모바일 단말을 이용한 대역 외 서버인증 프레임워크(패스워드리스 기술표준 X.1280)

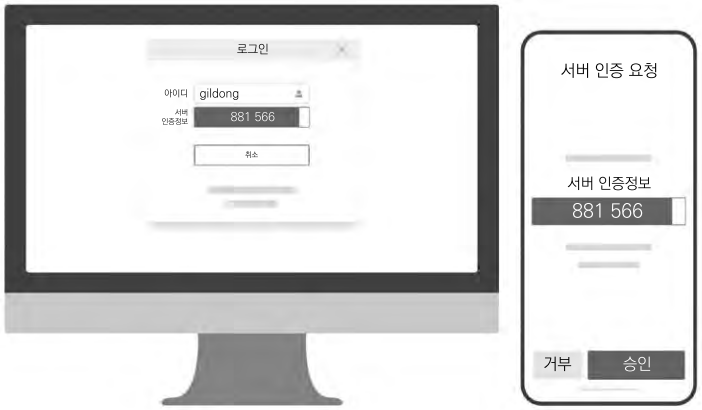
우종현 이스톰 대표

1. 머리말

강력한 인증기술은 사이버 보안의 핵심이다. 사이버 공격의 80% 이상이 사용자 인증값을 도용한 계정 탈취 공격으로 이뤄지기 때문이다. 그러나 기존 사용자 인증기술은 사용자의 진위 여부만을 확인한다. 사용자가 가짜 온라인 서비스에 접속해 인증정보를 제출하면 사용자 계정이 탈취될 수밖에 없는 상황이다.

최근엔 여러 온라인 서비스에서 스마트폰 기반 생체인증 기술로 사용자 인증기술을 대체하고 있다. 그러나 스마트폰 기반 생체인증 기술은 스마트폰 내에서 동작하는 모바일 서비스에서만 안전하다. 만약 생체인증 센서가 장착되지 않은 다른 기기에서 온라인 서비스를 동작하고 있을 경우, 대역 외로 스마트폰 생체인증을 시도하면 보안 취약점이 발생한다.

이에 국내 기술표준화 기구인 TTA PG502와 국제표준화기구인 ITU-T SG17 Q10에선 대역 외 서버 인증 기술(X.oob-sa, 2021)에 대한 표준을 제정했다. 이는 사용자가 접속한 온라인 서비스의 진위 여부를 명시적으로 확인하면서도, 생체인증 센서가 부착되지 않은 다른 기기에서도 온라인 서비스를 안전하게 사용될 수 있게 한다.



[그림 1] 온라인 서비스가 자동 패스워드를 제시하고, 사용자가 스마트폰에서 검증하는 실시 예시

2. 패스워드리스 X.1280 이해와 적용사례

2.1 패스워드리스 X1280의 핵심

본 표준은 사용자가 접속한 온라인 서비스의 진위 여부를 확인하지 못한 채 자신의 인증값(패스워드, OTP, 공동인증서, 생체인증정보 등)을 입력하는 기존 사용자 입증 책임 방식을 탈피한 것이다. 패스워드리스 X1280는 온라인 서비스가 먼저 사용자에게 자동 패스워드를 제시하고 사용자가 이를 스마트폰 앱에서 검증하는 상호인증 기술에 대한 표준이다.

또한 본 표준은 종래 생체인증 기술이 갖고 있던 고비용 구조를 낮추는 효과가 있다. FIDO를 포함한 기존 생체인증 기술은 대역 내 생체인증 기술로서 사용자 단말기(PC, 태블릿, 스마트 TV 등)마다 개별 생체인증 센서가 장착돼 있어야 했다. 만약 대역 내 생체 인증 기술을 임의로 대역 외로 전환하게 되면, 사용자의 생체인증값이 누구에게 제출되는지 확인하지 못하는 보안 취약점이 발생하게 된다.

본 표준은 이러한 취약점을 해소한다. 온라인 서비스가 자동 패스워드를 먼저 제출하고, 사용자가 스마트폰에 생성한 자동 패스워드와 일치하는 경우 스마트폰 생체인증을 통해 사용자 인증 정보를 제출한다. 이를 통해 스마트폰에서 생성된 생체인증 정보가 어느 온라인 서비스로 제출되는지 명시적으로 확인할 수 있다. 즉, 스마트폰의 생체인증 센서를 보안 취약점 없이 사용자의 모든 기기에서 대역 외로 사용할 수 있다.

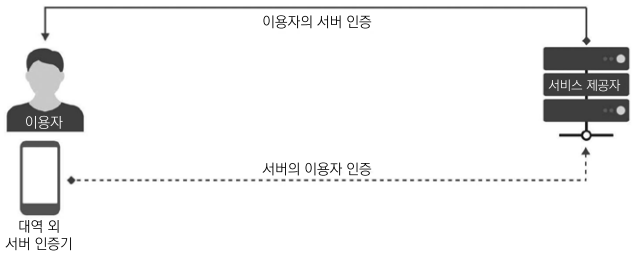
이뿐만 아니라, 자동 패스워드 기술은 사용자 단말기마다 파편화된 사용자 인증 수단을 하나로 단순화시킬 수 있다. 그간 사용자 단말기가 변경되면 단말기마다 다른 인증 수단을 사용해 왔다. 그러나 본 표준 기술은 사용자 단말기가 다르더라도, 하나의 범용 인증 수단으로 모든 사용자 단말기에서 사용자 인증이 가능하다. 무엇보다 이런 상호인증 방식은 종래 사용자 인증값을 탈취하던 사이버 공격(피싱, 파밍, 중간자공격 등)을 무력화시킬 수 있다.

2.2 패스워드리스 X1280 주요 동작 흐름

본 표준 기술은 서비스 인증, 사용자 인증이라는 두 단계로 진행되며, 한 번의 사용자 승인으로 동작한다.

첫 번째 단계인 서비스 인증은 다음과 같이 이뤄진다. 사용자가 서비스에 접속한 후 사용자 단말기에서 사용자 아이디를 입력하면, 온라인 서비스가 자동 패스워드(서버 인증정보)를 화면에 표출한다. 이후 사용자 스마트폰에서 자동 패스워드를 생성해 두 값이 같은 경우 서비스가 정당한 것인지 사용자가 검증할 수 있다.

두 번째 단계인 사용자 인증은 다음과 같다. 스마트폰에 생성된 자동 패스워드와 사용자 단말기에 표



[그림 2] 서비스 인증과 사용자 인증이 한 번의 사용자 승인으로 동작

출된 자동 패스워드가 같은 경우, 사용자는 스마트폰에 장착된 생체인증기로 서비스를 승인하고, 이때 스마트폰에서는 사용자 인증값을 생성해 온라인 서비스에 제출한다. 서비스 역시 사용자 인증값을 검증한 후 사용자 단말기에 온라인 서비스를 제공한다.

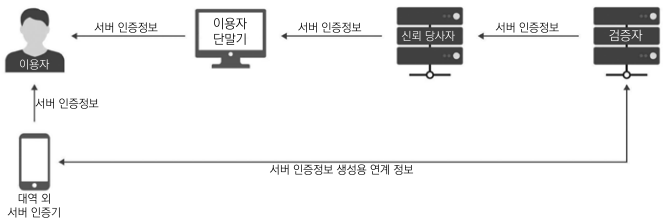
2.3 패스워드리스 X1280 활용 사례

2.3.1 웹이나 앱에서 온라인 서비스 로그인

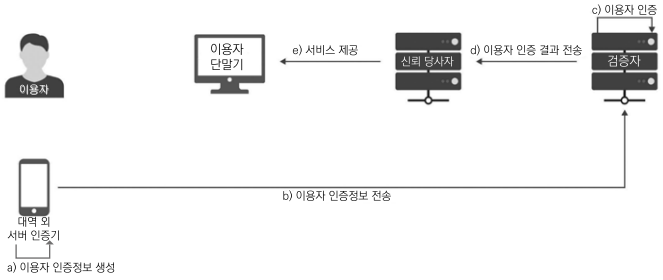
패스워드리스 X1280를 활용하면 온라인 서비스 이용자가 패스워드를 외우고, 주기적으로 변경하며, 일일이 입력할 필요가 없다. 온라인 서비스가 자동 패스워드를 제시하고, 사용자는 스마트폰에서 이를 검증·승인하면 된다. 이를 통해 편리하고 안전한 온라인 웹과 모바일 서비스 이용이 가능하다.

2.3.2 은행, 증권사 업무용 PC나 서버에서 스마트폰 기반 생체인증 로그인

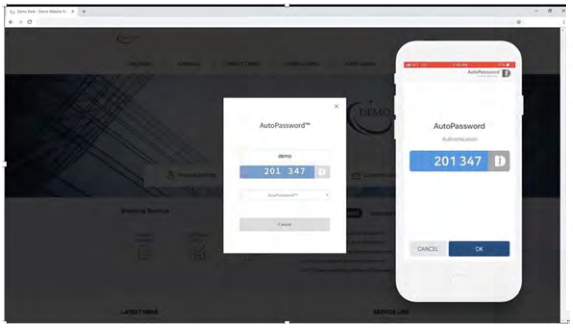
자동 패스워드 기술은 업무상 사용하는 PC(Windows), 서버(Linux)에서도 유용하다. PC나 서버에서 자동 패스워드를 제시하면, 사용자가 스마트폰에서 이를 검증·승인하기 때문에 안전하게 단말기를 이



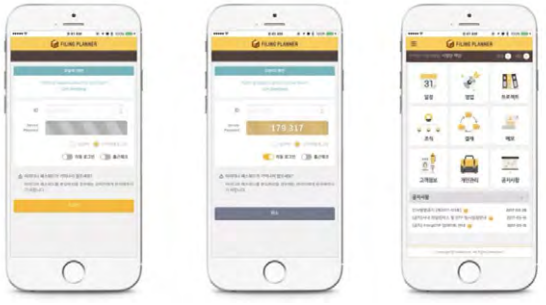
[그림 3] 모바일 단말을 이용한 서비스 인증 흐름



[그림 4] 모바일 단말을 이용한 사용자 인증 흐름



[그림 5] PC 웹 서비스에서 자동 패스워드 로그인 예시



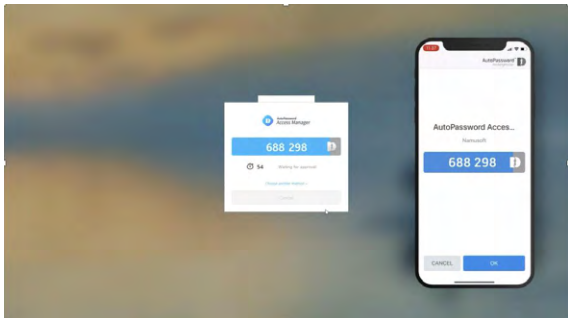
[그림 6] 모바일 앱에서 자동패스워드 로그인 예시

용할 수 있다. 특히 생체인증 센서가 부착되지 않은 PC나 서버에서 스마트폰에 장착된 생체인증기로 대역 외 생체인증이 가능해진다.

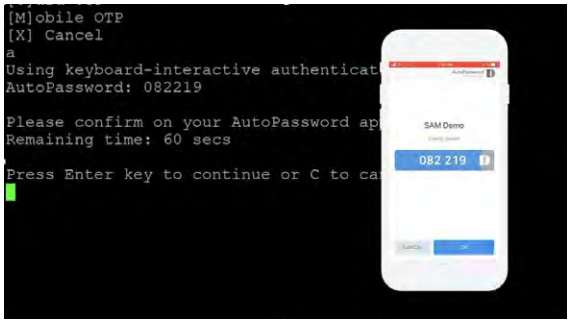
3. 맺음말

본 표준은 사용성, 보안성, 경제성을 두루 갖춘 패스워드리스 기술이다. 이뿐만 아니라 피싱, 파밍, 중간자 공격 등 현존하는 사이버 공격을 무력화시킬 수 있는 상호인증 기술표준이기도 하다. 이는 사용자가 온라인 서비스나 PC·스마트폰·클라우드 서비스 등을 이용할 때 사용자 패스워드를 없애는 동시에, 스마트폰 생체인증 기술을 범용적으로 적용할 수 있는 대역 외 상호인증 기술이다.

현재 본 표준을 전 세계 B2C 온라인 서비스에서 무료로 사용할 수 있도록, 패스워드 얼라이언스(www.passwordalliance.org)에서 프리 소프트웨어를 제공하고 있다. 사용자는 모바일 앱스토어에서 Passwordless X1280 앱을 무료로 다운로드해 스마트폰에 설치할 수 있으며, B2C 온라인 서비스에서도 Passwordless X1280 인증 서버를 무료로 다운로드 받아 기존 서비스에 적용할 수 있다.



[그림 7] 업무용 윈도우즈 PC 로그인 때 자동 패스워드로 로그인 예시



[그림 8] 업무용 리눅스 서버 로그인 때 자동 패스워드로 로그인 예시

참고문헌

[1] Recommendation ITU-T X.1280 (03/2024), Framework for out-of-band server authentication using mobile devices
[2] Recommendation ITU-T X.1254 (09/2020), Entity authentication assurance framework
[3] NIST, SP 800-63B(06/2017), Authentication and Lifecycle Management

주요 용어 풀이

- **FIDO**(Fast IDentity Online): 패스워드 대체를 목표로 개발된 국제표준 인증기술
- **OTP**(One-Time Password): 로그인할 때마다 그 세션에서만 사용할 수 있는 일회성 패스워드를 생성하는 보안 시스템
- **생체 인증**(biometric authentication): 지문, 홍채, 음성, 생체신호 등 인간의 생체 정보를 본인 인증에 활용하는 기술