주민등록번호 유출을 방지하는 Duplicated Information 과 Connecting Information 방법론

양정훈*, 이희조
*고려대학교 컴퓨터 정보통신대학원 디지털 정보 미디어공학과
e-mail :austinnn@korea.ac.kr, heejo@korea.ac.kr

Duplicated Information and Connecting Information Method of Preventing the Leakage of Personal Information

Jung-Hoon Yang*, Heejo Lee
*Graduate School of Computer & Information Technology, Korea University

요 약

본 논문은 인터넷에서 주민등록번호가 유출 또는 도용되고 있는 문제점을 해결하기 위해 인터넷 사업자에게 이용자의 중복가입을 확인할 수 있는 방법 DI(Duplicated Information) 와 사업자간 동일 사용자를 식별하는 방법 CI(Connecting Information)을 제안한다. 인터넷 사업자가 이용자의 인터넷 사이트에 중복으로 가입하는 것을 확인 할 수 있는 정보를 제공하기 위한 중복 가입확인 정보 메시지 형식 규정을 제안하고, 인터넷 사업자가 타 인터넷 사업자와 연계 정보, 포인트 적립 등 제휴 서비스를 제공하기 위해 동일 이용자를 식별 할 수 있도록 연계 정보 메시지 형식 규격을 제안한다. 이용자의 개인 정보를 보호하는 수단을 제공하고 인터넷 사업자에게는 이용자의 유일성을 확인할 수 있는 수단을 제공할 것이다.

1. 서론

주민등록번호는 한번 부여 받으면 변경할 수 없다는 고정불변성, 1 인당 1 개씩만 부여되는 유일성, 생년월일, 성별 등의 유용한 개인정보를 숫자로 담고 있는 이용 편리성으로 국내 웹사이트에서 광범위하게 활용되고 있으며, 국내 인터넷 사이트의 60% 이상이 회원 가입 시 본인확인 등을 위해 주민등록번호를 수집, 저장 하고 있다. 하지만 최근 해킹, 내부관리 소홀, 마케팅 경재 심화 등 다양한 원인으로 인해 주민등록번호가 대량으로 유출 개인정보침해사고가 계속 발생하고 있다.[9]

본 논문은 주민등록번호를 유출을 방지하기 위해 I-PIN 의 기능인 인터넷 사용자에게 이용자의 중복가입을 확인할 수 있는 중복 가입 확인 정보 DI(Duplicated Information)와 사업자 간 동일 사용자를 식별할 수 있도록 연계 정보 CI(Connecting Information)의 서비스를 이용해 다양한 원인으로 주민등록번호가 대량으로 유출, 개인정보 침해사고가 계속 발생하고 있는 문제를 개선시킬 수 있으며, 유출된 주민등록번호를 이용하여 명의도용 등의 2 차적 피해로부터 웹사이트에서 무분별한 주민등록번호 수집, 저장이 인터넷상의 심각한 위험으로 확대되는 것을 방지 할 수 있다.

본 논문의 구성은 다음과 같다. 2 절에서는 관련연구로서 기존 본인인증 수단의 대한 정의와 문제점에 대해서 살펴본다. 3 절에서는 주민등록번호 유출을 방지 할 수 있는 DI(Duplicated Information) 과 CI(Connecting Information)의 대해서 정의할 것이다. 4 장에서는 기존 본인인증 대해서 비교 분석을 하였다. 마지막 5 장에서는 결론 및 향후 연구를 맺는다.

2. 기존 본인인증 기술

기존 본인인증 기술이 여러 가지가 있지만 대표적인 휴대전화, 공인인증서, I-PIN 기술에 대해서 살펴본다.[5][7]

2-1. 휴대전화 본인인증

휴대전화를 이용한 본인확인방법은 휴대전화를 개통할 때 수집된 개인정보를 기반으로 수행된다. 이동통신회사들은 전기통신사업법에 의거하여, 휴대전화의 사용요금을 위해 본인확인절차를 거친다. 이 때문에 온라인상에서 회원가입을 위해서 휴대전화를 이용한 본인확인절차가 사용이 가능하다.

웹 사이트에서 회원가입을 할 때 회원가입을 요청하는 사용자가 자신의 정보를 입력하였는지 본인확인이 필요하다. 이때, 휴대전화를 이용하여 본인확인을 한 후 회원가입 절차가 진행된다. 서비스 제공자는 사용자의 휴대전화를 요구한 후 수집된 휴대전화번호를 이용해 통신사에게 본인확인을 요청하게 된다. 통신사는 서비스 제공자의 요청에 의해 해당 휴대전화번호로 인증번호를 발송한다. 인증번호는 제한된 시

간 내에 서비스를 제공하는 웹 사이트에 입력되어야 하며, 시간 내에 인증번호가 입력되면 휴대전화를 소유한 사람이 사용자임을 확인하게 된다. 통신사는 확인된 사용자의 유효 값을 서비스 제공자에게 전송하고, 서비스제공자는 서비스를 계속해 제공한다.

2-2. 공인인증서 본인인증

공인인증서는 공개키 기반 구조 기반으로 공개 키에 소유자 정보를 추가하여 만들어진 일종의 전자신분증이다, 공인인증서의 기능으로는 전자서명을 통해 거래 내역의 위, 변조 방지 및 부인방지, 거래자 신원 식별등을 보장 등이 있으며 이를 통해 안전하게 거래할 수 있도록 지원하고 있다.

공인인증서의 기능으로는 전자서명을 통해 거래내역의 위 변조 방지 및 부인방지, 거래자 신원식별 등을 보장 등이 있으며 이를 통해 안전하게 거래 할 수 있도록 지원하고 있다. 사용자는 먼저 공인인증기관에서 대면확인을 통해 공인인증서를 발급 받을 수 있도록 신청한 뒤 발급기관에서 자신이 공인인증서를 발급받는다. 발급받은 공인인증서를 통해 사용자 인증을 시도하게 되면 전자서명은 전자문서 등을 HASH 값으로 변환해 이를 서명자의 전자서명 생성키(개인키)로 암호화 하여 전송하는 것이며 이를 전달받은 거래자는 전자서명 검증키(공개키)를 이용해 복호화 하고 전자문서를 HASH 한 값과 비교하여 전송받은 정보를 검증한다.

2-3. I-PIN 본인인증

I-PIN 을 발급받기 위해서 사용자는 I-PIN 을 발급하는 본인확인기관의 사이트나, I-PIN 이 도입된 사이트를 통해 발급 받을 수 있다. 사용자가 I-PIN 발급을 요청하면, 본인확인 기관에서는 사용자 식별정보를 입력 요청한다. 요청하는 식별정보는 사용자의 성명과 주민등록번호가 있고, I-PIN 을 이용하기 위한 ID 와 Password 도 함께 입력한다. 이 후 발급기관은 신원확인 정보를 요청하는데, 신원확인 방법에는 대면확인, 공인인증서, 휴대폰 등이 있으며, 사용자는 이 중 하나를 선택하여 신원을 확인을 받을 수 있다. 신원확인까지 완료되면, 본인확인기관에서는 사용자 식별정보와 신원 확인정보를 이용하여 사용자를 확인하고, 발급을 완료한다.

I-PIN 을 발급받은 사용자는 웹 사이트에 I-PIN 을 이용하여 본인확인을 할 수 있다. 사용자는 웹 사이트의 서비스를 제공받기 위해 회원가입 요청을 하면, 웹 사이트는 본인확인을 위해 본인확인기관의 I-PIN 인증을 요청한다. 본인확인 기관은 팝업 창을 통해 I-PIN 인증 창을 사용자에게 제공한다. 사용자는 I-PIN 인증 화면에 I-PIN 가입 시 등록한 ID 와 Password 를 입력하면 본인확인 기관에서 ID 와 Password 를 확인하고, 그에 해당 하는 결과 값을 웹 사이트에 제공하여 사용자가 웹 사이트에 가입 할 수 있도록 한다.

3. 주민등록번호 유출 방지- DI, CI 활용

주민등록번호를 유출을 방지하기 위해 인터넷 사용자에게 이용자의 중복 가입을 확인할 수 있는 중복가입 확인 정보 DI(Duplicated Information)와 사업자 간 동일 사용자를 식별할 수 있도록 연계 정보 CI(Connecting Information)의 서비스를 이용해 다양한 원인으로 주민등록번호가 대량으로 유출, 개인정보 침해사고가 계속 발생하고 있는 문제를 개선시킬 수 있다.

3-1. DI(Duplicated Information) - 중복 가입 확인 정보

인터넷 사업자가 본인 확인 정보의 유효성 확인 요청 또는 이용자의 본인 확인 정보를 인터넷사업자에게 전달하도록 요청하는 경우에 중복 가입 확인 정보를 함께 인터넷 사업자에게 제공한다.

본인 확인 기관은 인터넷 사업자로부터 본인 확인 정보 유효성 확인 요청을 받은 경우 또는 이용자의 본인 확인 정보를 인터넷 사업자에게 전달하도록 요청하는 경우 중복 가입 확인 정보를 생성하여 인터넷 사업자에게 함께 제공한다. 위의 각각의 경우에 인터넷 사업자의 사이트 식별 번호는 반드시 본인확인 기관에 전달되어야 한다. 본인 확인 기관은 중복 가입 확인 정보를 아래의 생성 절차에 따라 생성하여 인터넷 사업자에게 제공해야 한다.[2]

- 본인 확인 기관은 이용자의 주민등록번호(RN)와 요청 시 전달 받은 웹사이트 식별 정보(SI)를 연접하여 안전한 해시 함수에 입력하여 해시 값을 얻는다.

$$Temp = H(RN \| SI)$$

- 본인 확인 기관 간 공유 비밀 정보(SK)를 키 값으로 해시 값($Temp$)를 안전한 해수 함수에 입력하여 해시 기반 메시지 인증 코드(HMAC) 값을 생성하여 중복 가입 확인 정보(DI)를 얻는다

$$DI = HMAC_{SK}(Temp)$$

본인 확인 기관은 위의 절차에 따라 생성된 중복가입 확인 정보, 본인 확인 정보 소유자의 실명(UN) 및 본인 확인 정보를 인터넷 사업자에게 전달한다. 본인 확인 기관에서 전달받은 중복 가입 확인 정보의 값을 검증 하는 부분이다.

- 인터넷 사업자는 본인 확인 기관으로부터 전달받은 본인 확인 정보 소유자의 실명(UN)에 해당하는 가입자가 있는지 회원 데이터베이스를 검색한다[4]

- 회원 데이터베이스 검색결과 동일한 실명을 갖는 가입자가 없다면 본인 확인 정보와 중복 가입 확인 정보(DI)를 이용하여 신규 가입 절차를 수행한다.

- 회원 데이터베이스 검색 결과 동일한 실명을 갖는 가입자 동일한 실명을 갖는 가입자 수가 있다면 해당 가입자의 중복 가입 확인 정보(DI_i, $1 \le i \le s$)와 본인 확인 기관으로부터 전달 받은 중복 가입 확인 정보(DI)를 비교한다

- 동일한 중복 가입 확인 정보를 갖는 가입자가 있다면 해당 가입자의 아이디로 가입되어 있어 신규 가입 절차를 중단한다는 메시지를 가입자에게 보여준다.

- 동일한 중복 가입 확인 정보를 갖는 가입자가 없다면 본인 확인 정보와 중복 가입 확인 정보를 이용하여 신규 가입 절차를 수행한다

3-2 CI(Connecting Information) – 연계 정보

인터넷 사업자는 주민등록번호가 아닌 본인 확인 정보를 통해 이용자를 식별하기 때문에 이용자의 중복 가입이 가능하여, 인터넷 사업자가 이용자의 중복 가입 여부를 확인할 수 있는 표준으로 'KCS.KO-12.3800' 표준을 제정하고 있다. 본인 확인 기관은 인터넷 사업자에게 본인 확인 정보와 함께 중복 가입 확인 정보를 생성하여 전송함으로써 이용자의 중복 가입 여부를 'KCS.KO-120038'를 통해 확인 할 수 있다. 그러나 중복 가입 확인 정보는 이용자가 가입 하는 인터넷 사업자별고 서로 다른 값으로 생성되어 인터넷 사업자 간 연계 정보, 포인트 적립 등의 서비스 제휴가 불가능하여 인터넷 사업자 간 동일 이용자를 식별할 수 있는 연계 정보가 필요하다.[3]

본인 확인 기관은 본인 확인 정보와 함께 아래의 생성 절차에 따라 생성된 연계 정보를 인터넷 사업자에게 전송해야 한다.

- 본인 확인 기관은 이용자의 주민등록번호(RN)와 Padding 정보를 연접하고, 연계 정보 생성을 위해 본인 확인 기관 간 공유한 비밀 정보(S_A)와 배타적 논리합(XOR)한다

$$Temp = (RN \| Padding) \oplus S_A$$

- 연계 정보 생성을 위해 본인 확인 기관 간 공유된 비밀 키(SK)를 이용해 해시 값($Temp$)을 256 비트 이상의 출력 값을 갖는 안전한 해시 함수에 입력하여 해시 기반 메시지 인증코드(HMAC)값을 생성하여 연계 정보(CI)를 얻는다.

$$CI = HMAC_{sk}(Temp)$$

4. 기존 본인인증 기능 비교

(표. 1) 에서는 대표적인 본인인증수단인 휴대전화, 공인인증서, I-PIN 에 대한 기능 비교를 하고 있다. 현재 이용자들은 편리함과 간단함 때문에 휴대전화, 공인인증서를 많이 사용하고 있다. 하지만 공인인증서는 주민등록번호 대체수단으로는 부족한 부분이 많다고 볼 수 있다. 현재 이용자들은 편리함과 간단함 때문에 휴대전화, 공인인증서를 많이 사용하고 있다.

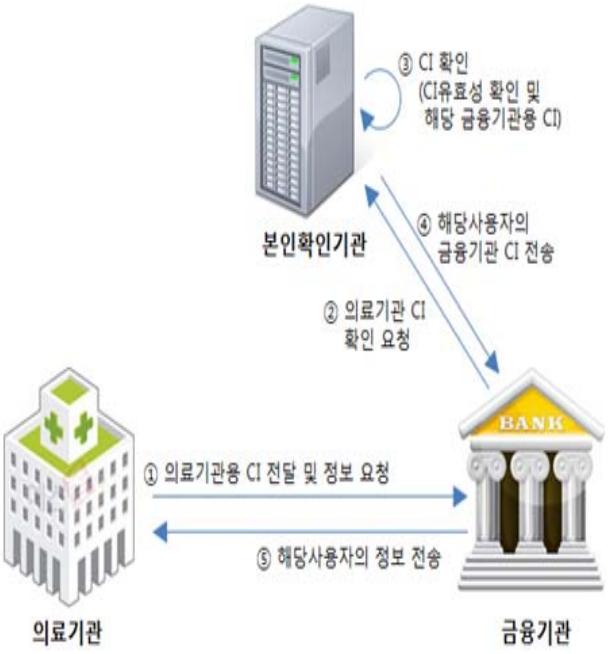
	휴대전화	공인인증서	I-PIN
본인확인 판단 정보	소유하고 있는 기기	비밀번호	ID, PW
인증 기술 분류	소유 기반	지식, 소유 기반	지식 기반
본인인증 기관에서 전달 받는 정보	DI, CI, 요청 번호, 요청 일시, 휴대전화 번호, 이동통신사, 생년월일, 내외국민 정보, 성별, 성명, 결과 코드, 결과 값	없음	DI, CI, 개인식별 번호, 이름, 생년월일, 나이, 성별, 내외국민 정보
존재성 판단 정보	휴대폰 번호, 성명	서명 값	DI , CI
개인 유출 시 방법	번호 변경	인증서 변경	재 발급
본인인증 값 변경 후 존재성 판단 유무	가능	불가능	가능
장점	1. 편리함 2. 간단함	1. 편리함 2. 간단함	1. 유출 시 사용자 정보 유추 불가 2. 누구나 발급 가능
단점	1. 휴대전화 미사용자 및 국외 거주자 문제 2. 대포 폰, 복제 폰 등 타인의 명의를 무단으로 사용하여 휴대전화 인증 사용 문제	1. 공인인증서 유출 문제 2. 전자거래를 하지 않은 사용자에게 보급률 저조 3. 저장매체의 보안 취약점	1. I-PIN 이용 방법의 대한 홍보 및 인식 부족

<표 1. 기존 본인인증 기능 비교>

하지만 공인인증서는 주민등록번호 대체수단으로는 부족한 부분이 많다고 볼 수 있다. 공인인증서 경우에는 중복체크는 가능하지만 사이트 간에 연계를 할 수가 없고 이력조회를 통해 도용을 추적 및 예방을 할 수가 없다. 반면휴대전화 와 I-PIN 경우에는 DI 와

CI 을 웹 사이트에 제공을 하기 때문에 웹 사이트 사용자 중복 체크 와 사이트 간의 연계를 할 수가 있고, 이력조회를 통해 도용을 추적 및 예방을 할 수가 있다. I-PIN 과 휴대전화를 이용하여 주민등록번호를 대신해서 본인인증을 받을 수 있지만 두 가지 본인인증에도 차이점은 있다. 휴대전화 경우에는 휴대전화 미사용자 및 국외 거주자 경우에는 휴대전화로 본인인증을 할 수 없다는 단점이 있고, 대포 폰, 복제 폰 등 타인의 명의를 무단으로 사용하여 휴대전화 인증을 할 수 있다는 문제가 있다.

본 논문은 주민등록번호 대신 본인인증을 받는 수단은 I-PIN 이 효율적이라고 볼 수 있다. I-PIN 을 통하여 DI 와 CI 를 활용 할 수도 있고, 다른 본인인증 수단과 달리 누구나 발급이 가능하며 I-PIN 사용자 정보가 유출이 되더라도 해당 정보를 유추 할 수가 없다는 장점이 있다. 하지만 I-PIN 도 앞으로 개선해야 할 부분은 있다. 아직까지 사용자로 하여금 I-PIN 이용 방법의 대한 인식이 부족하기 때문에 많은 홍보가 필요하다. 본 논문에서 제안하는 DI 와 CI 을 활용할 때도 고려 해야 하는 부분도 있다. 인터넷상으로 업종별로 다양한 CI 가 이용 된다면, 제한적으로 다른 업종의 본인인증 값은 서로 연결 되는 것을 허용되어야 한다. 정보통신 분야 본인인증 값과 의료분야의 본인인증 값은 평상시에는 서로 독립적으로 사용되지만, 정보통신 사이트와 의료 분야 사이트가 연결되어 또 다른 서비스를 사용자에게 제공 할 수 있다. 이를 위해서 서로 다르게 관리되는 사용자를 동일한 사용용자로 식별할 필요가 있다. 대표적으로, 세금 연말정산을 위해서는 다양한 분양에 사용되는 CI 를 이용해 하나의 사용자를 식별하기 위한 연결 서비스의 제공도 고려되어야 한다. 또한, 이를 위한 온라인 오프라인 연계 체계의 운영도 고려되어야 한다.[1]



(그림 4) 업종별 다른 CI 사용 시 연계 방안[7]

(그림 4)는 업종별 다른 CI 사용 시 연계 방안을 제시한 그림이다. 의료 기관은 의료 업종 CI 를 사용하며, 금융기관은 금융 업종 CI 을 사용한다. 각 업종간 연계가 필요할 시 본인확인기관을 통해 연계가 가능하다.

3- 결론 및 향후 연구

대부분의 홈페이지는 회원가입, 글쓰기 시 실명확인 방법으로 성명과 주민등록번호를 입력 받아 확인하고 있습니다. 이러한 실명인증 방법은 타인이 명의 도용이 가능하기 때문에 개인정보 침해사고가 발생할 수 있습니다. 타인의 명의 도용은 당사자의 피해 이외에도 경제, 사회적으로 범죄에 악용되고, 확대/재생산 되어 다수의 피해자를 양산해 낼 수 있습니다. 본 논문에서는 DI(Duplicated Information) 와 CI(Connecting Information) 이용자 같은 경우 본인의 개인정보가 도용 또는 유출이 의심되는 경우에는 폐기 후 신규로 재발급 받을 수 있으므로 개인정보 침해 가능성이 매우 낮아져 보다 안전하고 편리한 웹 사이트 이용이 가능해 질뿐 아니라 연계서비스를 통해 동일인 인식이 가능하며 포인트연계, 제휴서비스를 위해 개별 기업에서 별도의 비용을 투자하지 않아도 된다.

향후 연구로는 휴대폰본인확인서비스, 공인인증서 등 여러 본인 확인 수단과의 상호 연동 및 호환성 등 여러 본인 확인 수단과의 상호 연동 및 호환성을 높이는 노력이 요구되며 이에 대한 연구 및 분석이 필요하며, 다양한 보안 위협에 대한 여러 가지 대응 방안에 대하여 고려해 보아야 하겠다.

참고문헌

[1] 행정안전부 “정책 연구 용역 보고서 –업종별 주민등록번호 사용 현황에 따른 대체 수단 연구”, 2012
[2] 방송통신위원회 “KCS.KO-12.0038 서비스 중복 가입”, 2012
[3] 방송통신위원회 “KCS.KO-12.0170 서비스 연계 정보)”, 2012
[4] 이형효, “개인정보보호를 위한 주민등록번호 대체 수단에 대한 구현 취약점 분석”, 한국정보기술학회, 2010
[5] 장인용, 염흥열, “인터넷상의 본인확인수단인 I-PIN 의 활성화 방안 연구”, 정보보호학회, 2009
[6] 최윤성, 이윤호, 김승주, 원동호, “ 주민등록번호 대체수단에 대한 구현 취약점 분석”, 정보보호학회, 2007
[7] 박상환, “ 인터넷상의 주민번호 대체수단 안전성 확보기술 연구”, 고려대학교 석사학위 논문, 2010
[8] 윤덕중, “ 인터넷 본인 확인 제 도입에 따른 행정기관 홈페이지 운영방식 개선방안”, 숭실대학교 석사학위 논문, 2008
[9] 이영현, “ 개인정보 유출방지를 위한 개인식별 방법 연구”, 서울산업대 석사학위 논문, 2008