19 전시기술

차세대 FIDO 기술

스마트시티

+ Inventor Information

김수형 박사
한국전자통신연구원 정보보호연구본부

연구이력

1) 범용인증플랫폼(FIDO) 기술 연구

2) NFC/BLE기반 간편결제 및 인증기술 연구

3) 스마트지갑(모바일결제) 기술 연구

+ Applications

- 모바일 바이오 인식(E-payment 등)
- 컴퓨터정보시스템보안
- 물리보안(출입통제, 근태관리 등)
- 의료복지(E-Healthware 등)
- 국방 및 수사(지문감식, DNA분석 등)

+ Contact Point

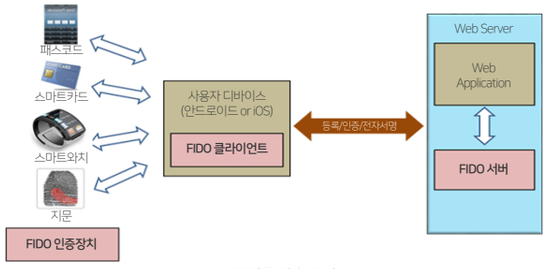
- 소속 : 한국전자통신연구원 사업화협력실
- 담당자 : 김호민
- 전화 : 02-860-1804
- E-mail : hominkim@etri.re.kr
- Hompage : www.etri.re.kr

+ Background

- 패스워드 기반 사용자 인증은 보안상 취약점이 있지만 비용이 적게 들고 편리성 때문에 현재까지 광범위하게 사용되고 있음
- 패스워드 기반 인증의 보안 취약성을 개선하기 위해 생체 인증을 사용하거나 다중 요소 인증 기술을 적용하려는 시도는 기술에 따라 사용자의 편리성이 떨어지거나 광범위하게 설치하기에 비용 부담이 증가하여 응용서비스에 적용하기에는 무리가 있음
- 기존 FIDO 인증 방법은 인증서를 사용하지 않고 웹사이트 접속 시마다 서로 다른 인증키를 등록하여 사용하는 번거로움이 있음

+ Key Technology Highlights

- 핀테크 서비스의 보안성과 편의성을 강화한 국제표준 FIDO(Fast Identity Online) 기반 범용인증 플랫폼 기술임
- 얼굴, 음성, 행위, 환경정보 등 사용자별 고유패턴 정보를 분석하여 명시적 인증을 최소화해 사용자 불편 없이 보안을 강화한 무자각 지속인증 기술임



FIDO 플랫폼 기술 구성도

+ Discovery and Achievements

- 특정 인증기술에 의존하지 않고, 패스코드, 스마트카드, 스마트와치 등 다양한 인증기술을 편리하게 사용하며 보안성을 높이는 인증 서비스를 구현하며, 국제표준 FIDO 인증 기술을 준용하여 기존 서비스 서버에서 쉽게 연동할 수 있음
- 기존의 단순한 앱래핑이 아니라, 특정 기능의 업그레이드나 추가 코드를 안정적으로 삽입하는 등의 복잡한 경우도 처리가 가능함
- 난독화 툴로 암호화된 바이너리 앱에 보안 모듈 탑재 가능하며, 앱래핑으로 탑재할 보안모듈의 기능 및 구동 위치를 선택할 수 있음
- 얼굴, 목소리 등과 함께 적용한 FARM 인증 기술과, 무자각 상태로 행위/환경 특성 정보를 활용한 가변 멀티팩터 인증을 수행하는 지속인증 기술에서 차별성을 갖고 있음
- 행위 기반 특성과 더불어 사용자의 환경 특성을 이용하여 보다 포괄적인 인증 기술을 제공할 수 있음(상황에 맞는 4단계 인증 레벨)

+ Intellectual property rights

No.	출원번호	특허명	현재상태 (2018년 4월 기준)
1	10-2016-0116491	F I D O 2.0에서 인증서를 이용한 사용자 인증 방법 및 장치	출원
2	10-2016-0143633	카쉐어링 서비스를 위한 사용자 지속인증 장치 및 방법	미공개특허
3	10-2016-0148305	얼굴 인식 시스템 및 그 방법	미공개특허
4	10-2016-0149840	보안 정책을 지원하는 단말 관리 방법 및 장치	미공개특허
5	10-2016-0082926	비대칭 패스워드 기반 인증된 키 합의 방법	출원
6	10-2016-0129549	패스워드와 I D 기반 서명을 이용한 인증 키 합의 방법 및 장치	출원
7	10-2016-0108328	방위각 기반 사용자 근접 감지 시스템 및 방법	출원
8	10-2016-0024978	어플리케이션 사용패턴을 고려한 프라이버스 보호 방법 및 장치	출원
9	10-2016-0019360	화이트 박스 암호화 기반의 연산 방법 및 그 방법을 수행하는 보안 단말	심사중
10	10-2015-0190867	출입 통제 방법 및 장치, 사용자 단말, 서버	심사중

+ Exemplary Claim

Patent number : 10-2016-0116491

- 존속기간(예상)만료일 : 2036년 9월 9일

<청구항 계층 분석>

1

Claim Structure

- 전체 청구항(1), 독립항(1), 종속항(0)

Exemplary Claim

- 사용자의 인증서를 저장 수단에 관리하는 인증서 관리 모듈
- 사용자의 등록 비밀키를 저장 수단에 관리하는 등록키 관리 모듈
- 사용자 단말에 연결된 상태에서, 네트워크상의 서버로부터의 요청을 사용자 단말에서 수신하고 전달받음에 따라, 인증서를 포함하고 등록 비밀키로 전자서명된 정보를 포함하는 인증키를 생성
- 사용자 단말을 통해 인증키를 서버로 전송하여 등록하는 인증키 관리 모듈을 포함하는 인증장치