일회용 암호, OTP의 메커니즘과 표준

김준래 사이언스타임즈 객원기자

인터넷 뱅킹 사용이 익숙하지 않은 개인사업자 이 모(62) 씨는 최근 거래를 시작한 B사에 물품대금을 송금하려다 큰 낭패를 봤다. 그날까지 1500만 원을 송금하기로 약속을 했는데, 인터넷 뱅킹으로는 1000만 원 이상을 보낼 수 없었던 것이다.

이유를 몰라 은행에 전화를 하니 '보안 등급이 낮은 보안카드를 사용하고 있기 때문에 하루에 1000만 원 이상은 보낼 수 없다'라는 답변이 돌아왔다. 급한 마음에 보안등급을 올리려면 어떻게 해야 되느냐고 묻자 은행직원은 '가까운 은행 지점을 방문하여 기존 보안카드를 OTP로 바꾸면 된다'라고 알려줬다.

OTP에 대해 궁금해 할 틈도 없이 부랴부랴 은행을 찾은 이 씨는 보안카드를 변경한 끝에 무사히 송금을 마칠 수 있었다. 은행 문을 나서며 OTP를 만지작거리던 이 씨는 그제야 이 조그만 단말기에 대한 궁금증이 생겼다. 누르면 6자리 번호가 뜨는 이 단순한 기능의 단말기가 무엇이기에, 하루 송금금액을 수십 배나 높일 수 있는 것일까?

OTP 인증번호는 수학적 유추 불가능

'일회용 인증번호 생성기'라는 의미의 OTP(One Time Password)는 고정된 인증번호 대신 무작위로 생성되는 일회용 인증번호를 이용하는 사용자 인증 방식의 단말기다.

OTP는 미국의 벨 통신연구소가 세계 최초로 개발한 보안 시스템으로, 카드 뒷면에 인증번호가 적혀있는 기존 보안카드의 취약점을 극복하기 위해 도입되었다.

보안카드가 취약한 이유는 수십 개의 고정된 인증번호가 반복되어 사용되기 때문이다. 그렇게 반복되어 사용하다 보면 아무래도 노출될 가능성도 커진다는 것이 보안 전문가들의 설명이다.

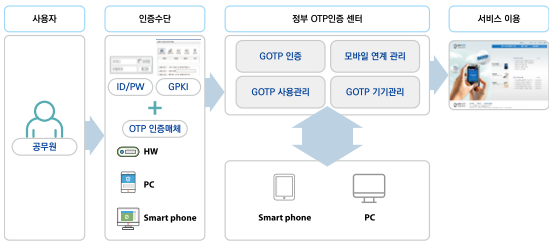
더군다나 보안카드의 경우는 사용자가 휴대폰으로 찍은 인증번호가 유출되는 사례가 빈번하게 발생하면서 인증 도구로서의 한계를 보여 왔다. 인증번호가 찍힌 이미지 파일이 메일이나 웹하드에서 돌아다니며 보안상의 취약점이 드러난 것이다.

이에 따라 벨 통신연구소 연구진은 자신들의 주력 사업인 통신을 활용한 보안 단말기 개발에 착수했고, 그 결과 인증번호를 한번 사용하고 버리는 방식의 OTP를 개발하였다.

OTP의 장점은 사용할 때마다 매번 인증번호가 변경되기 때문에 현재의 인증번호로부터 다음번 인증번호를 유추하는 것이 수학적으로 불가능하다는 것이다. 따라서 현재 사용한 인증번호를 해킹 등의 방법으로 입수했다 하더라도 이후에는 재사용이 불가능하다.

OTP 생성의 핵심 메커니즘은 거래하는 은행과 동일한 시간 내에서 암호화된 인증번호를 생성하는 것이다. 그리고 생성되는 인증번호는 매번 달라야 한다는 점도 중요하다.

이 같은 핵심 사항을 충족시키기 위해 OTP 단말기에는 고유한 인증번호를 만들어 내는 생



※출처: 정부 OTP 인증센터

[그림 1] 정부 OTP 인증센터 시스템 소개

성기와 작은 시계가 내장되어 있다. 따라서 사용자가 버튼을 누르면 작동시킨 시간에 맞춰 6자리의 인증번호로 나타나게 된다.

생성된 인증번호가 스마트폰의 모바일 뱅킹이나 컴퓨터의 인터넷 뱅킹 시 입력되면, 이후 은행 서버는 6자리 인증번호의 값이 맞게 입력되었는지를 확인하여 맞으면 거래가 시작된다. 물론 틀리면 거래가 취소된다.

다시 말해 사용자가 가진 OTP의 숫자 생성기가 거래은행의 서버에도 동일하게 탑재되어 있어서, 같은 시간대에 OTP에서 만들어진 인증번호가 은행 서버에서 만들어지는 인증번호와 일치하게 되면 인증에 성공하는 것이 핵심 메커니즘인 것이다.

OTP 통합인증 서비스 개발로 국내 기술의 표준화 주도

OTP 서비스를 처음 개발한 국가는 미국이지만, OTP를 보다 편리하게 사용할 수 있도록 다양한 서비스를 개발한 국가는 바로 우리나라다. 지난 2007년 금융보안연구원(현재 금융보안원)에서 'OTP 통합인증센터'를 설립할 때부터 다양한 응용 서비스를 개발하여 표준화를 이끌었다.

대표적 사례는 'OTP 통합인증 서비스'다. OTP 생성단말기는 금융회사마다 제조회사 및 모델이 다르다. 그러다보니 한 사람이 다수의 금융기관을 이용할 경우, 금융기관 별로 각각의 OTP를 소지해야만 했다. 많게는 7~8개의 OTP를 보유하는 경우도 생겼다.

이 같은 문제를 개선하기 위해 국내 금융기관들은 뜻을 모았고, 결국 하나의 OTP 생성단말기로 모든 금융기관들이 공동으로 사용할 수 있는 OTP 통합인증 서비스를 세계 최초로 상용화하는데 성공했다.

편리함과 신속함에 있어서 OTP 통합인증 서비스가 좋은 평가를 받자 이를 글로벌 표준으로 인정받기 위한 다양한 작업을 추진했다. 먼저 2009년에는 OTP 통합인증 서비스 프레임워크를 TTA 단체표준으로 신청하여 제정됐다.

또한 2년 뒤인 2011년에는 해당 표준안이 국제전기통신연합 전기통신표준화부문(ITU-T)에서 국제표준으로 등록되는 성과도 거뒀다. 이렇게 국내 및 국제 표준까지 확보함으로써 우리나라의 OTP 관련 기술력은 전 세계에서 인정받게 되었다.

대표적으로는 국내 OTP 통합인증 시스템을 벤치마킹한 싱가포르의 경우를 들 수 있다. 지난 2011년부터 국가인증프레임워크(NAF)를 구축하고 시민과 영주권자에게 무료로 OTP 토큰을 배포하면서 금융 및 공공서비스 등에서 활용하고 있다.

보안이 담보되지 않은 전자금융 서비스는 사실상 무용지물에 불과하다. 그런 점에서 볼 때 OTP 통합인증 서비스는 현존하는 최고의 표준 보안기술이라 할 수 있다. 전자금융 분야를 넘어 전자상거래 및 의료 등 다양한 분야에서 활용될 날이 멀지 않았다.

실제로 OTP 통합인증 표준 시스템은 최근 들어 아파트 홈네트워크 보안기술로도 검토되고 있어 주목을 끌고 있다. 홈네트워크 보안은 스마트홈 IoT 보안솔루션을 적용해 사이버 해킹을 원천적으로 차단하는 방식이다.