AutoPassword™

WHITE PAPER

AutoOTP & AutoPassword

생체 인증과 서버 인증을 결합한 대역외 상호 인증 시스템

Prepared By:
John Woo, CEO
+82-10-3386-4017
jhwoo@dualauth.com

Table of Contents

Executive Summary

인증수단은 개인화된 온라인 서비스를 제공하는데 가장 근간이 되는 기술이다. 로그인을 시도하는 사용자가 이전에 가입했던 사용자인지를 식별하고 검증할 수 있어야 개인화된 온라인 서비스가 가능하다. 전통적인 사용자 인증 수단인 패스워드가 PKI 인증서 기술, FIDO 생체인증 기술, 모바일 Push 인증 기술 등으로 대체되고 있으나, 여전히 단말기가 바뀔 때 마다 인증수단을 재등록해야 하는 불편함을 갖고 있거나 서비스 제공자를 사칭하는 공격에 노출되는 한계점 등을 해결하지 못하고 있다. 본 문서에서는 기존 인증기술들이 갖고 있는 한계점을 설명하고, 대역외 서버인증과 생체인증을 결합한 AutoOTP와 AutoPassword를 제시하여, 어떻게 단말 독립적이면서도, 중간자 공격에 대비된 대역외 상호 인증 기술이 작동하는지를 설명한다. 마지막으로 새로운 대역외 상호 인증기술이 정부기관, 은행, 기업, 기관 등에서 어떻게 보안성과 편리성을 개선하였는지를 설명한다. 본 문서는 인증수단을 선정해야 하는 기업 보안담당자나 온라인 서비스 관리자를 위해서 작성되었다.

다양한 사용자 인증기술의 도래와 인증기술을 구분하는 방법

사용자 인증기술은 보안성과 편리성을 중심으로 계속 진화하고 있다. 사용자 인증기술은 사용자 비밀번호를 시작으로 보안카드(암호코드표), 일회용비밀번호 생성기, 문자메시지/ARS/이메일을 통한 일회용 비밀번호 서비스, 공인인증서를 필두로 한 PKI 인증서(X.509), 지문/홍채/안면 등 FIDO기반 생체인증, 블록체인 기반 DID 인증 등으로 고도화되고 있다.

보안카드, PKI 인증서, 지문/홍채/안면, 블록체인 DID 인증기술 예시

고도화되고 있는 다양한 인증 기술들을 이해하기 위한 방법으로는 개별 인증 기술이 동작하는 방식을 분석하는 방법도 있겠지만 기술 표준화 단체에서 인증기술을 구분하는 분류 방식을 통해서도 빠르게 이해할 수 있다. 표준화 단체에서 인증 기술을 구분하는 방법으로는 크게 3가지로 나누어진다. 요인으로 구분는 방법, 통신방식으로 구분하는 방법, 보안 수준으로도 구분하는 방법이다.

요인으로 구분하는 방법은 사용자를 확인하는데 있어서 어떠한 요인을 통해서 사용자를 인증할 수 있는가에 대한 구분 방식이고, 통신 방식을 통한 구분 방식은 인증 값을 전달하는 통신 채널에 의한 구분 방식이며, 마지막으로 보안 수준에 의한 방식은 어떠한 인증 수단이 더 보안성이 뛰어난 인증 수단인가로 구분하는 방식이다.

요인에 의한 구분

요인에 의한 구분	설명	예시
Something you know	사용자가 알고있는 것으로 증명하는 방식	암기하고 있는 사용자 패스워드나 PIN
Something you have	사용자가 소지하고 있는 것으로 증명하는 방식	보안카드(암호표), 대역외인증기(푸시기반 인증코드 전송이나 QR코드 스캔하는 모바일 인증앱

	OTP동글, USIM기반 모바일 인증기 등 (단, 문자메시지, ARS, 이메일 등으로 인증코드를 제공하는 방식은 소지가 아닌 서비스 가입 방식으로 착신전환과 같은 공격시 소지를 증명할 수 없어 소지 기반 인증수단에서 제외됨) 소지 증명 인증기를 활성화시키기 위해 다른요인(Something you know나 Something you are)과 결합하여 사용될 수 있음	또는 USIM 소지를 확인하는 모바일 인증앱), 단일요인OTP생성기, 다중요인OTP생성기(지문인식/PIN입력OTP), 단일요인암호화소프트웨어(파일기반 인증서), 단일요인암호화기기(인증서를 보관하는 보안토큰,단말기와 연결된 버튼방식 인증기기), 다중요인암호화소프트웨어(모바일기기에서 생체인증과 결합한 파일기반 인증서, FIDO), 다중요인암호기기(전용인증 기기에서 생체인증과 결합한 파일기반 인증서)
Something you are	사용자의 생체정보로 증명하는 방식 생체정보는 그 자체가 비밀이 아니며, 확율을 기반으로 작동하기 때문에 오일치율을 고려하여 다른 확정적인 인증수단을 보조하는 요인으로 권장 서비스 제공자의 중앙화된 생체 인증값 비교방식 보다는 사용자 소지의 단말기에서 생체 인증값을 보관하고 비교하는 방식을 권장	Something you have의 추가 요인으로 사용

통신방식에 의한 인증기술 구분

동작방식	설명	예시
대역내 인증기술	사용자 단말기와 서비스 서버간의 통신 채널로 사용자 인증값을 전달하는 방식	예시 1; 온라인 서비스와 연결된 사용자 PC에 사용자패스워드/보안카드/일회용비밀번호(OTP 동글/SMS/ARS/Email등)등을 입력하는 방식 예시2; 온라인 서비스와 연결된 사용자PC에서 X.509기반 인증서로 사용자를 인증하는 방식(PKI인증서) 예시3; 온라인 서비스와 연결된 사용자 폰에서 안면 또는 지문 센서를 이용하여 사용자를 확인하고 사용자 인증값을 서버에 전달하는 방식(FIDO)

대역외 인증기술	사용자 단말기와 서비스 서버간의 통신 채널 이외에 다른 통신 채널로 사용자의 인증 값을 전달하는 방식	예시1; 푸시기반의 인증요청을 받아서 모바일에서 승인하는 방식 예시2; PC화면에 표출된 인증코드나 QR코드를 모바일 앱에 직접 입력하거나 스캔하는 방식 예시3; PC화면에 표출된 일회용 코드를 ARS 전화에 입력하는 방식

보안 수준에 의한 구분 - AAL(Authentication Assurance Level)

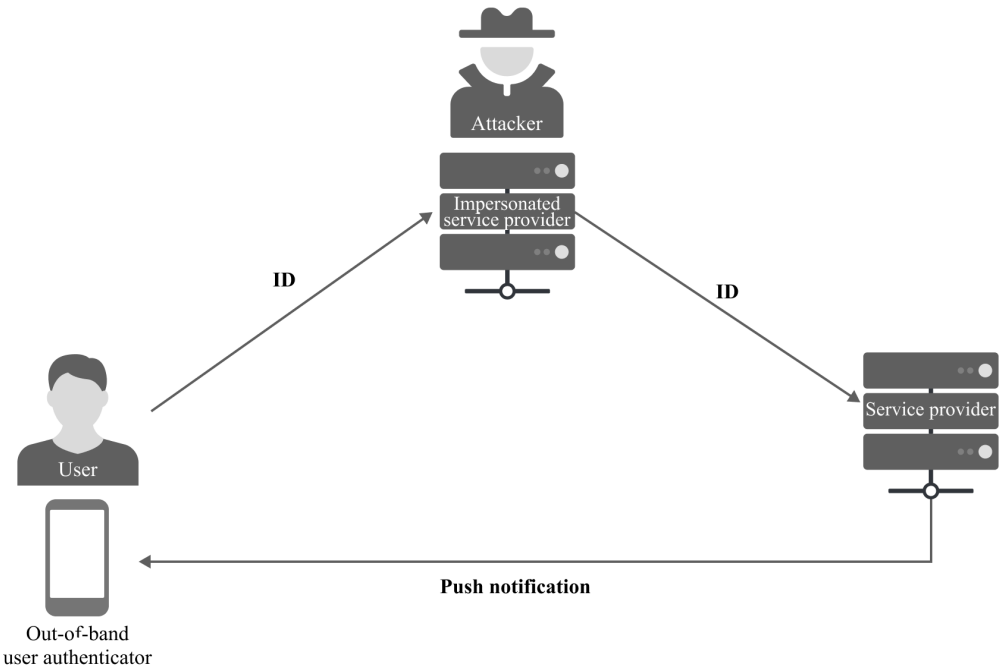
보증 레벨	설명	예시
1단계	사용자만 알고있거나, 사용자가 소지하고있거나, 사용자를 특정할 수 있는 생체 요인중 1개 이상의 요인으로 사용자를 확인하는 기술	암기하고 있는 사용자 패스워드를 입력받는 방식
2단계	3가지 요인중 2개 이상 요인으로 사용자를 확인하는 기술로 탈취된 코드를 이용한 재사용 공격에 저항력을 갖추 기술	암기하고 있는 사용자 패스워드와 소지하고 있는 OTP 생성기에서 생성된 일회용 패스워드를 입력받는 방식, 사용자 패스워드와 소프트웨어타입으로 PC나 모바일에 설치 제거 가능한 인증서
3단계	SSL/TLS와 같은 암호화 프로토콜을 이용하여 사용자가 암호키를 소지하고 있는 것을 확인할 수 있을 뿐만 아니라 연결된 서비스가 올바른 서비스인지까지 확인시켜 줄 수 있는 기술(사칭한 가짜 온라인 서비스에 대한 저항력 및 검증 서버 탈취시 대비할 수 있는 저항력 등)	물리적 보안 매체(보안토큰)에 저장된 사용자 인증서와 서비스를 확인할 수 있는 서버 인증서를 이용하여 사용자 인증뿐만 아니라 서비스를 사칭한 온라인 서비스 공격까지 대비된 방식, FIDO (UAF/CTAP2)

사용자 인증기술의 한계점

3가지 인증기술 구분 방식으로 최신 인증 기술 동향을 대입해 보면, 요인에 의한 구분은 생체인증 기술이 인증 요인의 보조적 수단으로 권장되면서 소지 요인인 스마트폰과 결합하여 확산되고 있고, 통신에 의한 방식은 사용자의 스마트 단말기가 많아지면서 단말 종속적인 대역내 인증 방식에서 단말 독립적인 대외외 인증 방식이 선호되고 있으며, 보안 수준에 의한 방식은 사용자 뿐만 아니라 서비스까지 인증할 수 있는 방식이 사용되고 있다. 즉 생체인증 기술을 이용한 모바일 인증기면서, 여러 단말기에서 사용이 가능한 대역외 인증을 지원하며 사용자 뿐만 아니라 서비스제공자까지 확인할 수 있는 방식으로 진화하고 있다.

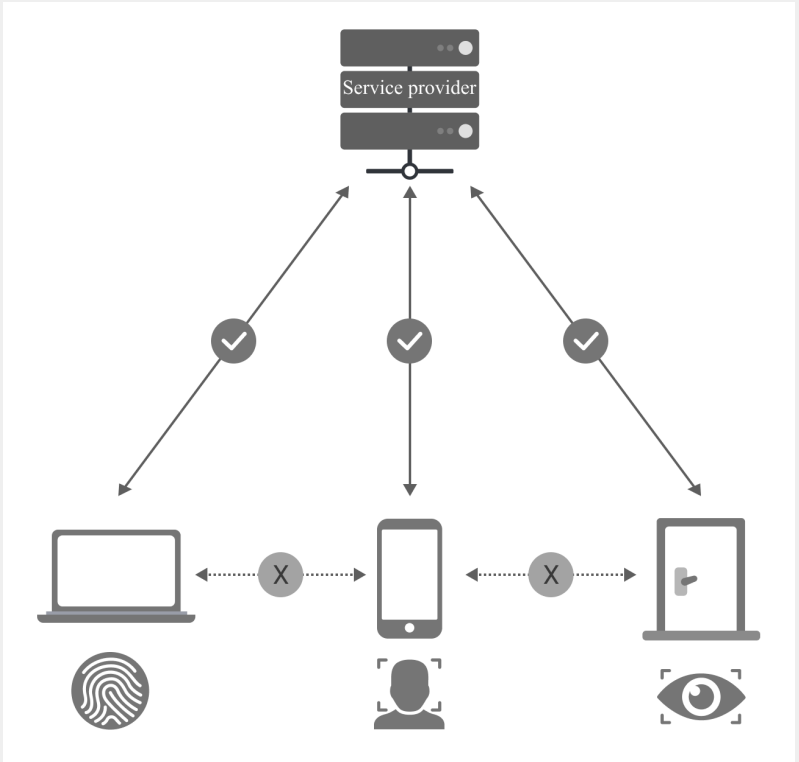
그러나 모바일 생체인증 기술(FIDO)은 대역내 모바일 인증기술이어서 모바일 내 구동되는 애플리케이션에 대해서만 사용자 인증이 유효하다. 일 예로 다른 PC나 태블릿에서 구동되는 애플리케이션에서 사용자 인증이 필요할때 스마트폰의 생체 인증기가 인증 수단으로 사용될 수 없다. (예; PC에서 인터넷 뱅킹을 사용하는 상황에서 사용자 인증이 필요한 시점에 스마트폰의 생체인증 기술로 PC의 인터넷 뱅킹 사용자를 인증하는 대역외 인증수단으로 사용될 수 없다.)

대역내 인증기술인 모바일 인증기술을 무리하게 대역외로 사용하게 되면 서비스 제공자를 사칭한 공격에 무력화될 수 있다. 아래 도면에서 보듯이 사용자가 접속한 서비스 제공자가 진짜 서비스 제공자가 아닌 서비스 제공자를 사칭한 공격자에 접속한 이후, 대역외로 사용자 인증요청이 시작되면 사용자는 해당 요청이 자신의 접속에 의한 인증 요청으로 오인하여 공격자의 인증 요청을 승인하게 된다. 대역내 인증 기술을 대역외로 운영하게 되면 서비스 제공자를 사칭하는 공격에 취약하게 된다.



도면 - 대역내 인증 기술을 대역외로 사용하게 되면 발생하는 취약점

또한 생체인증 기술은 대역내 인증 기술이어서 여러 사용자 단말기에서 사용되기 위해서는 생체인식 센서를 장착한 모든 단말기 마다 자신의 생체정보를 등록해 주어야 하는 번잡함이 발생한다.



도면 - 대역내로 운영되는 생체인증은 단말기 마다 매번 재등록이 필요

대역내 인증기술이 갖고 있는 단말기 종속적인 인증기술의 불편함을 탈피하고자 단말기기와 블루투스나 USB 통신으로 연결되는 외부 독립 인증기에 대한 시도가 있으나, 인증기가 연결되는 단말 기기 마다 무선 및 유선 연결방식이 제각각이어서 하나의 외부 인증기로 모든 단말기와의 연결 방식을 지원할 수 없다. 일예로 외부 인증기가 유선으로 PC와 연결될 때는 PC가 지원하는 물리적 포트(USB A, B, C타입) 인터페이스를 갖추고 있어야 하며, 스마트폰과 연결되기 위해서는 NFC, USB MINI, Lightning 포트 등을 갖추어야 하는데, 이 모든 통신 방식을 지원하는 외부 인증기는 없다.

외부인증기가 단말기와의 물리적 매체 호환성을 벗어나기 위하여 스마트폰과 PC의 블루투스를 이용한 모바일 기반 FIDO CTAP2 인증방식을 시도 하였으나, PC 블루투스 버전, 운영체제 버전, 애플리케이션 버전, 스마트폰 기종별 블루투스 페어링 및 통신 프로토콜을 다 맞추어야 가능하기 때문에 모든 애플리케이션과 하드웨어 기종을 포괄할 수 있는 스마트폰 기반 블루투스 CTAP2인증기 개발은 사실상 어려운 상황이다. 일 예로 구글의 경우도 PC에 안드로이드 폰을 블루투스로 등록한 이후 구글 크롬브라우저를 통한 구글 서비스에서만 안드로이드 CTAP2 인증이 되도록 하는 제한된 인증 서비스만을 제공하고 있다.

따라서 사용자의 생체인증을 포함하되 단말기 독립적인 외부인증기로 작동할 수 있으면서도 서비스 제공자까지 확인할 수 있는 보안성을 갖춘 새로운 인증 기술이 필요하다.

대역외 서버인증 기술과 모바일 생체인증 기술을 결합한 **AutoOTP**와 **AutoPassword**

대역내 서버 인증 기술과 한계점

서비스 제공자를 사칭하는 공격에 대비하는 일반적인 방법은 SSL/TLS 서버인증서를 확인하는 것이다. SSL/TLS 서버 인증서는 X.509 표준에 따라 모든 웹 브라우저의 녹색바와 자물쇠를 통해서 확인이 가능하다. 서버인증서는 서버와 연결된 웹브라우저에서만 인증서 확인이 가능한 기술이기 때문에 전형적인 대역내 서버 인증 기술로, 주요 공공 및 민간 온라인 서비스가 파밍이나 피싱 사이트 공격에 노출되지 않도록 의무 도입되고 있다.

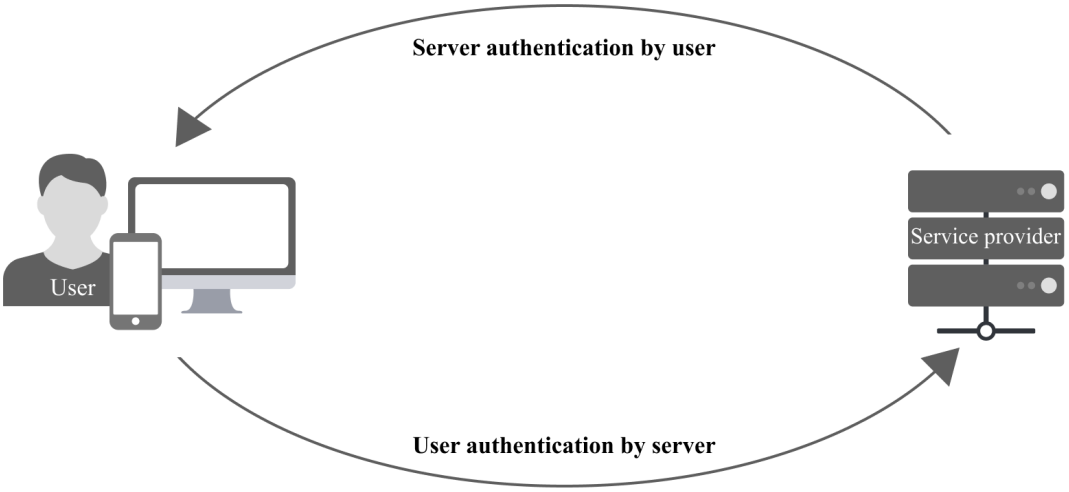
하지만 웹서버 인증서 기술은 사용자 인증 수단과 분리되어 있어 사용자가 매번 웹서비스에 접속할때 마다 서버 인증서를 별도로 확인해야 하는 불편함이 있어서 사용자가 쉽게 간과하고 있다. 게다가 유사도메인을 이용하여 서버인증서까지 제공하는 공격자를 만나게 되는 경우 녹색바에 자물쇠가 있어도 사용자 인증값을 쉽게 탈취할 수 있다. 또한 SSL/TLS 서버인증서는 인증서 발급자의 공개키를 관리하고 있는 웹 브라우저에서만 작동되어, 웹브라우저가 아닌 설치형 어플리케이션이나 운영체제 등에서는 사용할 수 없는 한계점이 있다. 웹서버 인증서는 서버 인증기술로 사용되기 보다는 주로 통신구간 암호화 기술로 사용되고 있는 실정이다.

대역외 서버 인증 기술

대역내 서버 인증기술의 한계점을 극복하고자 ITU-T SG17에서는 대역외 서버 인증 기술(X.oobsa)에 대한 표준화를 진행 중에 있다. 대역외 서버 인증기술은 사용자의 모바일 인증기로 서버와 사용자를 동시에 인증하는 기술이다. 대역외 서버 인증기술은 사용자의 PC 단말기에 연결된 서버가 서버 검증을 위한 일회용 패스워드를 사용자 화면에 먼저 제시하고, 사용자는 이를 스마트폰에 설치된 서버 인증앱에서 생성한 서버 검증용 일회용 패스워드와 일치하는지 확인하여 서버를 인증하는 기술이다. 서버가 제시한 일회용 패스워드와 사용자의 스마트폰에 설치된 서버인증 앱이 생성한 일회용 패스워드가 일치하면 연결된 서버가 검증된 서버임을 사용자가 인증하는 것이다.

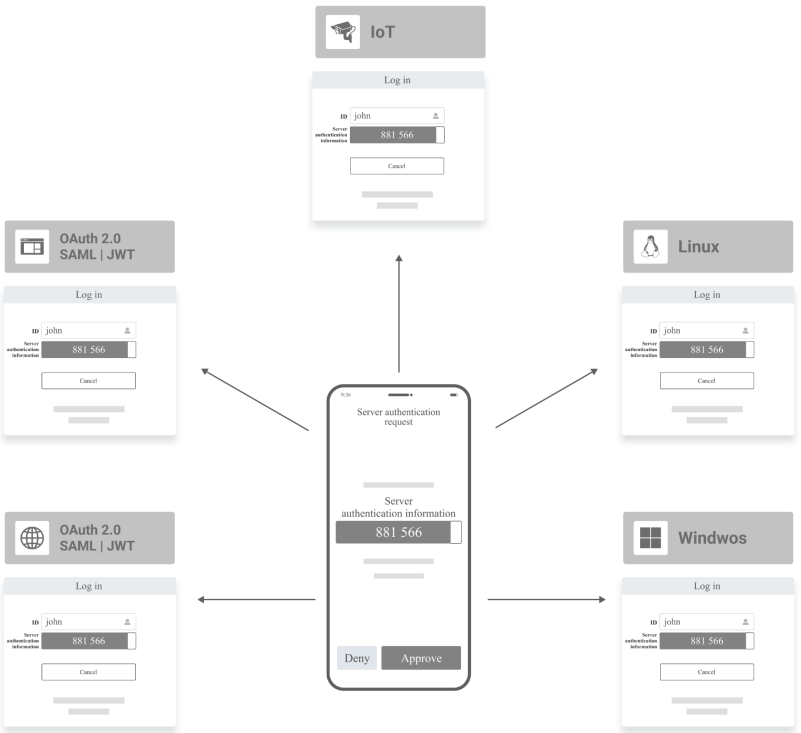
대역외 서버 인증기술과 결합된 사용자 인증 기술

사용자가 서버 검증용 일회용 패스워드를 스마트폰에서 검증할때 스마트폰앱이 사용자의 생체인증 값을 확인하여 정당한 사용자인 경우 사용자의 인증값을 서버에 제공하는데, 이때 사용되는 사용자 인증 기술은 생체인증과 결합된 OTP, PKI, FIDO 등의 검증된 전통적인 사용자 인증 기술이 적용된다.



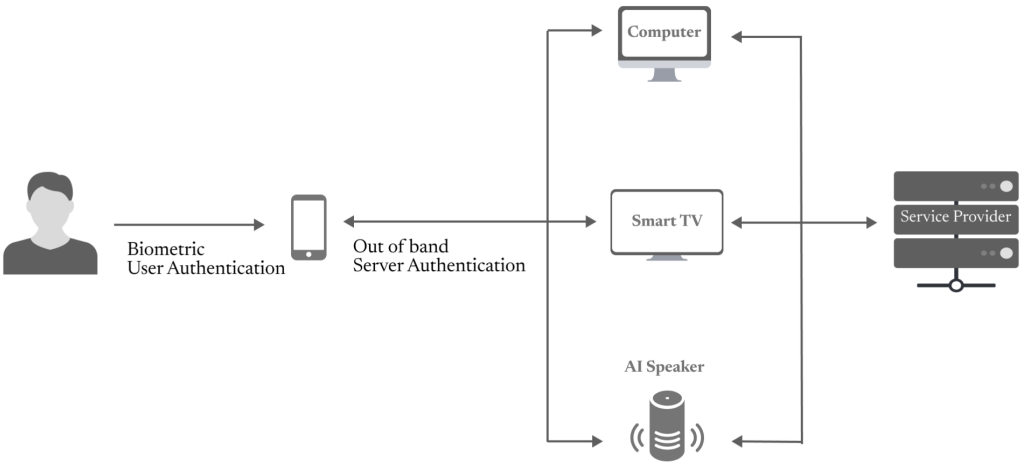
기술적 효과

1. 서버 인증과 사용자 인증이 한번에 이루어지는 사용자 중심의 상호인증 기술 대역내 서버 인증 기술인 SSL/TLS 서버 인증서는 사용자 인증과정과 분리되어 있어 의도적으로 사용자가 서버 인증서를 확인하지 않는한 서버인증 과정 없이 사용자 인증만 진행하게 된다. 이러한 사용자 행동 패턴을 이용하여 공격자는 동일 도메인 이름의 파밍 사이트로 사용자를 유도하거나, 자물쇠를 표시하는 유사도메인 이름의 악성 사이트 접속을 유도하여 사용자 인증정보를 탈취하고 있다. 그러나 대역외 서버인증기술과 사용자 생체 인증 기술이 결합된 대역외 상호 인증기술로 서버가 사용자에게 명시적인 서버인증용 일회용 비밀번호를 먼저 제시하게 하고, 사용자가 모바일 앱에서 이를 확인하여 승인하는 경우, 모바일 앱이 서버에게 사용자의 인증정보를 제공하여 서버역시 사용자를 확인하는 기술이다. 즉, 서버 인증과정과 사용자 인증과정을 연결하여 대역외 상호인증이 이루어 지도록 하였다.



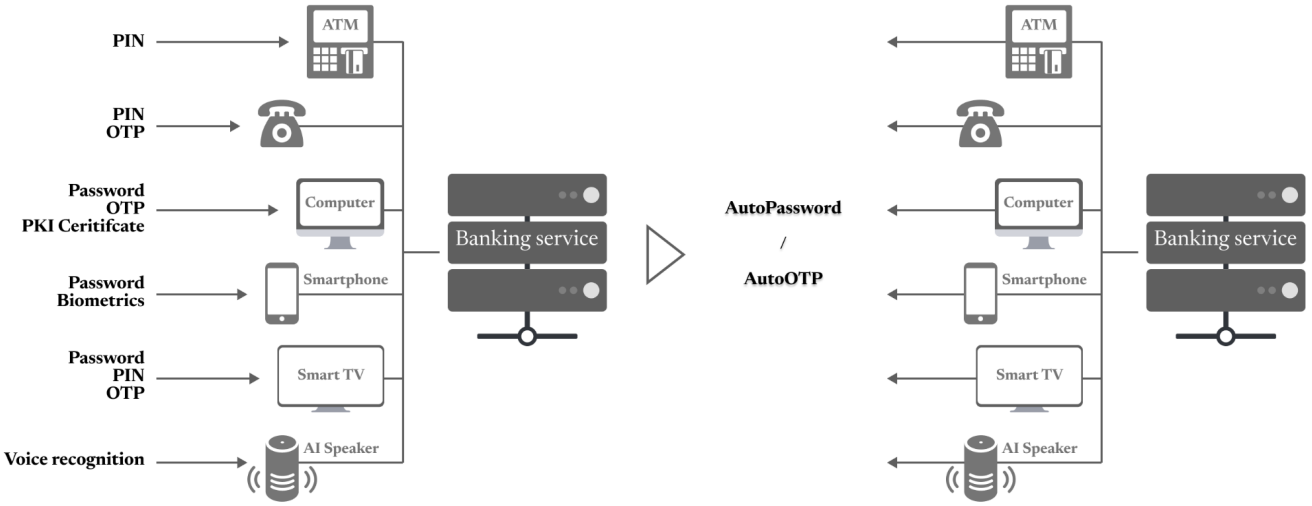
2. 생체인증을 지원하지 못하는 사용자 단말기에 모바일 생체인증 기술을 확대 생체인증 센서를 장착한 단말기에서만 유효했던 대역내 생체인증 기술을 생체인증 센서를 장착하지 못한 단말기에서도 사용자 스마트폰의 생체인증 기술이 적용될 수 있게 하는 대역외 상호인증 기술을 제공한다. 대역외 상호인증 기술을 사용함으로써

대역외 사용자 인증 기술이 갖고 있는 서비스 제공자 사칭공격에 대한 취약점을 해소하고, 스마트폰에 갇혀있는 사용자 생체 인증 기술을 생체인증 센서가 없는 단말기에 까지 확대시킬 수 있다. 예를들어 지문인식기 나 카메라와 같은 생체인증 센서가 없는 PC에 스마트폰에 있는 안면인식이나 자문인식을 이용하여 사용자는 PC의 사용자 인증을 수행할 수 있다. 즉 대역외 상호인증 기술은 사용자가 어디에 생체 인증값을 제출하는지 확인시켜 줄 수 있기 때문에 대역외로 생체인증 기술을 사용하더라도 안전하다.



3. 단말기 마다 파편화된 사용자 인증수단을 하나로 통합할 수 있는 상호 인증기술

멀티채널 서비스를 제공하는 은행의 경우, 고객은 기기 마다 다른 인증값을 제공해야 한다. ATM에서는 카드와 PIN코드를 제시해야 하고, 텔레뱅킹에서는 OTP코드를 입력해야 하며, 인터넷 뱅킹에서는 PKI인증서와 OTP를 입력해야 하며, 모바일에서는 지문이나 안면을 제시해야 하고, 스마트 TV에서는 리모컨으로 OTP를 입력해야 하고, AI스피커에서는 육성을 등록한 후 인증을 진행해야 한다. 서비스 매체 마다 인증 수단이 달라질 수 밖에 없는 단말기 종속적인 인증수단을 사용하기 때문이다. 하지만 대역외 상호인증 기술인 AutoPassword가 적용되면 모든 서비스 채널에서 하나의 인증 수단이 적용될 수 있다. 모든 서비스 채널이 사용자에게 먼저 서비스 인증 정보를 제공하고, 이를 사용자가 승인하기 때문에 매체별가 다르더라도 단일화된 인증 수단을 이용할 -수 있게 된다.



4. 사용자 패스워드를 함께 관리

서비스가 제시하는 일회용 패스워드를 사용자가 모바일에서 인증할때 마다 서비스의 사용자 패스워드가 자동으로 갱신되어 사용자가 패스워드를 변경하고 암기해야 했던 관리 방식에서 벗어나게 된다. 대역외 상호인증 기술은 사용자 패스워드를 대체하는 수단이지만 사용자 패스워드를 없애는 수단은 아니다. 모든 인증기술이 킬패스워드(Kill Password)나 패스워드레스(Passwordless)를 외쳐도 결국 스마트폰을 분실한 상황에서는 사용자 패스워드로 복원해야 하는 한계점이 남아 있다. 본 대역외 상호인증 기술은 사용자가 인증할 때 마다 서비스의 사용자 패스워드를 대소문자, 특수문자, 숫자 등을 섞어서 무작위로 갱신하기 때문에 사용자가 패스워드를 변경 관리를 하지 않아도 되고, 사용자가 스마트폰을 분실하였거나 갱신한 경우 본인 확인 과정을 거쳐서 사용자 패스워드를 초기화 한 이후 온라인 서비스에 로그인하여 사용할 수 있다. 물론 사용자가 스마트폰 변경시 사용자 패스워드 초기화로 재설정도 가능하다.

대역외 상호인증 기술 적용 사례

1. **PC**로 업무를 수행하는 은행 및 정부기관

2만명의 임직원이 PC를 통한 업무를 수행하는데 있어서 PC에 별도의 생체인증 센서를 구입하지 않고 사용자의 스마트폰에 AutoPassword 앱을 설치하여 업무용 PC 및 웹서비스 로그인을 자동화하였다. 사용자가 로그인을 시도할때 마다 자동 패스워드가 사용자에게 제시되고 사용자가 AutoPassword 모바일 앱으로 이를 검증하여 사용자는 암호관리로 부터 자유로워졌고 보안성은 크게 개선되었다. 특히 종전 3개월 마다 사용자 패스워드가 변경하고 숙지해야 하는 관리 부담으로 부터 자유로워져 사용자의 자발적 도입과 함께 보안에 대한 변화관리를 크게 개선시켰다.

2. 고액의 포인트 서비스를 제공하는 온라인 도매 쇼핑몰

온라인으로 도매 서비스를 제공하여 소매상들에게 구입금액의 일정 금액을 현금과 같이 사용할 수 있는 포인트를 제공하는 쇼핑몰에서 계정 탈취 및 도용을 방지하고자 AutoOTP를 적용하였다. 종전 일반 OTP는 사용자가 6자리 코드를 읽고 입력해야 했던 것에 반하여 도매 온라인 쇼핑몰은 AutoOTP코드를 먼저 제시하고, 사용자가 모바일 앱에서 확인함으로써 OTP코드 입력에 대한 불편함을 해소하였고, 피싱이나 파밍 공격으로 탈취될 수 있는 OTP코드와 탈취되지 않는 보안성을 함께 제공하였다.

3. 기업용 **Gmail** 서비스 및 클라우드 서비스

중요 업무가 Gmail을 통해서 이루어지는 기업에서 사용자 인증수단을 AutoPassword로 대체하여 피싱이나 파밍 공격으로 부터 사용자 이메일 계정이 탈취되지 않도록 하였다. 특히 업무용 클라우드 서비스를 집이나 회사 PC, 태블릿, 스마트폰 등을 통해서 수행할때 기기 마다 별도의 생체인증 등록 과정이 필요했으나, 추가적인 생체등록 과정 없이도 사용자가 아이디만 입력하고 화면에 표시된 AutoPassword를 하나의 스마트폰에서 검증하여 기기별 사용자 인증 수단 등록과정을 생략 할 수 있게 되었다.

4. 중요 서버의 접근제어

중요 데이터를 보관하고 운영하는 서비스 서버에 관리자가 접근하는데 있어서 관리자를 증명하는 키 파일 입력 방식이나 OTP 입력 방식은 관리자 PC를 통해서 쉽게 탈취될 수 있다. 관리자 PC에 멀웨어가 침투하게 되면 관리자 PC내 모든 계정 데이터 및 입력 값이 제3자에게 탈취될 수 있다. AutoPassword를 도입하여 리눅스 서버에 접근할때 사용자가 인증값을 입력하는게 아니라 리눅스 서버가 사용자에게

인증값을 제시하고 사용자가 대역외로 스마트폰에서 검증하기 때문에 안전하게 서버의 접근제어를 구현할 수 있다.