [Fig. 3]과 같은 절차로 진행된다.



[Fig. 3] i-PIN Authentication

사용자는 회원가입을 하고자 하는 웹에 회원가입을 신청하고 아이핀 인증기관에서 제공한 아이핀 로그인 창에 로그인을 한다. 사용자가 입력한 아이핀 ID와 패스워드의 정보는 아이핀 인증기관의 데이터베이스에서 조회하여 본인확인 정보를 웹으로 전송한다. 웹은 사용자가 사용할 ID와 패스워드 등의 회원정보를 사용자에게 요청한다. 웹은 사용자로부터 수신한 회원정보를 데이터베이스에 저장하고 회원가입이 완료되었음을 사용자에게 알린다.

2.3 기존 방식의 문제점 분석

주민등록번호를 이용한 인증은 반드시 주민등록번호가 이용된다. 주민등록번호에는 출생지, 성별, 생년월일 등 필요 이상의 개인정보들을 기반으로 구성되어 있고 변경 및 갱신이 어려워 유출이 일어날 경우 지속적으로 도용이 발생한다. 또한 모든 공공기관, 기업, 민간기구 등에서 사용자의 식별을 주민등록번호로 처리하기 때문에

파급력이 크다. 주민등록번호는 마지막 자리의 숫자인 오류검증번호만 검증하면 가짜 주민등록번호를 생성할 수 있는 취약한 위조검증 체계를 가지고 있으며 주민등록번호 자체에 대한 유효성 검사만을 거치는 웹에서 위조 주민등록번호를 이용할 수 있는 문제가 있다. 즉 실명확인만을 수행할 뿐 실제로 사용자가 해당 성명과 주민등록번호의 주체가 맞는지 인증되지 않는다. 그러므로 실명인증이 필요하다[11,13,14].

이러한 주민등록번호의 문제점들을 개선하기 위해 아이핀 방식이 도입되었다. 그러나 아이핀을 이용하기 위해 아이핀 발급을 위한 추가적인 회원가입이 필요한데 이는 아이핀 ID와 패스워드 그리고 웹에서 사용할 ID와 패스워드를 함께 기억해야하는 불편함이 있다. 아이핀 인증기관은 아이핀을 발급하고 난 뒤 사용자의 이름, 주민등록번호, 본인확인 정보, 전자우편을 데이터베이스에 저장한다. 즉, 각 웹에 분산되어 저장 및 관리 되던 개인정보들이 한 곳에 저장되므로 아이핀 사용자들의 주민등록번호가 대량으로 보관된다. 그러므로 인증기관에서 개인정보 유출이 발생할 경우 대규모 피해가 예상된다. 아이핀 인증은 발급 받은 아이핀 계정으로 로그인하여 인증한다. 웹의 사용자는 아이핀 인증 외에 웹 이용을 위해 웹의 계정으로 한 번 더 로그인해야 하므로 두 차례 로그인을 하는 번거로운 방식이 될 수 있다. 때문에 기존의 인증방식들에 비하여 이용률의 저조함을 불러온다[15]. 그리고 아이핀 계정만으로 본인 인증이 가능하므로 아이핀 ID와 패스워드가 유출될 경우 누구나 다른 사람의 명의로 본인확인이 가능해진다. 다른 누군가 타인의 아이핀 ID와 패스워드로 인증을 시도할 경우 실시간으로 확인 할 수 없어 타인의 도용 여부를 알 수 없거나 뒤늦게 발견할 수 있다. 고정된 본인확인 정보를 이용하는 것도 주민등록번호의 범용성을 그대로 가지는 문제점이 있다.

주민등록번호 인증을 대체하기 위한 수단인 아이핀의 문제점을 해결하기 위해서 3장에서 통합 ID를 이용하여 모든 웹에서 이용할 수 있는 통합 ID 인증 프로토콜을 제안한다.

3. 웹 사용자를 위한 통합 ID 인증 프로토콜

본 장에서는 주민등록번호와 아이핀 인증방식의 취약점을 개선하기 위하여 하나의 ID를 사용하여 모든 웹에서 서비스를 이용할 수 있는 인증 프로토콜을 제안한다. 제안한 인증프로토콜은 안전성을 높이기 위해서 사용자 검증값을 암호화하여 인증기관의 데이터베이스에 고유식별번호로 저장한다. 그리고 해당 웹에 로그인하기 위해 필요한 패스워드는 일회용 난수를 인증기관으로부터 수신하기 때문에 사용자가 패스워드를 따로 기억할 필요가 없고 스마트폰을 사용하여 난수를 수신한다.

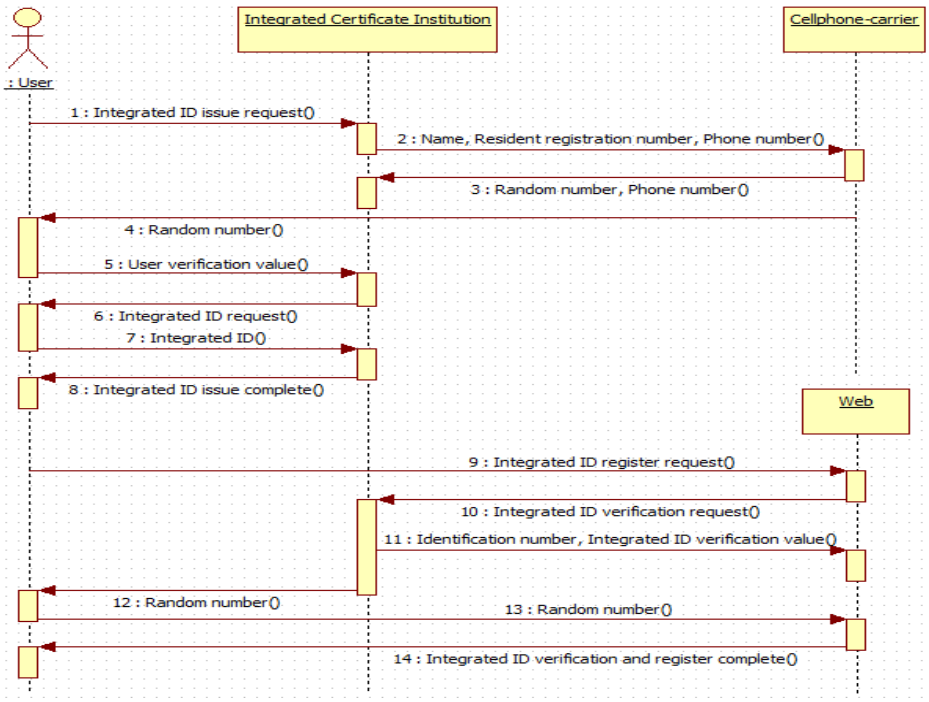
3.1 통합 ID 등록 및 인증에 관한 시퀀스 다이어그램

[Fig. 4]는 사용자가 인증기관에 통합 ID를 등록하는 과정과 서비스를 이용하고자 하는 웹에서 통합 ID를 인증하는 과정에 관한 시퀀스 다이어그램이다. 시퀀스 다이어그램에서 사용자의 통합 ID 등록과정은 ①~⑧까지의 단계이며, 웹에서 사용자의 통합 ID 인증과정은 ⑨~⑭까지의 단계이다.

3.1.1 통합 ID 등록과정

사용자는 모든 웹에서 사용할 통합 ID를 발급받기 위해 이름, 주민등록번호의 해시값 그리고 전화번호의 해시값을 인증기관에 전송한다. 인증기관은 사용자가 정당한 사용자인지를 확인하기 위해 이동통신사에게 이름, 주민등록번호의 해시값 그리고 전화번호의 해시값을 전송하여 사용자 본인 확인을 요청한다. 이동통신사는 인증기관으로부터 수신한 정보들로 데이터베이스에서 사용자를 조회하여 일치여부를 검사한다. 일치할 경우, 이동통신사는 사용자 검증값을 생성할 때 필요한 난수의 해시값과 전화번호를 인증기관에게 전송하고 검증값을 생성할 때 필요한 난수를 사용자에게 SMS로 전송한다. 사용자는 사용자 검증값(주민등록번호 해시값과 난수의 해시값으로부터 생성한 값)을 인증기관에게 전송한다.

인증기관은 사용자로부터 수신한 주민등록번호의 해시값과 이동통신사로부터 수신한 난수의 해시값을 이용하여 사용자 검증값을 생성, 사용자로부터 수신한 사용자 검증값과 비교한다. 일치할 경우, 모든 웹사이트에서 사용할 통합 ID를 사용자에게 요청한다. 사용자는 자신이 사용할 통합 ID를 인증기관에게 전송, 인증기관은 사용자의 통합 ID를 데이터베이스에 저장하고 통합 ID의 발급이 완료됨을 알린다.



[Fig. 4] Sequence diagram of Integrated ID register and authentication

3.1.2 통합 ID 인증과정

사용자가 인증기관에 등록한 통합 ID를 웹에서 사용하기 위해선 통합 ID 인증이 필요하다. 사용자는 자신의 통합 ID를 웹으로 전송한다. 웹은 사용자로부터 수신한 통합 ID를 인증기관으로 전송하여 인증을 요청한다. 인증기관은 통합 ID와 사용자의 고유 식별번호 그리고 통합 ID를 검증하기 위한 통합 ID 검증값(고유 식별번호의 해시값과 난수의 해시값으로부터 생성한 값)을 웹에게 전송하고 통합 ID 검증값을 생성할 때 필요한 난수를 사용자에게 SMS로 전송한다. 사용자는 난수의 해시값을 웹에게 전송한다. 웹은 인증기관으로부터 수신한 고유 식별번호의 해시값과 사용자로부터 수신한 난수의 해시값을 이용하여 통합 ID 검증값를 생성하고 인증기관으로부터 수신한 통합 ID 검증값과 생성한 통합 ID 검증값을 비교한다. 일치할 경우, 사용자의 통합 ID를 웹에 등록하고 사용자에게 전송한다.

3.2 통합 ID 인증 프로토콜

제안한 통합 ID 인증 프로토콜은 등록단계와 인증단계로 구성된다. 그리고 통합 ID 인증 프로토콜에서 사용할 표기법은 <Table 1>과 같이 정의한다. 통신채널간의 정보들은 해시하여 송수신이 이루어진다. 이동통신사는 사용자의 정보(주민등록번호, 전화번호 등)를 해시값으로 데이터베이스에 저장한다.

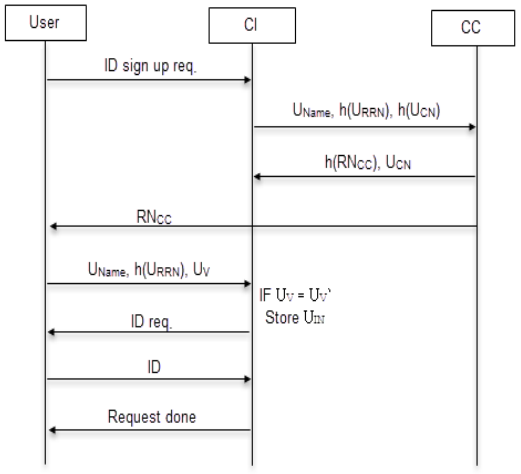
〈Table 1〉 Notation

Notation	Definition
CI	Integrated Certificate Institution
CC	Cell-phone Carrier
ID	Integrated ID
U_{Name}	User's Name
U_{RRN}	User's Resident Registration Number
U_{CN}	User's Cell-phone Number
h()	Hash Algorithm
$E_k()$	Encryption Algorithm
RN_{CC}	Cell-phone Carrier's Random Number
RN_{CI}	CI's Random Number
U_V	Verification value for User
ID_V	Verification value for Integrated ID
U_{IN}	User's Unique Identification Number

3.2.1 통합 ID 등록

통합 ID 등록과정에서 사용자는 U_{RRN}과 R_{NCC}를 각각

해시하여 XOR 연산한 값을 다시 해시하여 사용자 검증값 U_V을 생성하고 인증기관에게 전송한다. 인증기관은 수신한 사용자 검증값 U_V을 암호화하여 고유 식별번호로 사용한다. 통합 ID 등록과정은 [Fig. 5]와 같다.



[Fig. 5] Protocol of integrated ID register

- step 1 : 사용자는 CI에게 통합 ID 등록을 신청하기 위해 필요한 U_{Name}, $h(U_{RRN})$, $h(U_{CN})$을 전송한다.
- step 2 : CI는 U_{Name}, $h(U_{RRN})$ 그리고 $h(U_{CN})$을 CC에게 전송한다. CC는 수신한 정보를 데이터베이스에서 조회하여 정당한 사용자인지를 확인하고 CI에게 $h(RN_{CC})$과 U_{CN}를 전송하고 정당한 사용자에게 RN_{CC}를 SMS로 전송한다.
- step 3 : 사용자는 U_{Name}, $h(U_{RRN})$ 그리고 U_V를 CI에게 전송한다. U_V의 무결성을 검증하기 위해 CI는 사용자로부터 수신한 $h(U_{RRN})$과 CC로부터 수신한 $h(RN_{CC})$를 이용하여 U_V'를 생성한다. 그리고 $U_V = U_V$'이면 U_{IN}을 데이터베이스에 저장한다.

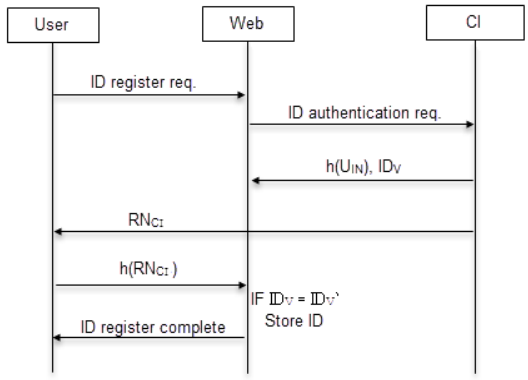
$$U_V = h(h(U_{RRN}) \oplus h(RN_{CC}))$$
$$U_V' = h(h(U_{RRN}) \oplus h(RN_{CC}))$$
$$U_{IN} = E_k(U_V)$$

- step 4 : 사용자는 ID를 CI에게 전송한다. CI는 수신한 사용자 ID를 데이터베이스에 저장한다.

Step 3에서 U_{IN}을 생성할 때 사용한 암호화 키는 U_V를 복호하기 위해 사용하는 것이 아니라 암호화 과정을 통하여 U_{IN}이라는 새로운 값을 생성하기 위한 것이므로 키를 저장할 필요가 없다. 암호화 키는 데이터베이스에 저장된 U_{IN}가 유출되어도 유출된 U_{IN}을 U_V로 복호하는 것을 어렵게 하기 위해서 사용자 별로 각각 다른 키를 사용하여 전수조사의 대상을 늘린다.

3.2.2 통합 ID 인증

사용자의 고유 식별번호 U_{IN}은 통합 ID를 검증하기 위한 검증값 ID_V을 생성하는 정보 중에 하나이다. 이 정보는 통신채널 상에서 송수신되지 않는다. 검증값 ID_V는 고유 식별번호를 해시한 값 $h(U_{IN})$을 사용하여 생성한다. 따라서 통합 ID를 등록할 때 사용한 $h(U_{RRN})$과 $h(RN_{CC})$를 알더라도 U_V로부터 $h(U_{IN})$의 정보를 알 수 없다. 통합 ID 인증과정의 프로토콜은 [Fig. 6]과 같다.



[Fig. 6] Protocol of integrated id Authentication

- step 1 : 사용자는 통합 ID를 웹에게 전송한다.
- step 2 : 웹은 사용자로부터 수신한 통합 ID를 CI에게 전송한다. CI는 통합 ID를 인증하기 위해 데이터베이스에서 조회한다. 정보가 일치할 경우, $h(U_{IN})$과 ID_V를 웹에게 전송하고 RN_{CI}를 사용자에게 SMS 전송한다.

$$ID_V = h(h(RN_{CI}) \oplus h(U_{IN}))$$

- step 3 : 사용자는 $h(RN_{CI})$를 웹에게 전송한다. 웹은 사용자로부터 수신한 $h(RN_{CI})$와 CI로부터 수신한 $h(U_{IN})$을 사용하여 ID_V'를 생성한다. $ID_V = ID_V$'이면 통합 ID는 정당한 ID이다.

$$ID_V' = h(h(RN_{CI}) \oplus h(U_{IN}))$$

3.2.3 사용자 패스워드 변경

웹에 인증된 통합 ID는 이후에 해당 웹에 로그인 할 때 사용한다. 그러므로 각각의 다른 웹에 통합 ID를 등록하면 서로 다른 웹에서도 동일한 ID를 이용할 수 있게 된다. 웹은 사용자가 로그인을 시도할 때마다 인증기관 CI에게 알려 인증기관이 생성한 난수 RN_{CI}를 패스워드로 사용할 수 있도록 사용자의 스마트폰으로 전송한다. 그리고 웹은 인증기관으로부터 $h(U_{IN})$과 ID_V를 제공받아 사용자가 입력한 RN_{CI}를 검증한다. 이 때 RN_{CI}는 일회성 난수를 이용하여 ID_V가 매번 변경되도록 한다.

4. 통합 ID 인증 프로토콜 분석

본 장에서는 통합 ID 인증 프로토콜에 대한 안전성을 분석한다. 안전성은 통신채널 상에서 전송되는 검증값들을 생성하는 정보와 검증값인 U_{RRN}, RN_{CC}, RN_{CI}, U_V, U_{IN}, ID_V들이 제 3자에게 유출되었다고 가정하고 등록 단계와 인증단계에서의 취득 정도를 나누어 생성할 수 있는 값과 그 값을 통해 해당 사용자의 정보를 알 수 있는지 분석한다.

4.1 등록단계에서 UV, h(URRN), h(RNCC), RNCC가 유출될 경우

등록단계에서 제 3자는 통신채널에서 U_V, $h(U_{RRN})$, $h(RN_{CC})$를 획득할 수 있고 SMS를 가로채어 RN_{CC}를 획득할 수 있다. 하지만 U_{RRN}은 해시하여 송수신되므로 통신채널 상에서 획득할 수 없기 때문에 주민등록번호가 공개되는 일은 없다. 제 3자는 획득한 $h(U_{RRN})$, $h(RN_{CC})$으로 U_V를 생성할 수 있다. U_V는 사용자를 검증하기 위한 값으로 실제 인증기관의 데이터베이스에는 U_V를 암호화한 U_{IN}을 사용자의 식별번호로 사용한다. 그렇기 때문에 U_V를 알아도 암호화 과정으로 해당 사용자의 U_{IN}을 알 수는 없다. 그리고 RN_{CC}를 가로채어도 RN_{CC}는 매번 변경되는 값이기 때문에 짧은 입력 시간을 두고 값을 변경하면 제 3자가 재사용하기 어렵다. 또한 U_V를 생성할 때 RN_{CC}가 사용되므로 모든 사용자가 등록과정을 수행할 때 마다 매번 다른 값이 되어서 유출되어도 다시 사용되지 않아 안전하다.

4.2 인증단계에서 IDV, h(RNCI), h(UIN), RNCI가 유출될 경우

인증단계에서 제 3자는 통신채널에서 ID_V, $h(RN_{CI})$, $h(UI_N)$를 획득할 수 있고 SMS를 가로채어 RN_{CI}를 획득할 수 있다. 하지만 UI_N은 해시값으로 송수신되므로 통신채널 상에서 획득할 수 없기 때문에 사용자 식별번호가 공개되는 일은 없다. 제 3자가 등록단계에서 사용한 U_V를 이미 획득한 상태여도 인증기관에 저장된 사용자 식별번호 UI_N은 U_V를 암호화하여 저장한 값이므로 암호화 키를 모르면 인증단계에서도 UI_N을 만들어 낼 수 없다. 그리고 제 3자는 획득한 $h(RN_{CI})$, $h(UI_N)$으로 ID_V를 생성할 수 있지만 RN_{CI}도 RN_{CC}와 마찬가지로 매번 변경되는 값이기 때문에 짧은 입력 시간을 두고 값을 변경하면 제 3자가 재사용하기 어렵다.

아이핀 인증기관에 집약된 주민등록번호가 유출될 경우 웹을 통한 주민등록번호 유출보다 더 큰 피해를 낳을 수 있기 때문에 제안한 인증 프로토콜을 사용하는 인증기관은 주민등록번호를 해시함수와 암호알고리즘을 이용하여 사용자의 고유 식별번호를 난수처럼 보이게 만들어 개인정보를 숨기고 안전성을 높였다. 아이핀을 발급받고 난 뒤, 아이핀 ID, 패스워드만으로 본인인증이 가능하므로 아이핀 정보가 유출될 경우 도용인증이 가능하지만 통합 ID를 이용하면 ID만 기억하고 패스워드는 일회용 난수로 사용자의 스마트폰을 통해 지급받기 때문에 안전하며 개인 식별번호만으로 검증하는 것이 아니라 난수를 이용해서 검증 값을 생성하므로 매번 다른 값으로 사용자를 인증 및 로그인한다. 그리고 인증 및 로그인을 시도할 경우, 사용자의 스마트폰으로 RN_{CI}가 발송되므로 본인 외의 누군가가 자신의 ID로 로그인을 시도하면 SMS 메시지를 통해 파악하기 용이하다. 때문에 제 3자의 계정 도용이 어렵다. 사용자는 모든 웹에서 동일한 ID를 이용하기 때문에 웹마다 계정을 기억할 필요가 없다.

5. 결론

본 논문에서 제안한 인증 프로토콜은 모든 웹에서 하나의 ID를 이용하여 서비스를 제공한다. 인증을 위한 정보들은 각 객체(사용자, 인증기관, 이동통신사)에서 각각 하나의 값들을 알고 있고 이 정보를 결합하여 검증값을

이용해 무결성을 가지며 정적인 패스워드가 아닌 매번 임의의 일회성 난수를 이용하여 인증을 수행함으로써 정적인 패스워드에 비해 안전성이 높다. 그리고 통신채널 상의 정보들은 검증 값과 검증 값을 생성하기 위한 정보 모두를 해시값으로 전송하므로 수정 및 변조에 대해 안전하다. 웹은 데이터베이스에 사용자의 개인정보를 저장하지 않기 때문에 개인정보 관리가 용이하며 사용자에게는 통합 ID 하나만 기억하고 매번 일회성 난수를 패스워드로 발급받아 여러 ID와 패스워드를 기억하고 관리하지 않아도 되는 편리성이 있다. 이러한 통합 ID 프로토콜을 웹 서비스 외에 다양한 IT 기술이 접목된 분야에서 응용하면 단일 식별자로 각 분야별 통합 인증을 가능하게 할 것이다.

REFERENCES

[1] Yoon-Su Jeong, Yong-Tae Kim, “Security Protocol of u-Healthcare User Information based on i-PIN”, Korean Institute of Information Technology, The Journal of Korean Institute of Information Technology, Vol.9, No.10, pp.133-141, 2011.

[2] Yoon-Su Jeong, Sang-Ho Lee, “User Authentication Protocol through Distributed Process for Cloud Environment”. Korea Institute of Information Security & Cryptology, Journal of The Korea Institute of Information Security & Cryptology, Vol.22, No.4, pp.841-849, 2012.

[3] Young Seop Ahn, Jeong Kyung Moon, Yeon-i Kang, Hwang Rae Kim, Koo Rack Park, Dong Hyun Kim, “An User Authentication Protocol for Cloud Computing”. Korean Society for Internet Information, Korean Society for Internet Information Academic Annual Conference Proceedings, pp.51-52, 2011.

[4] Yoon-Su Jeong, Yong-Tae Kim, “Personal Authentication Protocol of IPTV Game User using PIN Code”. The Korea Institute of Information and Communication Engineering, Journal of the Korea Institute of Information and Communication Engineering, Vol.15, No.12, pp.2670-2678, 2011.

[5] Kwang-Hee Choi, Jong-Chan Ahn, Gang-Shin Lee, Seung-Ho Ahn, “i-PIN 2.0 Service Framework for Replace RRN on The Internet”. Korea Institute of Information Security & Cryptology, Review of KIISC, Vol.20, No.6, pp.88-95, 2010.

[6] Chan-Joo Chung, Yoon-Jeong Kim, Jin-Won Kim, Kwang-Jin Park, “Technical Standard and Service Framework for Develop The Alternative(i-PIN) of RRN”, Korea Institute of Information Security & Cryptology, Review of KIISC, Vol.18, No.6, pp. 20-27, 2008.

[7] Jung-Dong Kim, Kwan-Tae Cho, Dong-Hoon Lee, “A Study of Online User Identification Based on One-Time Password with Guaranteeing Unlinkability”, Korea Institute of Information Security & Cryptology, Journal of The Korea Institute of Information Security & Cryptology, Vol.21, No.5, pp.129-139, 2011.

[8] Seung-Hyun Kim, Seok-Hyun Kim, Seung-Hun Jin, A Study on an Alternation of RNN and Access Control for Offline Environments by using I-PIN, Korea Information Processing Society, Vol.18, No.1, 2011.

[9] Java Card Technology, http://www.oracle.com /technetwork/java/javacard/overview/index.html

[10] KISA, http://www.signgate.com

[11] Chan-Joo Chung, Seung-Joo Kim, Dong-Ho Won, “A Study on The On-line Identification Plan by Using Financial Security OTP”, Korea Institute of Information Security & Cryptology, Review of KIISC, Vol.18, No.5, pp.73-83, 2008.

[12] Seung-Hyun Kim, Seok-Hyun Kim, Seung-Hun Jin, “A Study on an Alternation of RNN and Access Control for Offline Environments by using I-PIN”, Korea Information Processing Society, Korea Information Processing Society Conference, pp. 840-843, 2011.

[13] Hyung-Hyo Lee, “An Alternative Resident Registration Number System and Management Framework for Privacy Protection”, Korean Institute of Information Technology, The Journal of

Korean Institute of Information Technology, Vol.8, No.6, pp.49-58, 2010.

[14] Hyung-Hyo Lee, Hee-Man Park, Sang-Rae Cho, Seung-Hun Jin, "The Suggestion for A New On/Off-line Personal Identification Number System Offering The Privacy Safeguards", Korea Institute of Information Security & Cryptology, Review of KIISC, Vol.20, No.1, pp.74-87, 2010.

[15] In-Yong Jang, Heung-Youl Youm, "A Study on Activation Plan of i-PIN for Identification on The Internet", Korea Institute of Information Security & Cryptology, Review of KIISC, Vol.19, No.5, pp. 81-94, 2009.

신 승 수(Shin, Seung Soo)

- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 2월 : 충북대학교 컴퓨터공학과(공학박사)
- 2005년 ~ 현재 : 동명대학교 정보보호학과 부교수
- 관심분야 : 네트워크보안, USN, 스마트카드, 헬스케어보안.
- E-Mail : shinss@tu.ac.kr

한 군 희(Han, Kun Hee)

- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 멀티미디어, 유비쿼터스, DB보안, 암호 프로토콜/알고리즘
- E-Mail : hankh@bu.ac.kr