금융사기 피해 방지, 일회용 패스워드(OTP)로

글 김형자(과학칼럼니스트)

인터넷 뱅킹의 해킹사고와 전자금융거래에 대한 사용자들의 불안감이 높아지고 있다. 그와 함께 보안 대책의 목소리도 높아지고 있다. 그래서 등장한 기술이 '일회용 패스워드(OTP)'다. 2010년대 초반 인증방법 등급이 존재하던 시절, OTP는 전자금융거래에서 1등급으로 분류될 만큼 보안이 강력하다. 대체 OTP가 얼마나 대단한 것이기에 강력한 보안수단으로 작용하고 있는 것일까.

일회용 암호, 수학적으로 유추 불가능해

OTP는 'One Time Password'의 약자로, 일회용 비밀번호 생성기를 말한다. 고정된 패스워드 대신 무작위로 생성되는 일회용 패스워드로 사용자를 인증하는 방식이다. 패스워드 인증 방식에 보안카드도 있는데, 왜 굳이 OTP를 만든 것일까.

한마디로 보안 때문이다. 일반적인 아이디/패스워드를 사용하는 인증기법의 경우, 가장 우려되는 것이 패스워드의 노출이다. 우리가 흔히 쓰고 있는 보안카드는 수십 개의 고정된 패스워드가 반복되어 사용되는 방식이다. 사용자가 로그인 할 때마다 매번 같은 패스워드를 사용하다 보면 해킹이나 추측 등을 통해 유출될 수 있다. 또 두세 군데 은행을 이용하면서 은행별로 발급한 보안카드를 지갑에 몇 장씩 넣고 다니면 불편하면서도 불안하다.

OTP는 이와 같은 취약성을 보완하고, 보안을 강화하고자 도입된 시스템이다. 패스워드 도난 문제를 예방하는 것이 OTP의 목적이다. 만약 로그인을 할 때마다 서로 다른 패스워드가 사용된다면 어떨까. 패스워드 노출이라는 문제점이 사라지지 않을까.

OTP는 로그인 할 때마다 다른 패스워드를 사용하는 인증 기술이다. 로그인 할 때 매번 일회성 패스워드가 만들어지고, 한번 사용하고 난 패스워드는 폐기돼 재사용이 불가능하다. 이를테면 하루에 로그인을 10번 하면 10번 모두 새로운 패스워드가 생성된다. 그렇기에 다음 사용할 패스워드를 수학적으로 유추해내기 어렵다. 이것이 OTP의 장점이다.

만약 마지막 로그인 때 사용한 패스워드를 해킹 당했다고 하자. 그래도 염려 없다. 서버에는 이전의 로그인에 사용된 패스워드 값만 저장된다. 다시 로그인 할 때는 자동으로 패스워드가 변경된다. OTP가 패스워드 보안을 강화할 수 있는 이유다.

어떻게 이런 일이 가능할까. OTP는 대체 어떤 방식으로 패스워드를 생성하는 것일까. 또 은행은 사용자의 OTP에서 생성된 패스워드를 어떻게 알고 인증하는 것일까. OTP에는 아무런 통신 장치도 없는데 말이다.

OTP의 원리는 간단하다. 사용자와 은행이 일회용 패스워드가 산출하는 공식을 '공유'하는 것이다. OTP 단말기 안에는 패스워드를 만들어내는 생성기와 작은 시계가 내장되어 있다. OTP를 '시계가 내장된 하나의 전자계산기'라고 생각하면 이해하기 쉽다. 전자계산기

같은 역할을 하는 생성기 버튼을 사용자가 누르면 6자리의 패스워드가 출력되는데, OTP에 부여된 수학 공식을 통해 현재 시간을 투입 값으로 하여 6자리의 패스워드를 계산해낸다. 버튼을 누를 때마다 다른 패스워드가 나오는 것은 바로 누르는 시간이 다르기 때문이다. 보통 30초~1분에 한번씩 OTP를 생성한다.

사용자가 등록한 OTP의 패스워드 생성기는 거래 은행의 서버에도 똑같이 내장되어 있다. 따라서 OTP에서 사용자가 6자리 패스워드를 입력할 경우, 같은 시간 은행 서버에 만들어지는 패스워드와 일치하게 되면 거래가 시작되고 틀리면 서버가 알아서 취소한다.

OTP는 주로 금융권에서 온라인 뱅킹 등의 전자금융(인터넷 뱅킹, 모바일 뱅킹, 텔레뱅킹 등) 거래에 사용된다. OTP의 형태는 여러 가지인데, 현재 소형 단말기 모양의 토큰(token)형과 신용카드처럼 생긴 카드형이 대표적이다. 최근엔 스마트 OTP에 관심이 쏠리고 있다. 스마트 OTP는 NFC(근거리 무선통신)가 지원되는 스마트폰에 IC칩이 내장된 스마트 OTP를 접촉하면 IC칩에서 일회용 패스워드가 생성돼 OTP 번호가 자동으로 입력된다. 사용자가 패스워드를 직접 입력하지 않으면서도 보안성이 그대로 유지되는 새로운 기술이다. 스마트폰에 내장하는 방식이기 때문에 단말기를 들고 다니지 않아도 돼 편리하다.

OTP 통합인증 기술, 국내 및 국제 표준까지 확보

우리나라는 언제부터 OTP 서비스가 시작되었을까. 2007년 6월, 금융보안연구원(FSA)에서 운영하는 'OTP 통합인증센터'가 열리고부터다. 지금은 금융결제원에서 OTP 서비스를 주관하고 있다.

OTP 생성기는 금융회사마다 별도로 배포한다. 따라서 다수의 금융회사를 이용하는 사용자의 경우 다수의 OTP를 소지해야 하는 불편함이 따른다. 이에 한 개의 OTP 생성기로 다수의 금융회사에서 공동으로 사용할 수 있는 OTP 통합인증 서비스를 세계 최초로 도입했다. 예를 들어 자사에서 발급한 OTP는 '대체인증서버'를 통해 인증하고, 타행 등록 OTP는 통합인증센터를 통해 인증하는 방법으로 서비스가 가능하다.

또 2009년부터는 OTP 통합인증 서비스와 관련된 국내외 표준을 활발히 진행했다. 먼저 2009년 'OTP 통합인증 서비스 프레임워크(TTAK.KO-12.0128)'를 TTA 단체표준으로 제정했고, 2011년에는 해당 표준안이 국제전기통신연합 전기통신표준화부문(ITU-T) X.1153 국제표준으로 등록되었다. 국내 및 국제 표준까지 확보함으로써 대내외적으로 세계적 수준의 기술력을 인정받게 된 셈이다. 싱가포르에서는 2011년부터 OTP 통합인증 서비스 기반의 국가인증프레임워크(NAF)를 구축하고, 국가차원에서 전 국민을 대상으로 OTP 서비스를 제공하고 있다.

보안이 담보되지 않은 전자금융 서비스는 결국 사상누각에 불과하다. 그런 의미에서 OTP 통합인증 서비스는 1등급 보안 기술이다. 앞으로 전자금융 분야뿐 아니라 전자상거래, 의료 등 다양한 분야에서 활용도가 높아질 것으로 기대된다.