情 報 保 護 學 會 誌
第21卷 第4號, 2011. 6

모바일 지갑을 위한 스마트 채널 보안 기술 동향

마 건 일*, 이 정 현**, 최 대 선***

요 약

모바일 지갑은 사용자의 디지털 ID 정보를 활용하여 다양한 개인화 서비스를 제공하고, 사용자의 갖고 있는 지불 수단을 통합하여 지능형 지불 결제 서비스를 제공하는 하나의 모바일 단말 어플리케이션이다. 이러한 모바일 지갑 서비스는 근거리 범위의 다양한 단말과 무선통신을 통해 이루어진다. 이때 무선통신은 사용자의 디지털 ID 정보와 지불정보 데이터를 포함하고, 모바일 지갑은 이를 통해 다양한 사용자 편의 서비스를 제공하므로 이를 스마트 채널이라 부른다. 하지만 무선 통신은 근본적으로 공격자에게 쉽게 노출 될 수 있는 취약점이 존재한다. 따라서 모바일 지갑 서비스가 안전하게 이루어지기 위해서는 근거리 무선 단말간의 세션 보호 기술 연구 개발이 반드시 필요하며, 실제 이에 관련된 많은 연구가 진행되어왔다. 모바일 지갑을 위한 스마트 채널 보안 기술의 효과적인 연구를 위해 본 논문에서는 모바일 지갑의 스마트 채널 보안 기술로 응용될 수 있는 기존의 근거리 무선 단말 간 세션 보호 기술 연구 사례를 조사 분석해본다.

Ⅰ. 서 론

최근 계속되는 스마트폰의 기술적 발전과 스마트폰 중심 인프라의 대폭적 확대로, 기존에 독립적으로 제공되었던 다양한 사용자 편의 서비스들이 하나의 스마트폰 안으로 통합되고 있다. 이러한 스마트폰 중심 서비스의 행보는 특히 모바일 지갑에 대한 연구 개발 필요성을 가져왔으며, 이에 대한 활발한 연구개발이 진행되고 있다. 모바일 지갑은 사용자의 다양한 지불 수단을 통합하여 지불 결제 서비스를 제공할 뿐만 아니라, 향후에는 사용자의 디지털 ID 정보를 활용하여 다양한 개인화 서비스를 제공하는 하나의 모바일 단말 어플리케이션 플랫폼이다.

모바일 지갑은 근거리 내 다양한 단말들과 무선통신을 통해 사용자 디지털 ID정보 및 결제 관련 정보와 같은 개인정보를 송수신 함으로써 다양한 지능형 사용자 편의 서비스를 제공한다. 모바일 지갑과 단말 사이의 이와 같은 무선 통신은 와이파이, 블루투스, NFC 등의 여러 무선 채널을 통해 이루어질 수 있으며, 본 논문에서는 이와 같은 모바일 지갑의 무선 통신채널을 스마트 채널이라 통칭한다.

하지만 무선통신은 공격자에게 매우 쉽게 노출될 수 있는 취약성이 존재한다. 때문에 수많은 개인정보 송수신이 이루어지는 모바일 지갑 서비스가 실제 이루어지기 위해서는 스마트 채널에 대한 보안 기술의 연구 개발이 반드시 필요하다. 따라서 본 논문에서는 스마트 채널의 보안 이슈를 분석하고, 현재까지의 스마트 채널 보안 기술 연구 동향을 정리하고 분석해 봄으로써 향후 모바일 지갑을 위한 스마트 채널 보안기술 연구의 바탕을 마련한다.

본 논문의 구성은 다음과 같다. 2장에서는 모바일 지갑의 개념을 살펴본다. 3장에서는 스마트 채널 보안 이슈를 분석해 보고, 4장에서는 현재까지의 스마트 채널 보안 기술 동향을 살펴본다. 이후 5장에서는 기존 스마트 채널 보안 기술을 분석해보고 6장에서 결론을 맺는다.

Ⅱ. 모바일 지갑 개념

모바일 지갑은 작게는 모바일 단말용 클라이언트 소프트웨어이며, 크게는 이를 위한 지원 서버군까지 포함

본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업의 일환으로 수행하였음.(10035219-2010-01)
* 숭실대학교 대학원 컴퓨터학과 석사과정(gima@ssu.ac.kr)
** 숭실대학교 컴퓨터학부 교수 (jhyi@ssu.ac.kr)
*** 한국전자통신연구원 책임연구원 (sunchoi@etri.re.kr)

〔표 1〕 모바일 지갑에 저장되는 모바일 ID의 구성

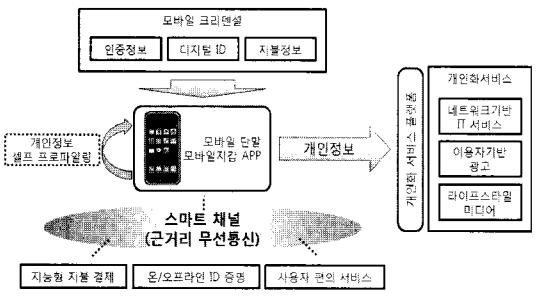
종류	내용
온오프라인 ID	주민등록번호, 신분증, 신용카드번호
온오프라인 인증수단	출입증, ID, PW, 스마트키 등
정태적 개인정보	구매기록, 이동기록, 출입기록
퍼스널 컨텍스트	사용자 위치, 시간, 주변 환경
관심정보	선호도, 관심 분야

되어 구성되는 시스템이다. 모바일 단말에 저장, 이용되는 개인 정보를 모바일 ID[1]라 하며, 구성은 [표 1]과 같다. 모바일 지갑 서비스 개념은 다음과 같다.

- 모바일 ID를 스마트 채널 통신을 통해 모바일 단말에 발급받아 안전하게 저장, 관리
- 모바일 ID를 온오프라인 환경의 인증, 신원 확인, 지불에 안전하고 편리하게 사용
- 위 과정에서 자체 프로파일링된 동태적 개인정보를 개인화 서비스를 위하여 프라이버시를 보호하며 제공

스마트 채널 통신을 통해 이루어지는 이러한 모바일 지갑 서비스의 개념은 [그림 1]에 표현되어있다.

모바일 지갑은 통신 채널을 통해 인증정보, ID, 지불정보와 같은 모바일 크리덴셜을 발급받는다. 이러한 모바일 크리덴셜은 모바일 지갑의 부정사용방지 기능에 의해 안전하게 유지될 수 있다. 모바일지갑을 이용해 스마트지불, 온/오프라인 ID 증명 및 기타 다양한 사용자 편의 서비스들을 수행하고, 이때 근거리 무선통신의 스마트 채널을 통해 통신이 이루어진다. 또한 모바일 지갑 사용 과정의 개인 활동은 모바일 지갑 내에 프로파일링되어 축적된다. 축적된 개인정보는 개인화 서비스에 제공될 수 있다. 개인화 서비스의 예는 이용자기반광고, 라이프스타일미디어, 네트워크 기반 IT서비스가 있다.[1]



〔그림 1〕 모바일 지갑 서비스 개념

Ⅲ. 스마트 채널 보안 이슈

모바일 지갑의 안전한 스마트 채널을 위해서는 스마트 채널 양 단말 사이의 비밀키 공유와 공유된 비밀키로 암호화되는 세션 확립이 필요하다. 따라서 스마트 채널 보안기술의 핵심은 양 단말 사이의 세션키를 안전하게 공유하는데 있다.

3.1 모바일 지갑 서비스 환경

모바일 지갑은 다양한 단말과 매번 새로운 근거리 무선통신을 통해 지불 서비스를 포함하는 여러 개인 편의 서비스를 제공할 수 있다. 따라서 모바일 지갑의 스마트 채널 보안 기술은 사전공유 값이 없어야 하며 공통의 TTP(Trusted Third Party)나 오프라인 CA(Certification Authority), PKI(Public Key Infrastructure)를 필요로 하지 않고, 통신 구간이 짧은 특성이 고려되어야 한다.

Diffie-Hellman(DH)[2] 프로토콜을 사용하는 디바이스 페어링(Device pairing) 기술은 이러한 모바일 지갑의 스마트 채널 보안 기술 요구사항을 충족한다. 페어링은 서로 다른 두 디바이스가 어떠한 사전 공유 값없이 근거리 무선 통신을 통해 세션을 확립하는 과정을 일컫는다.

3.2 중간자 공격

DH 프로토콜을 사용하는 페어링을 통한 세션 확립의 가장 큰 문제점은 중간자 공격[3] 위협에 대한 노출이다. 페어링을 통해 세션을 확립할 때 사용자는 중간자 공격의 침해 여부를 확인하기 어렵다. 따라서 페어링을 통해 확립된 세션키의 무결성을 검증하기 위해 OOB (Out-of-Band) 채널을 활용하는 기술들이 제안되고 있다. OOB 채널 인증 기법은 인증과정에 사용자의 개입이 이루어지므로 보안성과 사용성을 동시에 고려해야하는 문제가 있다.

3.3 사용성과 보안성

OOB 채널 인증 기법은 인증 판단 주체에 따라 크게 사용자 결정(UC: User Controlled) 방법과 단말 결정

(DC: Device Controlled) 방법으로 나뉠 수 있다.[4] UC 방법은 사용자가 OOB 채널의 출력을 통해 직접 세션키의 위변조 여부를 판단하는데 반해, DC 방법은 단말 스스로 OOB 채널을 통해 세션키 위변조 여부를 판단한다. UC 방법은 추가적인 인증절차 없이 간단한 확인 과정만을 요구하므로 사용성이 높은 장점이 있는 반면 Rushing User[4]에 대한 취약점이 존재한다. Rushing User란 인증과정에 신중한 판단 없이 무조건적인 승낙결정으로 확인단계를 자체 생략하는 사용자를 말한다. DC 방법은 추가적인 인증절차를 요구하므로 사용성이 비교적 낮은 반면 rushing user에 대한 취약점은 없다. OOB 채널의 좁은 대역폭 또한 사용성에 대한 핵심 고려 요소이다. OOB 채널의 출력에 대한 사용자의 직접적인 개입을 통해 세션키 인증과정이 진행 되므로 OOB 채널에 사용되는 데이터의 크기는 제한적일 수 밖에 없다.

Ⅳ. 스마트 채널 보안 기술 동향

스마트 채널 보안 기술의 동향은 기존 페어링의 보안 기술연구 동향에서 찾을 수 있다. 본 장에서는 스마트 채널 보안기술로 사용되는 페어링 기술 동향에 대해 살펴본다.

4.1 이미지 비교

페어링을 통해 양 단말 사이에 확립된 세션키의 무결성을 확인하는 가장 확실한 방법은 OOB 채널을 통해 사용자가 직접 비교확인 하는 방법이다. 하지만 사용자가 직접 세션키의 바이너리 값을 비교 판단하기에는 그 길이나 너무 길다. 이에 바이너리 값을 사용자가 인식할 수 있는 길이로 짧게 자르는 방법이 있지만 이는 보안성이 취약하다.

따라서 세션키의 해쉬를 통해 생성된 인증코드를 OOB 채널의 이미지로 출력하여 사용자의 시각을 통해 직접 양 단말 출력 이미지 사이의 동일 여부를 비교 판단하여 공개키의 무결성을 확인하는 기술들[5][6]을 제안하였다. 하지만 이러한 기술은 랜덤 이미지 생성 알고리즘, 고해상도의 출력 이미지로 인해 비교적 높은 사양의 모바일 단말 하드웨어를 요구, 그리고 이미지의 복잡성으로 인한 사용성 저하의 단점이 있다. 또한 보안성 측면에서 세션키의 해쉬 이미지에 대한 second pre-image[3] 공격에 취약하다.

4.2 Seeing-is-Believing

초기 OOB 채널 인증 기법을 사용하는 페어링 방법들은 사용자가 인증 코드의 진위 여부를 결정하는 UC 기반이다. 하지만 UC 기반 페어링 방법은 사용자 판단 오류비율이 안전성에 영향을 미치는 한계가 있다. 따라서 Mccune, et al.[7]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 해쉬 값을 사용하며 68비트 길이를 사용한다. 이는 역시 second pre-image 공격에 취약하다. SiB기술은 이와 같은 공격에 대한 대응으로 여러 개의 바코드를 사용하는 다중 바코드 방법과 DH 공개키에 대한 해쉬를 사용하는 방법을 제안하였다. 하지만 다중 바코드 기법은 여러 개의 12X12 크기 그리드의 바코드를 한 화면에 출력할 수 있는 디스플레이가 필요하며 단일 바코드에 비해 사용하기 불편하다.

4.3 Blinking-is-Believing

Saxena, et al.[8]는 인증코드를 SiB의 바코드 대신 LED의 점멸로 표현하는 또 다른 비주얼 채널 페어링 기술을 제안하였다. 본 논문에서는 이 기술을 Blinking-is-Believing(BiB)라 부른다. BiB 기술은 LED의 점멸 패턴 값을 수신하기위해 SiB 기술과 마찬가지로 카메라를 필요로 한다. 하지만 BiB 기술은 LCD 디스플레이 대신 하나의 LED만을 요구하므로 SiB 기술보다 송신 단말의 하드웨어 요구 조건이 낮다. 또한 비주얼 채널을 통해 단 방향 상호인증이 가능한 VIC (Visual authentication based on Integrity Checking) 프로토콜[8]을 사용함으로써 SiB의 양 방향 상호인증의 절차를 간소화 했다. 또한 VIC 프로토콜은 MANA-3[9] 프로토콜을 활용하여 난수가 포함된 해쉬를 생성하므로 second pre-image 공격에 대해 안전하다.

4.4 Loud and Clear

SiB와 BiB 기술에 필요한 카메라는 모바일 기기의 필수 요소가 아니며, 장착되어 있더라도 바코드를 인식하기 위해서는 촬영에 필요한 충분한 빛이 확보 되어야

한다. 뿐만 아니라 높은 수준의 보안이 요구되는 시설에서 카메라 사용은 제한될 수 있다. 따라서 SiB나 BiB에서 사용되는 비주얼 채널 대신, Goodrich, et al.[10]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-speech 기법을 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. 또는 양 단말 모두 디스플레이를 통해 문장을 출력할 수 도 있다. L&C 기술은 이와 같이 사용자에게 비주얼 채널과 오디오 채널 모두 제공함으로써 사용 환경에 따른 사용성을 높였다.

4.5 BEDA

Claudio Soriente, et al.[11]에 의해 제안된 Button-Enabled Device Association(BEDA) 기술은 OOB 채널로써 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 단말간에 공유된 비밀 값과 MANA-3 응용 프로토콜을 사용하여 안전하게 DH 공개키 값을 교환 하고 세션키를 확립한다.

4.6 HAPADEP

기존 페어링 기술들은 인증 기술에는 OOB 채널을 사용하는데 반해 DH 키 공유는 WiFi 기반의 Ad-hoc 연결을 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)[12] 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.

이와 같이 사람이 직접 비교 판단하는 인증 오디오 채널을 사용하는 일반적인 HAPADEP 기술과 달리, 인증 오디오 채널에서 사용자 개입 없이 단말의 마이크로폰을 통해 전송받은 인증코드를 사용하여 단말이 공개키 위변조 유무를 판단하는 응용 HAPADEP[13] 기술 또한 제안되었다.

4.7 Shake Well Before Use

OOB 채널을 통해 사용자가 세션 키 공유 과정에 직접 개입하는 페어링 방법들이 많이 연구되어오면서, 기존 OOB 채널을 사용하는 페어링 기술들의 사용성분석에 대한 연구들[13][14]과 함께 사용성 개선을 위한 연구가 계속되었다. Mayrhofer, et al.[15]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 프로토콜[16]을 사용하여 안전하게 DH 공개키 교환 및 세션키를 확립한다. 단순히 양 단말을 손에 들고 흔드는 동작만을 요구하므로 기존 페어링 기술들에 비해 사용성이 뛰어나다. 하지만 이와 같은 흔들기 페어링기법은 사람의 손으로 흔들기 무리가 없을 정도의 작은 크기의 모바일 단말 사이에서만 사용이 가능한 한계가 있다.

[표 2]는 위 스마트 채널 보안기술들의 특징 요약을 보여준다.

V. 스마트 채널 보안기술 분석

본 장에서는 스마트 채널 보안기술 분석으로써 4장에서 살펴본 스마트 채널 보안기술들의 안정성 및 사용성을 비교 분석하여 본다.

5.1 안전성 분석

스마트 채널 보안 기술의 안전성은 해당 기술이 사용하는 세션 키 공유 프로토콜에 기반 한다. 위에서 설명한 페어링 기술들은 모두 세션 키 공유 프로토콜로써

〔표 2〕 스마트 채널 보안 기술 특징 요약

페어링 기법		단말 요구사항		사용자 행동 내용		OOB 채널	프로토콜/ 알고리즘
		송신 단말	수신 단말	1단계: 교환	2단계: 결과		
이미지 비교		디스플레이		두 이미지 비교	허가/거부 입력	비주얼	Hash
SiB		디스플레이	사진카메라	송신 단말 바코드를 수신 단말의 카메라를 통해 촬영	수신 단말의 판단을 토대로 송신 단말에 허가/거부 입력	비주얼	Hash, DH
BiB		LED	비디오카메라/ 빛 감지기기	송신 단말 LED 점멸을 수신 단말의 카메라를 통해 촬영	수신 단말의 판단을 토대로 송신 단말에 허가/거부 입력	비주얼	DH, MANA-3
L&C	디스플레이 -스피커	한쪽 단말에 디스플레이, 다른 한쪽 단말에 스피커		들리는 문장과 디스플레이의 문장 비교	양 단말에 허가/거부 입력	오디오+ 비주얼	Hash, DH
	스피커-스피커	스피커		들리는 두 문장 비교		오디오	
BEDA	진동-버튼	진동	한 개의 버튼	송신 단말의 각 신호(진동, LED, 비프)에 따라 수신 단말의 버튼 누르기	수신 단말의 판단을 토대로 송신 단말에 허가/거부 입력	촉각	DH, MANA-3
	LED-버튼	LED					
	비프-버튼	beeper					
	버튼-버튼	한 개의 버튼		양 단말의 버튼을 동시에 누르고 뗌을 출력 신호음 발생 전까지 반복 수행	동기화가 이루어지지 않으면 오류발생		
HAPADEP		스피커	마이크로폰	수신 단말의 신호음 대기 후 들리는 두 문장/멜로디 비교	수신 단말의 판단을 토대로 송신 단말에 허가/거부 입력	오디오	Hash, DH
Shake Well Before Use		2축 가속센서		출력 신호음 발생 전까지 양 단말을 함께 흔들기	동기화가 이루어지지 않으면 오류발생	촉각+ 움직임	DH, Interlock

공개키 해쉬값 전송 기법이나 DH 응용 프로토콜을 사용한다. 하지만 해쉬의 사용은 second pre-image 공격에 취약할 수 있고, 본래 DH 프로토콜은 중간자공격에 취약하다. 따라서 각 페어링 기술은 이와 같은 공격에 대한 대응하는 키 공유 프로토콜 및 사용하는 인증코드 길이에 따라 안정성 수준이 결정된다. [표 3]은 스마트 채널 보안 기술별 안전성 비교를 보여준다.

〔표 3〕 스마트 채널 보안 기술별 안전성 비교

페어링 기술		중간자 공격 성공 확률	second pre-image 공격 저항성	인증 코드길이 (비트)
SiB	단일 바코드	$2^{-n/2}$	×	68
	멀티 바코드	$2^{-n/2}$	○	68γ
BiB		$n2^{-n}\sum_{i=0}^{r}\binom{n}{i}$	○	24
L&C		$2^{-n/2}$	×	70
BEDA		2^{-n}	○	21
HAPADEP		$2^{-n/2}$	×	80
Shake Well Before Use		2^{-n}	-	$n \propto t$

기호설명; n: 인증 코드 비트길이, γ: 바코드 개수, r: 허용 오류개수, t: 흔들기 소요시간

안전성 분석 결과 MANA-3 프로토콜을 사용하는 BiB 기술 및 BEDA 기술이 짧은 길이의 인증코드를 사용하면서 동시에 높은 안전성을 보장하고 있다. 따라서 스마트 채널 보안 기술은 공개키에 대한 해쉬값을 인증코드로 바로 사용하는 방법 보다는 MANA-3프로토콜과 같이 양 단말간의 난수로 생성되는 인증코드를 사용하는 것이 인증코드의 길이를 줄이면서도 높은 안전성 보장에 유리하다.

5.2 사용성 분석

본 논문의 스마트 채널 보안 기술의 사용성 분석은 세션 키 확립까지의 소요시간과 치명적 에러비율 및 안전 에러비율을 기준으로 분석한다. 각 스마트 채널 보안 기술에 대한 세션 키 확립 소요시간 및 에러비율 측정

〔표 4〕 스마트 채널 보안 기술별 사용성 비교

기술 분류	페어링 기술		소요 시간(초)	fatal 에러	safe 에러
UC	이미지 비교		12.7	0%	15%
	L&C	디스플레이 -스피커	15.5	5%	0%
		스피커-스피커	21.3	10%	0%
DC	BiB		28.8	-	0%
	SiB		26.9	-	5%
	BEDA	버튼-버튼	31.9	-	-
	변형 HAPADEP		10.8	-	5%

에 대한 자료는 Ersin Uzun, et al.[13]의 Caveat Emptor 연구를 참조하였다. [표4]는 스마트 채널 보안 기술별 사용성 비교를 보여준다.

변형 HAPADEP 기술을 제외하고는 UC 방법의 페어링 기술들이 DC 방법이 페어링 기술들 보다 빠른 수행속도를 보인다. 이러한 결과는 DC 방법을 위한 추가적으로 요구되는 사용자의 행동이 UC 방법의 사용자 비교 판단 수행에 비해 사용자에게 더욱 많은 부담을 주는 것을 보여준다. 하지만 UC 방법은 DC에는 없는 치명적 오류의 확률이 존재하는 한계가 있다. 또한 변형 HAPADEP와 같이 추가적으로 요구되는 사용자 행동을 최소화할 경우, 치명적인 에러 발생을 방지함과 동시에 높은 사용성을 제공할 수 있다.

Ⅵ. 결 론

모바일 지갑 서비스는 스마트폰에 저장되어 있는 사용자 신용카드 정보 및 기타 다양한 개인 정보들을 기반으로 스마트 채널을 통해 지불 결제 서비스를 포함한 다양한 사용자 편의 서비스를 제공한다. 이때 스마트 채널은 모바일 지갑과 다양한 근거리 무선 단말 사이의 모든 무선 통신을 통칭한다. 수많은 개인정보 데이터가 송수신되는 스마트 채널은 무선통신을 기반으로 하므로 세션 보호기술이 반드시 필요하다. 또한 모바일 지갑의 세션 보호 기술은 모바일 지갑 특성이 반드시 고려되어야 한다. 이전부터 많은 연구가 진행되고 있는 무선 단말 사이의 안전한 세션을 위한 페어링 기술들은 이러한 스마트 채널의 보안기술로 적용되기 적합하다.

기존 페어링 기술들은 OOB 채널을 통해 세션키의 무결성을 보장하고자 한다. OOB 채널을 통한 페어링 기술은 사용자의 참여를 통해 이루어지며 따라서 사용성에 대한 고려가 필수적이다. 따라서 기존의 페어링 기술들은 충분한 안전성 보장과 동시에 사용성의 극대화를 위한 많은 연구를 진행하였다. 본 논문에서는 이러한 기존 페어링 기술 연구들의 동향을 분석해 보았으며, 이러한 분석은 향후 모바일 지갑의 스마트 채널 보안 기술 연구 방향을 제시해 줄 것으로 판단된다.

참 고 문 헌

[1] 최대선, 진승헌, "모바일 ID 보안 및 프라이버시를 위한 스마트 지갑", 정보과학회지, 27(12), pp. 50-59, 2009년.

[2] W. Diffie and M.E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644 - 654, Nov. 1976.

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

[4] N. Saxena and M. Uddin, "Secure pairing of 'Interface-Constrained' devices resistant against rushing user behavior", Applied Cryptography and Network Security, pp. 34-52, June 2009.

[5] A. Perrig and D. Song, "Hash visualization: A new technique to improve real-world security", Cryptographic Techniques and E-Commerce, pp. 131 - 138, 1999.

[6] I. Goldberg. "Visual key fingerprint Code", 1996.

[7] 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.

[8] N. Saxena, "Secure device paring based on a visual channel", IEEE Symposium on Security and Privacy, pp. 306-313, May 2006.

[9] S. Laur, N. Asokan and K. Nyberg, "Efficient mutual data authentication using manually authentication strings", Cryptography and Network Security, pp. 90-107, Dec 2006.

[10] M.T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun. "Loud and clear: Human-verifiable authentication based on au-

dio", IEEE International Conference on Distributed Computing Systems, July 2006.

[11] C. Soriente, G. Tsudik, and E. Uzun, "BEDA: Button-enabled device association", International Workshop on Security for Spontaneous Interaction, Sep. 2007.

[12] C. Soriente, G. Tsudik, and E. Uzun, "HAPADEP: Human-assisted pure audio device pairing", International Security Conference, pp. 385-400, Sep. 2008.

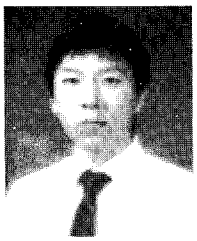
[13] A. Kumar, N. Saxena, G. Tsudik, and E. Uzun, "Caveat emptor: A comparative study of secure device pairing methods", IEEE International Conference on Pervasive Computing and Communications, pp. 1-10, May 2009.

[14] R. Kainda, I. Flechais, and A.W. Roscoe, "Usability and security of out-of-band channels in secure device pairing protocols", Symposium On Usable Privacy and Security, July 2009.

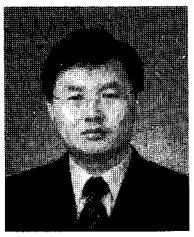
[15] R. Mayrhofer and H. Gellersen, "Shake well before use: Intutive and secure pairing of mobile devices", IEEE Transaction on Mobile Computing, pp. 792-806, 2009.

[16] R.L. Rivest and A. Shamir, "How to expose an eavesdropper", Communications of ACM, vol. 27, no. 4, pp. 393-394, April 1984.

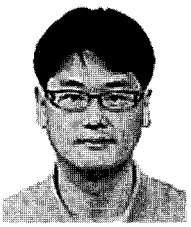
〈著者紹介〉



마 건 일 (Gun Il Ma)
학생회원
2009년 8월 : 숭실대학교 컴퓨터학부 학사
2009년 9월~현재 : 숭실대학교 컴퓨터학과 석사과정
관심분야 : 모바일 보안



이 정 현 (Jeong Hyun Yi)
종신회원
1993년 2월 : 숭실대학교 전자계산학과 학사
1995년 2월 : 숭실대학교 컴퓨터학과 석사
2005년 8월 : University of California at Irvine, Computer Science 박사
1995년 2월 ~ 2001년 8월 : 한국전자통신연구원 연구원
2000년 4월 ~ 2001년 3월 : 미국 표준기술연구원(NIST) 객원연구원
2005년 10월 ~ 2008년 8월 : 삼성종합기술원 수석연구원
2008년 9월 ~ 현재 : 숭실대학교 컴퓨터학부 조교수
관심분야 : 모바일 보안, 네트워크 보안



최 대 선 (Daeseon Choi)
정회원
1995년 2월 : 동국대학교 컴퓨터공학과 학사
1997년 2월 : 포항공과대학교 컴퓨터공학과 석사
2009년 1월 : 한국과학기술원 전산학과 박사
1997년 2월 ~ 1999년 6월 : 현대정보기술 선임연구원
1999년 7월 ~ 현재 : 한국전자통신연구원 책임연구원
2011년 3월 ~ 현재 : 한밭대학교 정보통신·컴퓨터공학부 겸임교수
관심분야 : PKI, 개인정보보호, 모바일 보안