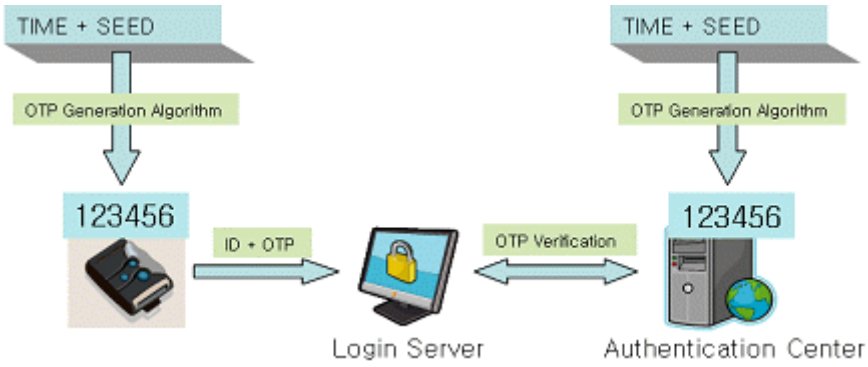
[공통기반] 당신의 금융 정보는 안전합니까?

인증이란 무엇이며 왜 필요한가?

우리나라는 인터넷 강국으로 불리우며 초고속 인터넷의 보급이나 사용, 무선 전화의 사용 등에서 어느 선진국 못지않은 훌륭한 인프라를 구축하고 있다. 작년 말에 전자 금융의 가입자 수도 이미 6,500 만 명을 넘어섰으며 이미 많은 사람들이 사용하고 있는 인터넷 뱅킹의 경우 유비쿼터스 시대에는 그 사용이 더욱 늘어날 것으로 생각된다. 그러나, 이러한 전자 금융 거래는 편리성 못지않게 불법 해킹, 인터넷 피싱 등의 피해에도 어느 정도 노출되어 있는 것이 사실이다. 우리나라에서는 2005년 5월 인터넷 뱅킹 사고, 2007년 1월 대형 은행 고객정보 유출, 2007년 2월 공인인증서 유출로 인한 은행 불법 인출 사건 등의 불법적 피해 사례가 늘어나고 있다. 이러한 사고로 인해 겪는 막대한 금전적 손해뿐만 아니라 이로 인해 겪는 정신적 피해 또한 증가하고 있는 실정이다. 따라서, 보안 위협을 막거나 최소화하기 위한 기술들이 소개되어 사용되고 있다. 주로 서비스를 이용하는 사용자가 정당한 사용자인지, 내가 접속한 사이트가 진짜로 존재하는 믿을만한 사이트인지 등에 대한 신뢰가 필요하다. 여러 가지 기술 중에 이러한 인증을 할 수 있는 기술을 소개하고 이의 장점과 단점 등에 대해 알아보도록 한다.

OTP를 사용하는 인증이란 무엇이며 어떻게 동작하는가?

안전한 통신을 하기 위해서는 암호화나 무결성과 같은 암호학적 기능 외에 가장 중요하게 생각되는 것이 사용자 인증이다. 올바른 사용자가 원하는 기능을 사용하도록 확인하는 것이 바로 인증 기능이다. 인증은 암호학적으로 그 목표를 달성할 수 있는 방법이 여러 가지 있는데 그 중 가장 많이 사용되는 방법이 우리가 인터넷 뱅킹이나 온라인 로그인에 사용하는 방식인 아이디/패스워드 방식이다. 그러나 이러한 방식은 추측이나 도청에 의해 쉽게 공격될 수 있다는 단점이 있다. 이러한 단점을 보완할 수 있는 기술이 바로 여기에서 소개하고자 하는 OTP(One Time Password) 기술이다. 이 기술은 사용자가 인증을 받고자 할 때 매번 새로운 패스워드를 생성해주는 방식으로 암호학에서는 가장 안전한 암호로 알려져 있다. 일반적인 패스워드는 도청이나 잘못된 사용으로 불법적으로 재사용될 위험이 있으나 OTP는 이미 사용된 패스워드는 사용하지 않으므로 이전 패스워드를 누군가가 알아냈다 하더라도 위험에서 벗어날 수 있다. 이러한 OTP 방식의 실제적인 사용은 크게 질의-응답 방식, 시간 동기화 방식, 이벤트 동기화 방식, 조합 방식 등의 네 가지로 나눌 수 있다. OTP 인증 과정을 설명하면 다음과 같다.



<그림 1> OTP 인증 과정

OTP 토큰은 인증 서버와 공유하고 있는 시간 정보와 SEED(서버와 OTP 토큰 사이에 공유된 비밀키, 카운터(사건의 횟수) 등)를 이용하여 OTP 생성 알고리즘을 통해 값을 생성하고 이 생성된 값을 아이디와 함께 login(로그인) 서버로 전송한다. 정보를 획득한 login 서버는 받은 정보를 인증 센터로 전달하여 인증 센터로 하여금 받은 정보를 확인하도록 한다. 인증 센터는 받은 아이디를 확인하고 해당되는 시간 정보와 SEED 정보를 OTP 토큰이 가지고 있는 정보와 동일한 정보를 이용하여 패스워드를 생성하여 이 값과 받은 정보가 일치하는지를 확인하여 login(로그인) 서버에 검증 결과를 알려준다. 이 때, OTP 토큰이라는 것이 필요하며 사전에 인증 센터와 동일한 알고리즘과 SEED 값을 분배 받아 사용자에게 지급된다.

우리나라에서의 OTP 활용 실태는 어떠한가?

이러한 OTP 인증 방법의 사용은 우리나라에서는 2007년 10월부터 모든 금융권에서 통합 OTP 인증 서비스가 개시되었다. 2006년 12월 OTP 연구회가 발족하여 활동하고 있으며 역시 2006년 12월에 금융보안연구원이 개원하여 전자 금융의 안전성 제고와 투자 효율성의 극대화를 목표로 OTP 통합 인증 센터를 구축하고 있다. 이러한 영향으로 우리 주변에서 OTP 토큰을 들고 다니는 금융권 사용자를 흔히 접할 수 있게 되었으며 이의 사용자는 앞으로 더욱 늘어날 전망이다.

OTP 기술의 국내외 표준화 동향은 어떠한가?

우리나라에서는 현재 OTP에 대한 표준화 움직임이 활발히 이루어지지 않고 있지만 '전자금융거래종합대책'에서 고객이 이용하는 거래 수단별로 보안 등급을 구분하고 보안 수준 1 등급을 맞추기 위해서는 OTP나 HSM(Hardware Security Module)의 도입을 시중 은행에 지시하고 있다. 그러나, 국제적으로는 미국의 RSA, VeriSign, IBM 등에 의해 활발히 표준화 작업이 진행되고 있다. OTP는 Bellcore 사가 최초로 기술을 개발하여 S/KEY라는 이름으로 IETF에서 표준화되었다. 그 후 RSA 진영과 OATH(Open AuTHentication) 진영으로 나뉘어 IETF를 중심으로 활발한 표준화 활동을 전개하고 있다.

미래 유비쿼터스 사회에서는 개인 정보보호를 얼마나 안전하게 관리하고 서비스를 제공하느

냐가 성공의 판단 잣대가 될 것이며 그 중심에 인증이 서 있다고 할 수 있다. 우리나라에서도 이러한 OTP 기술의 개발 못지않게 표준화에도 노력을 경주하여 국내 표준화뿐만 아니라 국제 표준화 작업에서 선도적인 역할을 수행할 수 있는 터전을 만들어야 한다. 이러한 노력의 일환으로 지난 10월 1일에서 4일까지 태국에서 열린 아·태 전기통신협회(ASTAP) 회의에서 OTP에 관한 기고문을 2건 제출하였으며 추후 이 회의의 연구 주제로 삼기로 하였다. 금융 등 관련 분야에서 꼭 필요한 기술로 산업에 미치는 영향이 지대하므로 향후 국내 표준안 작성과 이에 연계된 표준화 작업이 절실히 요구된다.

류희수 (경인교육대학교 수학교육과 교수, hsryu@ginue.ac.kr)