모바일 환경에서의 본인인증 동향

이호섭, 이환진, 전인경, 정현철
한국인터넷진흥원
e-mail:{leehosub, lhj79, ikjeun, hcjung}@kisa.or.kr

A Trend of Personal Identification over Mobile Environment

HoSub Lee, HwanJin Lee, InKyung Jeun, HyunCheol Jeong
Korea Internet & Security Agency

요 약

인터넷의 확산에 따라 온라인 뱅킹, 온라인 경매, 메신저 등과 같이 이전에는 상상할 수 없었던 사이버스페이스상의 서비스가 활성화되고 있으며, 사용자들은 다양한 서비스를 이용하기 위해 개인 정보를 제공하고 사용해야 한다. 그러나 이런 유/무선 통합 환경에 적합한 본인확인 정보의 관리 부재 및 오남용으로 많은 문제가 발생하고 있다. 따라서 본 논문에서는 본인 인증기술, 그 중에서도 모바일 환경에서의 인증 기술 및 적용 현황에 대해서 분석한다.

1. 서론

최근 참여와 공유라는 비전을 가진 웹 2.0의 등장은 사용자를 이전의 수동적인 정보 소비자에서 능동적인 정보 제공자로 변모시키고 있다. 이와 같은 환경에서 서비스를 받기 위해 사용자들은 개인 정보를 제공하고 사용해야 한다. 그러나 이런 유/무선 통합 환경에 적합한 본인확인 정보의 관리 부재 및 오남용으로 많은 문제가 발생하고 있다. 2005년 전 세계적으로 7억 1,400만 달러에 이르는 개인정보 도용 피해가 발생하고 있을 정도로 개인정보보호 및 본인확인 서비스는 사이버스페이스의 지속적인 발전을 위해 필수적으로 해결해야 할 요소가 되고 있다.

따라서, 본 논문에서는 모바일 환경에서의 인증 기술 및 적용 현황에 대해서 분석하였다.

본 논문은 2장에서 모바일 환경 본인 인증 기술에 대해 간략히 설명한다. 3장에서는 모바일 본인 인증 기술 적용 사례에 대해 기술하며, 4장에서 결론을 맺는다.

2. 모바일 환경에서의 본인인증 기술

모바일 환경에서의 본인을 확인할 수 있는 인증 기술로 모바일 OTP(One Time Password)[1], SMS 인증, 모바일 공인인증, PIN 인증 등이 있다.

2.1. 모바일 OTP

전용 OTP 토큰은 동적인 비밀번호만 전용으로 생성할 수 있다는 보안상 큰 장점에도 불구하고 사용자가 토큰을 별도 구입하여 휴대하여야 한다는 점에서 쉽게 대중화되지 못하는 요인이 되고 있다. 모바일 OTP는 사용자의 휴대 간편성을 높이고 항상 주머니에 가지고 다니는 휴대폰을 OTP 토큰으로 활용하여, 편의성 및 휴대성을 보완한 인증 기술이다.

2.2. SMS 인증

SMS 인증[2]은 이동통신사의 DB와 사용자가 입력한 정보를 대조하여 일치할 경우 일회용 인증번호를 발송하여 인증번호 입력 시 이를 대조하여 인증을 하는 기술로 기존 OTP에 비해 이동통신사의 DB와 대조하는 절차를 추가하여 보안성을 높인 인증 기술이다.

2.3. 모바일 공인인증

기존 공인인증서[3]는 파일 형태로 항상 휴대해야 하는 불편함을 보완한 방법으로서, 휴대폰 상에서 비밀번호를 입력하기 때문에 키보드 해킹을 통한 보안 사고를 사전에 예방할 수 있는 인증 기술이다.

2.4. PIN(Personal Identification Number) 인증

PIN코드 인증은 등록하고자 하는 사용처에 사전에 등록한 킷값을 대조하여 일치 여부를 판단하는 인증 방식으로 다양한 키 입력이 어려운 휴대폰 환경에서 널리 사용되어지는 인증 방식이다.

3. 모바일 본인인증 기술 적용 동향

3.1. 이동통신사

온라인 휴대폰 구매 : 공인 인증서, 신용카드 등을 이용하여 본인임을 인증하는 방식과 주민등록증 발급일자 혹은 운전면허 번호를 입력 후 주민등록번호 혹은 운전면허 번호가 신청자의 정보와 일치할 경우 SMS를 통해 인

증번호를 전송하여 인증하는 휴대폰 인증 방식을 이용하고 있다. 이 방법은 휴대폰 대리점까지 가야되는 불편함이 해소되지만, 제3자에 의한 공인인증서 유출이나 신분증 유출 복제 휴대폰 등에 의한 인증이 가능하여 대포 폰이나 휴대폰 대출에 악용될 소지가 있다.

성인인증 : 성인 콘텐츠를 사용 하기위해서는 사용자 본인임을 확인하는 주민등록 번호 입력을 통해 인증을 하며 이증 과정에서 성인 인증만을 위한 숫자로 된 비밀번호를 설정하게 된다. 이 방법은 1회 인증 이후에는 비밀번호 입력만으로 인증이 되므로 상대적으로 편의성이 뛰어나다. 그러나 비밀번호 유출등의 문제점이 예상된다.

온라인 결제 : 결제를 청구하고자하는 휴대폰의 가입자 주민번호와 통신사를 선택한 후 휴대폰 번호를 입력하여 승인 요청을 하면 인증업체는 해당 통신사에 데이터를 보내 해당 고객의 존재여부를 확인하여 존재할 경우 일회용 인증번호를 생성하여 SMS로 전송하여 인증번호가 일치할 경우 해당 통신사의 요금에 청구하는 형태로 구성되어있다. 이 방법은 인증 대기시간이 길며, 복제 폰이나 메신저를 통해 유출이 가능하고, 간편한 절차 때문에 대포폰이나 명의 도용에 의한 피해가 발생할 수 있다.

요금제/부가서비스 변경 : 휴대폰으로 고객센터에 접속 시 가입자의 주민번호 뒤 7자리 혹은 사업자등록번호 뒤 4자리 번호를 입력하면, 해당 단말기의 가입자 DB에 접근하여 일치하는지 여부를 가려 본인인증을 하는 방식이다. 이는 본인이 아닌 경우에도 주민등록 번호나 법인번호를 알고 있을 경우 인증이 가능하며, 사업자번호나 주민등록 번호의 경우 유출이 비교적 쉬운 보안적인 문제점을 가지고 있다.

3.2. 금융/증권사/카드사

거래내역 통보 SMS : 거래가 이루어지는 시점에 가입자 본인이 인증 받은 휴대폰의 번호로 거래의 내역을 안내하는 방식으로 거래 결과를 사용자에게 문자메시지로 알리기 때문에 잘못된 출금이나 제3자에 의한 출금 시 사후 조치가 가능하다. 그러나 거래가 발생한 이후에 안내하는 방식이기 때문에 사전에 해킹이나 문제 발생에 대한 예방이 불가능한 문제점이 있다.

키보드 보안 : 이는 해킹 툴에 의한 인증코드나 비밀번호의 유출을 예방할 수 있지만, 물리적인 해킹은 예방할 수 없고, 암호의 해독에 의한 데이터 유출 가능성이 있다.

공인인증서 : 공인인증서와 인증 암호를 통하여 인증하는 방식으로 공개키를 이용하여 암호를 해독하는 방식으로 인증서파일과 암호를 사용하는 방식이기 때문에 이중 보안요소를 제공한다. 그러나 네트워크상에서의 파일 가로채기와 키보드 해킹 툴을 이용한 인증 암호 유출의 가능성이 존재한다.

OTP : 인증번호를 생성하는 기기의 시간대별 비밀번호 생성 테이블을 서버에서 보관하고 있다 인증요청이 있는 시간에 기기에서 생성되어 나올 비밀번호 값을 사용자가 입력하는 비밀번호와 일치 여부를 대조하는 방식으로 비밀번호 값이 매 시간마다 변하기 때문에 상대적으로 안전하다. 또한 기기를 소유하고 있어야 하고 비밀번호 값이 일치해야 되기 때문에 2중 보안 요소를 충족한다. 그러나 제3자가 기기를 소유하고 있을 경우, 제3자에 의한 인증이 가능하며, 비밀번호를 입력하는 사용자가 본인인지 제3자인지에 대한 확인이 불가능하다.

3.3. 포털 사이트

I-PIN 인증 : 인증이 필요한 경우 공인된 인증기관의 인증 페이지를 호출하여 해당 인증기관에서 인증이 성공한 경우 인증기관에서 제공하는 회원정보를 전송 받는 방식으로 개인 정보를 웹사이트에 저장하지 않기 때문에 개인 정보에 유출을 예방할 수 있다. 그러나 웹사이트 별로 I-pin[4]인증기관이 상이하여 사용자가 가입하지 않은 인증기관의 경우 별도의 가입 절차가 필요하며, 사용자의 신용 거래 내역이 없을 경우 회원 가입에 제약이 따른다.

OTP 툴바 : 기존 ID Password 방식의 로그인 정보를 툴바가 저장하였다가 로그인이 필요한 경우 SMS OTP정보를 발생하여 로그인을 OTP로 대행하는 방식으로 일회용 패스워드를 사용하기 때문에 ID와 Password가 유출되어도 로그인이 불가하므로 보안이 강화되며, 일회용 비밀번호를 사용하기 때문에 인증 절차가 간소화 된다. 그러나 OTP 툴바가 설치되어있지 않은 PC에서는 로그인이 불가능 하다.

4. 결론

현재의 본인 인증 기술은 하나의 인증으로 여러 가지 서비스를 모두 인증하지 못하며, 각 서비스별 인증 방식이 다르기 때문에 인증 관련 시스템을 다양하게 구성 유지해야 한다. 그리고 동적인 비밀번호 방식이나 주민등록번호에 의한 인증의 경우 제3자에 의해 유출이 쉬운 문제점이 있으며, 주민등록번호의 경우 유출이 되었다 하더라도 수정이 어려운 문제점이 있다. 특히 제3자에 의한 중요정보 유출에 대한 대책이 필요하다.

참고문헌

[1] Schneier, B. "Applied Cryptography" 2nd Ed. Willey, 1995

[2] 김우경, 이경현, "SMS와 OTP 개념을 이용한 사용자 인증", 한국정보과학회 2004년도 가을 학술발표논문집, 제 32권, 제 2호(1), 2004

[3] 윤병남, 반형식, "공공분야의 정보보호-공공분야의 공인인증서비스-", 한국통신학회지 (정보통신), 제19권, 8호, 2002

[4] 최윤성, 이윤호, 김승주, 원동호, "주민등록번호 대체수단에 대한 구현 취약점 분석", 한국정보보호학회논문지, 제 17권, 2호, 2007