제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

# 일회용 패스워드 기반의 스마트 지갑 인증

최요한*, 서희석*
* 한국기술교육대학교 컴퓨터공학부
e-mail:histone@kut.ac.kr

# Authentication of the smart wallet based on One-time password

Yo-Han Choi*, Hee-Suk Seo*

*Dept of Computer Science & Engineering,
Korea University of Technology and Education

요 약

스마트폰의 보급과 함께 등장한 스마트지갑은 스마트폰을 이용한 지불 시스템이다. 스마트지갑을 이용하여 결제를 수행하기 위해서는 결제단말과 스마트폰의 페어링 과정이 필요하다. 페어링을 통해 결제가 이루어지는 만큼 페어링 과정의 보안이 중요하다. 하지만 현재의 페어링과정에 적용되는 보안절차는 이미지 비교, 바코드, 사운드 등의 원시적인 차원의 보안절차만이 적용되어 있는 수준으로 보안강도가 낮다. 본 논문에서는 일회용 패스워드를 이용하여 기존의 페어링의 취약점을 보완하려고 한다. 일회용 패스워드를 이용하기 위해서는 사용자의 모바일ID를 검증하는 인증서버가 필요하다. 인증서버와 사용자 인증을 수행하는 단말사이의 통신은 해시 값을 이용하여 통신함으로 보안성을 높일 수 있다.

또한, 일회용 패스워드 기반의 스마트 지갑은 지불 서비스 이외에도 출입인증수단으로 이용될 수 있다.

## 1. 서론

최근 스마트폰의 기술적 발달과 대중화로 2008년 아시아에서의 모바일 가입자 중 43.9%가 스마트폰을 소유하고 있으며, 2013년 49.8%에 이를 것으로 예상되고 있다. 증가하는 스마트폰 가입자를 위해서 각 이동통신사는 관련 인프라를 대폭적으로 확대하고 있으며, 기존에 독립적으로 제공되던 다양한 사용자 편의 서비스들이 스마트폰 안에 하나로 통합되고 있다. 이런 서비스를 스마트지갑이라고 하며, 이에 대한 연구가 시작되고 있는 단계이다. 모바일 지갑은 사용자의 다양한 지불 결제 서비스를 제공할 뿐만 아니라 향후에는 사용자의 디지털 ID 정보를 활용하여 다양한 개인화 서비스를 제공하는 하나의 모바일 단말 어플리케이션 플랫폼으로 발전할 것이다.

모바일 지갑은 근거리 내 다양한 단말들과 무선통신을 통해 사용자 디지털 ID정보 및 결제 관련 정보와 같은 개인정보를 송수신함으로써 다양한 지능형사용자의 편의 서비스를 제공한다.

하지만 무선통신은 공자에게 쉽게 노출될 수 있는 취약성이 존재한다. 때문에 수많은 개인정보의 전달이 이루어지는 모바일 지갑 서비스의 통신에 대한 보안 기술의 연구 개발이 필요하다. 본 논문에서는 모바일 지갑에 적용되는 무선통신 보안에 대해서 알아보고, 현재의 모바일지갑의 보안 문제를 해결할 수 있는 일회용패스워드 기반의 스마트 지갑 인증방법에 대해서 제안한다.

## 2. 모바일 지갑의 개념

모바일 지갑은 작게는 모바일 단말용 클라이언트 소프트웨어를 의미한다. 크게는 이를 지원하니 위한 서버군까지 포함되어 구성되는 시스템이다. 모바일 단말에 저장, 이용되는 개인 정보를 모바일 ID[1]라 한다. 모바일 ID를 구성하는 종류는 <표 1>과 같다.

<표 1> 모바일 ID의 구성

| 종류 | 내용 |
|---|---|
| 오프라인 ID | 주민등록번호, 신분증, 시용카드번호 |
| 온오프라인 인증수단 | 출입증, ID, PW, 스마트키 등 |
| 정태적 개인정보 | 구매기록, 이동기록, 출입기록 |
| 퍼스널 컨텍스트 | 사용자 위치, 시간, 주변 환경 |
| 관심정보 | 선호도, 관심 분야 |

모바일 지갑 서비스의 개념은 다음과 같은 것들이 있다.

- 모바일 ID를 무선통신을 통해 모바일 단말에 발급받아 안전하게 저장, 관리
- 모바일 ID를 온오프라인 환경의 인증, 신원 확인, 지불

에 안전하고 편리하게 사용

- 위 과정에서 자체 프로파일링된 동태적 개인정보를 개인화 서비스를 위하여 프라이버시를 보호하며 제공

스마트 지갑은 무선통신을 통해 인증정보, ID, 지불정보와 같은 모바일 자격정보를 발급받는다. 이러한 모바일 자격정보는 모바일 지갑의 부정사용방지 기능에 의해 안전하게 유지될 수 있다. 또한, 모바일지갑을 이용해 결제, 온오프라인 ID 증명 및 기타 다양한 사용자 편의 서비스들을 수행한다. 이때 무선통신을 통해 통신이 이루어진다. 또한 모바일지갑 사용 과정의 개인 활동은 모바일지갑 내에 프로파일링되어 축척된다. 축척된 개인정보는 개인화 서비스에 제공될 수 있다. 개인화 서비스의 예로는 이용자 기반광고, 라이프스타일미디어, 네트워크 기반 IT서비스 등이 있다.

## 3 관련 연구

모바일지갑은 근거리 내의 단말과 페어링 과정을 거친 뒤 서비스가 제공된다. 모바일지갑의 페어링(Device pairing)기술에는 Diffie-Hellman(DH) 프로토콜[2]을 사용한다. DH프로토콜을 사용하는 페어링에는 세션확립이 중요하다. 세션확립 과정 중 중간자 공격 위협에 대한 노출 문제가 존재한다. 페어링을 통해 확립된 세션키의 무결성을 검증하기 위해 OOB(Out-Of Band)채널을 활용하는 기술들이 제안되고 있다.

### 3.1 이미지 비교

페어링을 통해 양 단말 사이에 확립된 세션 키의 무결성을 확인하는 가장 확실한 방법은 OOB 채널을 통해 사용자가 직접 비교확인 하는 방법이다. 하지만 사용자가 직접 세션 키의 바이너리 값을 비교 판단하기에는 그 길이나 너무 길다.

따라서 세션 키의 해시를 통해 생성된 인증코드를 OOB 채널의 이미지로 출력하여 사용자의 시각을 통해 직접 양 단말 출력 이미지 사이의 동일 여부를 비교 판단하여 공개키의 무결성을 확인하는 기술들을 제안하였다. 하지만 세션 키의 해시 이미지에 대한 second pre-image[3] 공격에 취약하다.

### 3.2 Seeing-is-Believing

초기 OOB 채널 인증 기법을 사용하는 페어링 방법들은 사용자가 인증 코드의 진위 여부를 결정하는 UC기반이다. 하지만 UC 기반 페어링 방법은 사용자 판단 오류비율이 안전성에 영향을 미치는 한계가 있다. 따라서 Mccune, et al.[4]이 제안한 Seeing-is-Believing(SiB) 기술은 2차원 바코드로 인코딩된 인증코드를 수신 단말의 카메라가 그 값을 읽고, 인증 코드의 진위 여부를 단말 스스로 판단하는 DC 페어링 방법을 사용하였다. 바코드로 표현되는 인증코드는 공개키에 대한 해시 값을 사용한다. 이는 역시 second pre-image 공격에 취약하다. 하지만 SiB기술은 여러 개의 바코드를 사용하는 다중 바코드 방법과 DH 공개키에 대한 해시를 사용하는 방법을 제안하였다.

### 3.3 비주얼 채널 페어링

Saxena, et al.는 인증코드를 SiB의 바코드 대신 LED의 점멸로 표현하는 또 다른 비주얼 채널 페어링 기술을 제안하였다. 비주얼 채널 페어링 기술은 LED의 점멸 패턴 값을 수신하기위해 SiB 기술과 마찬가지로 카메라를 필요로 한다. 하지만 비주얼 채널 페어링 기술은 LCD 디스플레이 대신 하나의 LED만을 요구하므로 SiB 기술보다 송신 단말의 하드웨어 요구 조건이 낮다.

### 3.4 Loud and Clear

SiB와 비주얼 채널 페어링 기술에 필요한 카메라는 모바일 기기의 필수 요소가 아니며, 장착되어 있더라도 바코드를 인식하기 위해서는 촬영에 필요한 충분한 빛이 확보되어야 한다. 따라서 SiB나 비주얼 채널 페어링에서 사용되는 비주얼 채널 대신, Goodrich, et al.는 오디오 채널 페어링 기술 Loud and Clear(L&C)을 제안하였다. SiB 기술은 인증코드를 바코드로 표현한 반면 L&C 기술은 해당 데이터를 표현하는 단어들이 포함된 일련의 문장을 음성으로 들려주는 text-to-speech기법을 사용한다. 사용자는 양 단말의 스피커를 통해 출력되는 문장의 동일성 여부를 판단하거나 한 쪽 단말의 디스플레이를 통해 출력되는 문장과 다른 쪽 단말의 스피커를 통해 출력되는 문장의 동일성을 판단한다.

### 3.5 BEDA

Claudio Soriente, et al.에 의해 제안된 Button-Enabled Device Association(BEDA) 기술은 OOB채널로써 모바일 기기의 버튼 인터페이스를 사용한다. 따라서 기존의 다른 기술보다 하드웨어 요구사항이 가장 적다. BEDA 기술은 한 쪽 단말의 LED나 진동과 같은 출력을 사용자가 다른 쪽 단말의 버튼을 통해 입력하는 방법과 또는 사용자가 양 단말의 버튼을 동시에 누르고 때는 방법으로 비밀 값을 공유하게 된다. 이와 같이 양 단말 간에 공유된 비밀 값과 MANA-3 응용 프로토콜을 사용하여 안전하게 DH 공개키 값을 교환 하고 세션 키를 확립한다.

### 3.6 HAPADEP

기존 페어링 기술들은 인증 기술에는 OOB 채널을 사용하는데 반해 DH 키 공유는 WiFi 기반의 Ad-hoc연결을 사용한다. 이때 인증과정과 별개로 Ad-hoc 설정 과정은 사용자에게 사용성 측면에서 부담으로 다가올 수 있다. 따라서 Claudio Sorinete, et al.는 L&C 기술을 확장하여 키

공유 채널과 인증 채널 모두 오디오 채널을 사용하는 Human Assisted Pure Audio Device Pairing (HAPADEP)기술을 제안하였다. HAPADEP 기술의 DH 공개키 값은 fast codec으로 인코딩되어 공개키 교환 오디오 채널을 통해 빠르게 전송되고, 공개키 인증 코드는 slow codec으로 인코딩된 후 인증 오디오 채널로 전송되어 사용자의 정확한 공개키 인증을 돕는다. HAPADEP 기술의 인증 방법은 기존 L&C 기술과 같은 text-to-speech 비교 기법과 인증코드를 음계로 매핑한 멜로디 비교 기법을 제공한다.

### 3.7 Shake Well Before Use

OOB 채널을 통해 사용자가 세션 키 공유 과정에 직접 개입하는 페어링 방법들이 많이 연구되어오면서, 기존 OOB 채널을 사용하는 페어링 기술들의 사용성 분석에 대한 연구들과 함께 사용성 개선을 위한 연구가 계속되었다. Mayrhofer, et al.에 의해 제안된 Shake Well Before Use 기술은 양 모바일 단말을 함께 흔들어 줌으로써 가속 센서 값을 통해 비밀 값을 공유하고 이 비밀 값과 Interlock 프로토콜을 사용하여 안전하게 DH 공개키 교환 및 세션 키를 확립한다. 단순히 양 단말을 손에 들고 흔드는 동작만을 요구하므로 기존 페어링 기술들에 비해 사용성이 뛰어나다. 하지만 이와 같은 Shake Well Before Use 페어링 기법은 사람의 손으로 흔들기 무리가 없을 정도의 작은 크기의 모바일 단말 사이에서만 사용이 가능한 한계가 있다.

## 4. 일회용 패스워드 기반 인증

스마트지갑 클라이언트와 결제 단말간의 페어링을 위한 방법에 대해서 다양한 연구가 진행되고 있다. 현재의 페어링 과정에 사용되는 인증 방법은 이미지를 비교, LED점멸 등과 같은 원시적 차원의 방법을 통하여 인증을 수행한다. 또한 스마트지갑 클라이언트가 설치되어 있는 스마트폰을 분실했을 경우 사용자가 분실한 스마트폰에 부여받은 모바일 자격정보를 부인하기 전까지 사용이 가능하다는 단점이 존재한다. 이러한 단점을 해결하기 위해서 스마트폰과 단말 간의 통신을 수행하기 이전에 일회용 패스워드(OTP)를 이용하여 스마트폰을 소유하고 있는 소유자가 정당한 소유자인지를 확인한다. 또한 일회용 패스워드를 사용함으로써 스마트폰과 단말 사이의 페어링 과정에 발생할 수 있는 중간자 공격에 대해서 예방할 수 있다.

### 4.1 OTP의 특징

일반적인 패스워드는 정상적인 인증 수단으로 네트워크 도청으로 인해 패스워드를 알아냈을 경우 불법적으로 재사용할 위험이 있다. 그러나 OTP는 이미 사용된 패스워드는 재사용하지 않으므로 네트워크 도청을 통하여 패스워드를 알아냈다 할지라도 더 이상 사용할 수 없으므로 이러한 위험을 방지할 수 있다.[5] 따라서 OTP는 정적인 패스워드 사용에 따른 위험을 해결하고 개인 정보 유출에 따른 사용자 인증을 강화하기 위해 도입되었다. OTP는 OTP 생성매체에 의해 필요한 시점에 발생되고 매번 다른 번호를 생성한다.

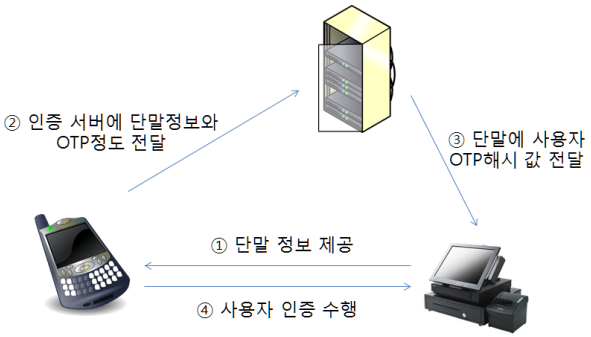
OTP는 사용자가 가지고 있는 OTP생성매체와 이에 의해 새성되는 패스워드로 사용자 인증을 수행하므로 이 중요소 인증 수단으로 정적인 패스워드와 같은 한 가지 인증요소만으로 인증 받는 방식에 비해 높은 보안 수준을 갖는다.

### 4.2 OTP를 이용한 스마트지갑 인증을 위한 구성

OTP를 이용한 스마트지갑 인증과정은 스마트폰, 스마트폰과 통신을 하기 위한 단말, 사용자의 모바일ID의 인증을 수행하는 서버로 구성된다.

사용자는 OTP를 이용하여 스마트지갑 인증을 위해서는 사전에 단말 혹은 인증서버에 자신의 모바일 자격정보와 OTP정보를 등록해야 한다.

사용자가 인증하려는 단말에는 사용자의 OTP정보를 저장되어 있지 않다. 따라서 사용자의 OTP정보에 대한 신뢰를 하기 위해서 인증 서버가 필요하다. 단말과 인증서버 간의 통신을 위해 네트워크가 연결되어 있어야 한다.




(그림 1) OTP를 이용한 인증 과정


(그림 2) 단말 정보 입력 화면


(그림 3) OTP 발급 화면

또한 단말에는 사용자의 OTP정보를 입력할 수 있는 키패드가 제공되어야 한다.

인증서버는 사용자와 단말 간의 인증을 위한 정보를 제공한다. 사용자가 인증서버에 단말 정보와 OTP정보를 전송하게 하면, 단말 정보와 OTP정보를 혼합하여 해시 값을 생성한다. 이렇게 생성된 해시 값을 단말에게 전달한다.

### 4.3 OTP를 이용한 스마트 지급 인증 과정

사용자와 단말 간의 인증을 위해서 사전에 인증 서버에 사용자의 모바일 자격정보와 OTP정보가 등록되어 있다고 가정한다.

사용자는 인증을 받기 위해서 (그림 2)와 같이 스마트지갑 클라이언트에 단말의 정보와 OTP를 발급받기 위한 패스워드를 입력한다.

사용자의 입력이 완료 되면 모바일 정보와 OTP정보를 인증서버에 전달한다. 인증서버는 사용자로부터 전달 받은 정보를 이용하여 단말에게 인증에 사용될 해시 값을 전송한다.

사용자는 스마트지갑에 표시되는 OTP번호를 단말에 입력한다. 단말은 사용자가 입력한 OTP번호와 자신의 정보를 연산하여 해시 값을 생성한다. 생성된 해시 값과 인증서버로부터 전송받은 해시 값을 비교하여 사용자 인증을 수행한다.

## 5. 결론

S통신사에서 제공되고 있는 스마트지갑 어플리케이션의 경우 바코드를 이용하여 사용자 인증을 수행한다. 이는 별도의 바코드를 인식할 수 있는 스캐너가 필요하다. 스캐너가 없거나 보안상의 이유로 스캐너를 사용할 수 없는 경우 사용자 인증을 수행할 수 없다는 단점이 있다.

본 논문에서 제안하는 일회용 패스워드 기반의 스마트지갑은 인증을 위해서 바코드 스캐너등과 같은 추가 장비가 필요하지 않다. 이러한 장점으로 보안을 위해서 스캐너를 사용하지 못하는 곳에서 스마트지갑을 이용할 수 있다. 또한 출입 인증 단말에 키패드가 존재하면 스마트지갑을 출입인증 수단으로 사용할 수 있을 것이다.

향후 일회용 패스워드 기반의 스마트지갑의 구성요소에서 발생할 수 있는 보안취약점을 분석하고 이를 보안할 수 있는 방법에 대한 연구가 진행되어 질 것이다.

## 참고문헌

[1] 마건일, 이정현, 최대선, "모바일 지갑을 위한 스마트 채널 보안 기술 동향", 한국정보보호학회, 정보보호학회지, 제21권 제4호 2011.6, page(s): 7-13

[2] 박선영, 김주영, 송홍협, "표준 모델에서 안전한 Diffie-Hellman키 교환 프로토콜", 한국정보과학회, 정보과학회논문지 : 정보통신, 제35권 제6호 2008.12, page(s): 465-473

[3] B.A. Forouzan, Cryptography and network security, 1th Ed., McGraw-Hill, 2008.

[4] J.M. McCune, A. Perrig, and M.K. Reiter, "Seeing-is-Believing: Using camera phones for human-verifiable authentication", IEEE Symposium on Security and Privacy, pp. 110-124, May 2005.

[5] 김기영, "일회용 패스워드를 기반으로 한 인증 시스템에 대한 고찰", 한국정보보호학회, 정보보호학회지, 제17권 제3호 2007.6, page(s): 26-31