Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.519

스마트워치를 이용한 스마트폰에서의 안전한 전자거래방법*

주 군,[1†] 최 진 춘,[1] 양 대 헌,[1] 이 경 희[2‡]
[1]인하대학교, [2]수원대학교

Secure Transaction Method on Smartphones with Smartwatches*

Jun Zhou,[1†] JinChun Choi,[1] DaeHun Nyang,[1] KyungHee Lee[2‡]
[1]INHA University, [2]The University of Suwon

요 약

기술의 발전에 따라, 스마트폰은 뛰어난 확장성과 성능을 제공한다. 스마트폰에 응용 프로그램을 손쉽게 설치할 수 있는 특징은 사람들의 스마트폰의 다양한 활용을 가능하게 한다. 과거에는 개인용 컴퓨터의 보안성 향상을 위해 스마트폰을 활용하였으나, 최근 스마트폰이 공격자의 주요 대상이 되고 있다. 따라서 스마트폰의 보안을 위해 신뢰할 수 있는 새로운 휴대용 장치가 필요하게 되었다. 스마트글래스, 스마트워치 등과 같은 다양한 웨어러블 장치들이 개발되고 있는데, 이러한 장치들이 우리가 필요한 스마트폰의 보안을 강화할 수 있는 장치로 활용될 수 있을 것이다. 이 논문에서는 스마트폰의 보안을 강화하는 데 있어 스마트워치가 새로운 장치가 될 수 있는지에 대해 연구하고, 스마트워치를 이용한 거래 내역을 확인하고 서명하는 기법과 스마트워치를 이용한 캡차 기반의 거래 내역 확인 기법, 스마트폰을 위한 캡차 기반 거래 연동 OTP 기법을 구현하고 사용자 실험을 통해 결과를 보였다.

ABSTRACT

With the development of technologies, smartphone provides excellent extensibility and performance. Users can install application programs easily in smartphone, so they can use smartphone in various way. In the past, users used smartphone for enhancing security in personal computer. Nowadays, smartphone has become a major target for attackers. Therefore we needs a reliable portable device for smartphone security. There are various wearable devices such as smartglasses and smartwatches, so they can be used for enhancing security in smartphone. In this paper, we study about that smartwatches can be role for enhancing smartphone security, and we implement transaction information verification scheme, Transaction information verification scheme based on CAPTCHA and CAPTCHA based transaction OTP scheme and experiment with users in prototype application.

Keywords: Smartwatch, Smartphone, CAPTCHA, secure transaction

I. 서 론

최근 스마트폰 등의 기기가 사용자들에게 많이 보급됨에 따라 다양한 어플리케이션이 스마트폰을 통해 사용되고 있다. 그 중 스마트폰을 이용하여 결제를 수행하는 어플리케이션의 경우 그 편의성 때문에 많은 사용자가 이용하고 있다[1]. 다만 스마트폰을 이용한 인증, 결제 등의 서비스를 이용할 때에 사용자들이 입력하고 사용하는 개인 정보에 대한 보안성 검증이 필요하다. 만약 스마트폰의 어플리케이션에서 사용자의 개인정보가 충분히 신뢰할 수 있는 보안 모델에서 사용되지 않는다면 사용자들은 이러한 서비스를 수행하는 어플리케이션을 이용할 때 불안감을 느

접수일(2015년 1월 13일), 수정일(2015년 4월 8일), 게재확정일(2015년 5월 11일)
* 이 논문은 인하대학교의 지원에 의하여 연구되었음.
† 주저자, zhoujun5458@hotmail.com
‡ 교신저자,khlee@suwon.ac.kr(Corresponding author)

끼거나 어플리케이션을 사용하기 꺼려할 것이다.

이 연구에서는 스마트워치를 이용하여 스마트폰에서의 안전한 이체가 수행되는 다양한 기법에 관한 실험을 수행하였다. OTP와 캡차(CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart)[2]를 이용한 거래연동 OTP 기법, 스마트워치를 이용한 콘텐츠 기반의 인증 기법 등에 대한 프로토타입 제작을 하고 사용자 실험을 실시하였다.

이 논문의 공헌도는 다음과 같다. 이 연구에서는 스마트폰과 스마트워치를 동시에 이용하여 사용자의 거래내용을 확인하고 인증하는 방법을 실험하였다. 스마트폰이 악성코드에 감염되거나, 분실되었을 때에도 사용자의 정보가 유출되거나 공격자가 사용자의 정보를 악용하여 거래를 수행하지 못하도록 하는 것이 목표이기 때문에 스마트폰의 보안을 강화하는 장비로 스마트워치를 활용하였으며, 이를 위해 약간의 사용성을 희생하였으나 사용자 실험을 수행한 결과 큰 손실은 없는 것으로 보인다. 기존의 거래연동 OTP[3,4]와 콘텐츠 기반 캡차[5] 등에 대한 다양한 연구를 스마트폰과 스마트워치라는 분리된 장비에서의 전자거래에서 활용할 수 있는 방안을 제시하고, 프로토타입을 제작하여 사용자 실험을 수행하였다. 또한 사용자가 거래내역에 대한 서명을 수행할 때 사용하는 키를 스마트폰에 저장하는 것이 아니라 스마트워치에 저장하고 필요시 서명하는 방법으로 사용자의 비밀을 분산시켜 두 장비가 동시에 있을 때에만 전자거래 등의 동작을 수행할 수 있도록 할 수 있다.

이 논문의 2장에서는 스마트워치가 필요한 연구배경에 대해 알아본다. 3장에서는 이체 서비스를 이용할 때에 스마트워치를 이용한 아이디어를 보이고 보안성 분석을 수행한다. 4장에서는 다양한 기법들에 대한 실용성을 분석한다. 5장에서는 이 논문에서 제안하는 스마트워치를 활용한 방법의 가치를 이야기하고 성능을 향상하기 위한 앞으로의 연구 계획에 대하여 언급하며 결론을 맺는다.

II. 배경 연구

2.1 스마트폰의 안전성

최근 스마트폰 이용자가 증가함에 따라, 모바일 인터넷을 언제 어디서나 사용할 수 있다. 또한 스마트폰에서의 보안 문제는 스마트폰 자체의 안전을 위협할 뿐만 아니라, 스마트폰이 연결되어 있는 모바일 네트워크와 인터넷의 운영을 위태롭게 한다. 인터넷의 전통적인 보안 위협들인 악성 프로그램, 원격 제어, 인터넷 공격 등은 모바일 네트워크로 빠르게 퍼지고 있으며, 모바일 네트워크의 비즈니스와 사용자 이익은 밀접한 관련이 있기 때문에 악의적인 결제, 개인정보 도용, 사기 등 악의적인 행위의 영향과 피해가 나타나고 있다. 위에서 말한 스마트폰의 보안 문제들은 다음과 같이 정리할 수 있다[6,7,8].

1. 분명하지 않은 출처나 공격자가 작성한 출처에서 사용자가 응용 소프트웨어를 다운로드 및 실행하는 경우, 사용자는 응용 소프트웨어에 어떤 조작이 되어 있는지, 응용 소프트웨어의 신뢰 여부를 확실하게 알 수 없다.
2. 스마트폰에는 3G/4G, 무선랜과 같은 여러 가지 방식의 무선 통신이 존재한다. 이러한 무선 통신은 잠재적인 위협이 존재하는데, 예를 들면 공공장소의 무선랜은 인증 없이 연결이 될 수 있는데, 사용자가 주의 깊게 확인하지 않으면 공격자가 스마트폰을 공격할 수 있다.

스마트폰 악성코드는 PC에서와 마찬가지로 스마트폰에 악영향을 끼칠 수 있는 모든 소프트웨어의 총칭이다. 악성코드는 기기의 취약점, 무선 침투, 이동저장장치, 사회 공학적 기법 등 다양한 경로로 침입해 스마트폰을 위협하며, 스마트폰 운영체제 및 웹 브라우저의 취약점을 공격한다. 블루투스, 무선랜, 이동통신망 등 네트워크에 존재하는 취약점을 통해 특수하게 조작된 패킷으로 전송된다. 무선랜, 이동통신망을 통한 인터넷 접속뿐만 아니라 USB, 블루투스를 통한 통신 기능을 이용한다. 감염된 메모리카드·PC와 스마트폰을 직접 연결하는 경우에도 악성코드가 침입할 수 있다.

이 밖에도 악성코드는 유용한 소프트웨어로 위장해 온라인 마켓, 이메일 및 문자 메시지의 첨부 파일 형태로도 침입한다. 악성코드에 감염된 스마트폰은 이용자가 모르는 사이에 개인정보유출, 과금 유발, 단말기 이용 제한 등의 악성행위를 수행한다. 일단 해커가 악성코드를 스마트폰에 침입시키면 이를 통해 스마트폰 내 통화내역·수신메시지·전화번호부·일정·메모·위치정보 등 개인 신상 정보를 비롯해 뱅킹·소액결제 등의 금융결제정보와 업무용 파일 등 기밀정보가 유출될 수 있다.

Table. 1. Comparison of H/W performance of major smartwatches

Smartwatch name	Galaxy Gear	Pebble E-Paper Watch	SmartWatch 2	Qualcomm Toq	I'm Watch	Neptune Pine
Manufacture	Samsung	Pebble Technology	Sony	Qualcomm	I'm	Neptune
OS	Android 4.2.2	Pebble OS	Micrium uC/OS-II	Qualcomm OS	I'm Droid 2	Android 4.1
CPU	800 MHz Exynos	ARM Cortex-M3	180MHz ARM Cortex-M4	200MHz ARM Cortex-M3	IMX233	1.2GHz Dual-Core ARM Cortex-A5
RAM	512 MB	512 KB	64 MB	512 MB	128 MB	512 MB
Storage	4 GB	32 MB	256 MB	2 GB	4 GB	16 ~ 32 GB
Camera	1.9 MP	-	-	-	-	5 MP
Communication	Bluetooth 4.0	Bluetooth 2.1+EDR	Bluetooth 3.0 / NFC	Bluetooth 4.0 LE	Bluetooth	Bluetooth 4.0 / Wi-Fi / GSM
Battery	315 mAh	140 mAh	140 mAh	5 days	450 mAh	810 mAh
Display	1.63″ 320x320	1.26″ 144x168	1.6″ 220x176	1.55″	1.54″ 240x240	2.4″ 320x240
Weight	74g	-	123g	-	90~170g	35.4~60.8g
Type	Extension	Stand-alone	Extension	Extension	Stand-alone	Stand-alone

또 SMS·MMS 등 스팸문자 발송을 비롯해 휴대전화 소액결제, 무선인터넷 이용, 유료 전화서비스, 국제전화 발신 등의 과금을 유발한다. 이뿐 아니라 단말기 UI 변경, 단말기 파손(오류 발생), 배터리 소모, 파일, 일정, 전화번호부 등의 수많은 정보와 프로그램을 삭제하는 피해도 남긴다. 따라서 스마트폰 악성코드 감염은 심각한 사회적 위협이 될 수 있다.

최근 스마트폰에 밀려 휴대용 게임기와 노트북 시장이 축소되는 것으로부터 알 수 있듯이, 스마트폰은 이제 개인용 컴퓨터를 대체하고 있는 기기이다. 아무리 노트북이 가볍다고 하더라도 항상 들고 다니기에는 무리가 있는 반면, 스마트폰은 휴대에 편리한 크기와 무게를 가지고 있고, 연산 능력 또한 빠르게 발전하고 있기 때문에 앞으로도 이러한 현상은 더욱 가속화될 것으로 보인다. 스마트폰은 이제 더 이상 개인용 컴퓨터를 보조하는 수단이 아니라 사용자들이 휴대하고 다니는 컴퓨터의 역할을 수행하고 있다.

2.2 스마트폰을 이용한 전자거래

스마트폰에는 사용자의 편의를 돕기 위한 다양한 어플리케이션과 기능들이 존재한다. 사용자는 PC에서 수행해온 전자거래를 스마트폰을 통해서도 진행할 수 있다. 스마트폰의 전자거래에서 보안 요구사항을 만족하기 위해서 사용자를 확인하기 위한 OTP, 공인인증서 등을 활용할 수 있고, 어플리케이션의 무결성 및 위·변조 방지를 위한 스마트폰용 보안 프로그램 등을 이용하여 사용자의 개인정보를 보호하고 안전한 거래를 수행할 수 있게 할 수 있다[9].

최근 스마트폰을 대상으로 한 악성코드 등이 개발되어 전자거래를 수행하는 사용자의 정보를 유출하거나, 사용자에게 보이는 화면을 속여 전자거래를 수행하는 공격이 이루어지고 있기 때문에 전자거래의 내역에 대한 사용자의 인증이 필요하게 되었다. 사용자가 거래내역에 대한 인증을 하는 방법으로는 거래연동 OTP 등의 부가적인 장비를 이용하는 방법이 있다[4].

이 연구에서는 스마트폰과 분리된 스마트워치에서 기존의 거래내역 인증방법을 적용하여 사용자가 확인할 수 있도록 하였다. 사용자가 스마트워치를 이용하여 전자거래에 대한 정보를 확인하거나, 전자서명에 필요한 키를 사용자의 스마트폰이 아닌 스마트워치에

저장하여 거래내역에 대한 서명을 스마트워치에서 수행할 수 있도록 하여 사용자의 비밀을 분산시킬 수 있었다. 또한 전자거래에 사용되는 OTP를 입력하는 경우에도 사용자에게 스마트워치를 이용하여 입력하도록 하여 사용자의 정보가 유출되는 것을 막을 수 있다.

2.3 스마트워치를 이용한 가능성

기술의 발전함에 따라, 스마트폰과 연동하여 동작하는 많은 전자 제품들이 개발되고 있다. 스마트워치는 바로 그 중에 하나이다[10, 11]. Table. 1은 다양한 스마트워치에 대한 하드웨어 정보를 비교하여 보여주고 있다. 스마트워치는 독립 구동형 스마트워치(Stand-alone)와 스마트폰 확장형 스마트워치(Extension)로 나눌 수 있다. 독립 구동형 스마트워치는 스마트워치의 앱이 스마트폰의 앱과 독립적으로 구동되는 스마트워치를 의미한다. 또한 독립형 스마트워치는 스마트폰과 독립적인 OS를 가지고 있다. 따라서 스마트폰의 앱이 스마트워치의 앱과 통신하기 위해서는 블루투스나 IEEE 802.11과 같이 일반적으로 사용하는 무선 통신 프로토콜을 이용하여야 한다. 이는 서로 다른 스마트폰 앱이 하나의 스마트워치 앱과 통신할 수 있음을 의미한다. 이러한 스마트워치는 스마트폰과 완전 독립적인 시스템이므로, 스마트폰이 악성코드에 감염 되었다고 해도 안전하게 동작한다. 반대로 스마트워치가 감염되었다고 해도 스마트폰은 안전할 수 있다.

스마트폰 확장형 스마트워치는 스마트폰과 독립적인 OS를 가지고 있지만 사용자가 독립적으로 앱을 설치할 수 있는 기능이 없다. 스마트워치에 구동되는 앱을 설치하기 위해서는 반드시 스마트폰에 앱을 설치해야 한다. 스마트워치의 앱은 독립적으로 실행되지 않으며, 스마트폰에 설치된 앱이 스마트폰으로 데이터나 명령 등 전송될 때에만 그에 대해 수동적으로 응답을 줄 뿐이다. 이러한 특징은 개발자에게 스마트워치용 앱의 개발을 쉽게 만들어 준다. 그러나 이러한 확장형 스마트워치의 경우 사실상 스마트폰에 설치된 앱에서 스마트워치를 제어하는 구조이기 때문에 스마트폰이 악성 프로그램에 감염되었을 경우, 스마트워치의 안전성에도 문제가 발생할 수 있다. 설령 스마트워치에 TPM과 같이 안전하게 키를 보관할 수 있는 영역이 있다고 하더라도 스마트워치의 제어는 여전히 스마트폰에 설치된 앱이 수행하기 때문에 안전하다고 보기 힘들다. 따라서 보안성을 확보하기 위해서 스마트워치를 사용 할 경우, 이러한 구조를 가진 스마트워치는 배제하는 것이 좋다고 볼 수 있다.

스마트워치에서는 데이터 처리와 기억 장치, 그리고 입출력 기능 등을 수행하고 내·외부의 센서로 정보를 수집한다. 이후 스마트폰을 통해서 데이터를 활용할 수 있다. 또한 스마트워치는 블루투스, 와이파이와 같은 무선 통신을 지원한다. 이러한 스마트워치는 "손목 컴퓨터"로, 다른 원격 시스템의 입출력 인터페이스의 역할을 하는 것도 가능하다.

이후 스마트폰을 보조할 수 있는 기기가 필요하게 되면 그러한 기기는 스마트워치가 될 것임에는 이론의 여지가 없을 것이다.

III. 스마트워치를 이용한 보안 방법

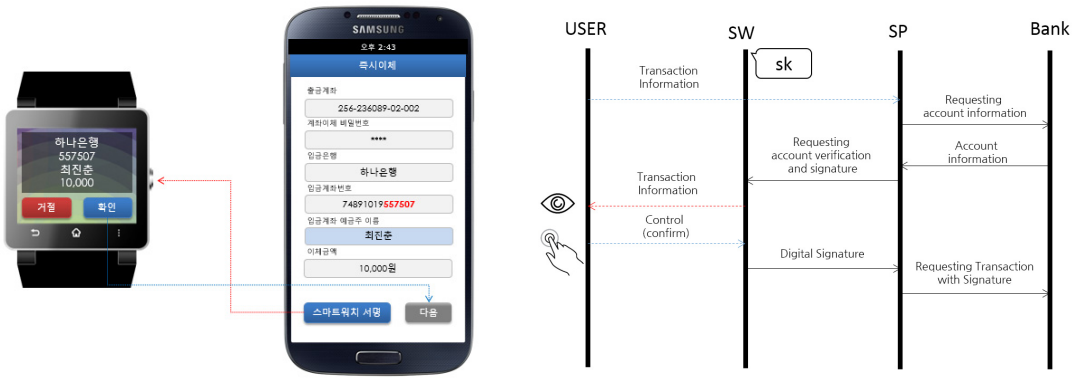
3.1 스마트워치를 이용한 거래 내역 확인

스마트워치를 이용한 거래 내역을 확인하는 방법 다음과 같이 구성되어 있다. 먼저 스마트폰에 입력한 거래 이체 정보가 스마트워치에 정상적으로 출력되는지 확인하고, 확인 버튼을 누르는 것으로 거래 내역 확인과정이 완료된다.

Fig. 1(a)는 스마트워치를 이용한 이체 화면을 나타낸 그림으로 스마트폰에서 이체를 할 때 스마트워치의 서명 버튼을 누르면 스마트워치에서 거래 내역을 확인할 수 있다. 거래 내역은 입금은행, 입금계좌번호의 마지막 여섯 개 숫자, 예금주 이름, 이체금액으로 구성된다. 스마트워치와 스마트폰의 거래 내역이 일치하면 스마트워치에서 확인버튼을 누르고 스마트폰에서 다음 버튼을 누른다. 만약 거래 내역이 다르게 표시되면 사용자는 스마트폰이나 스마트워치가 공격자에 의해 조작되었을 수 있음을 인지하고 거래를 중단하여야 한다.

3.1.1 보안성 분석

Fig.1(b)는 스마트워치 거래 내역 확인 방법의 통신 과정을 나타낸다. 기술적으로 스마트워치는 은행이 알고 있는 자신의 공개키에 해당하는 비밀키를 알고 있어야 하고 이를 이용하여 디지털 서명을 수행해야 한다. 만약 확인만 하고 스마트폰에서 서명하게 한다면, 스마트폰의 악성코드가 스마트워치에 보인 것과 다른 내용에 대해서 서명하고 은행에 전송할 가



(a) example (b) procedure

Fig. 1. Verification procedure and protocol for information of transaction via smartwatch

(a) example (b) procedure

Fig. 2. Verification procedure and protocol for information of transaction based on CAPTCHA via smartwatch

능성이 있다.

이 방법은 사용자에게 있어서 편리하지만, 스마트워치가 악성 코드에 의해 감염되었을 경우에는 무력화될 수 있다. 물론, 스마트워치가 특정한 스마트폰과 통신을 수행할 때에만 이체를 수행하도록 하면 스마트워치가 악성 코드에 의해 감염되었다 하더라도 어느 정도 안전성을 유지할 수 있지만 이는 이 기법의 범위를 벗어나는 보안 방법이다. 따라서 디지털 서명만 단독으로 수행하기 위해서는 위험한 측면이 있어, 서명을 나누어서 수행하거나, 다른 비밀을 추가로 적용해서 사용해야할 필요성이 있다.

3.2 스마트워치를 이용한 콘텐츠 기반 캡차를 이용한 거래 내역 확인

3.1절에서의 방법처럼 텍스트 상태의 거래 내역을 확인하는 경우, 스마트워치가 악성 코드에 감염되는 경우 거래 자체가 위험할 수 있으며, 이를 해결하기 위해 캡차를 이용하여 사용자에게 거래 내역을 확인하도록 하는 방법을 사용할 수 있다. 이를 위해 스마트워치를 이용하여 거래 내역을 확인하는 방법 중 하나로 이상호 등이 제안한 콘텐츠 기반 캡차를 이용하여 거래 내역을 확인하는 방법[5]을 스마트워치에 적용하였다.

Fig. 2(a)는 예금주의 이름을 확인하는 캡차 기반의 거래 내역 확인 방법과 그 과정에 대해서 보여준다. 스마트폰을 이용한 즉시이체에서 예금주 확인

버튼을 누르면 스마트워치에서는 선택할 수 있는 이름들이 표시된다. 사용자는 예금주 이름과 같은 이름을 선택하고 확인한다. 이러한 방법은 이후 사용자 실험에서 볼 수 있듯이 사용할 때 편리함을 알 수 있다.

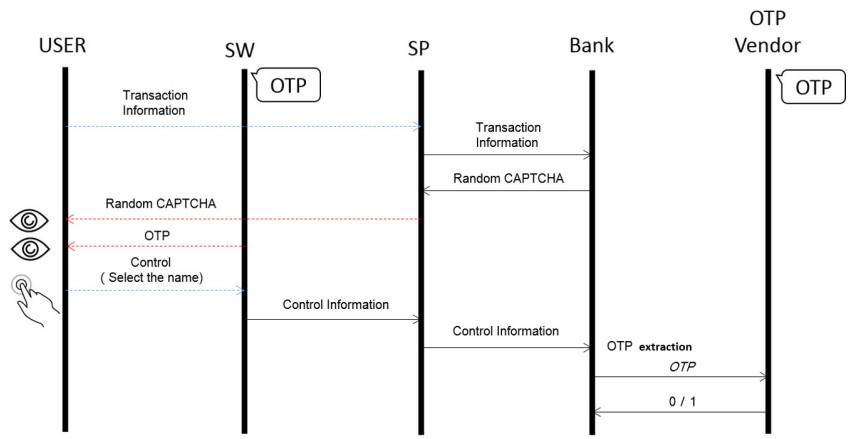
3.2.1 보안성 분석

Fig.2(b)는 콘텐츠 기반의 캡차를 이용한 거래내역 확인 방법의 통신 과정을 나타낸다. 이 과정에서 서명은 스마트폰에서 수행되는 것으로 표현되었지만 서명은 스마트폰의 위험성을 고려할 때 스마트워치에서 수행되는 것이 더 바람직하다. 만약 스마트폰에서 서명을 수행한다면 공인인증서의 비밀키를 저장해 둔 파일의 비밀키를 입력하는 단계가 추가적으로 요구되며, 이는 사용성을 더 낮출 수 있다. 또한 이 방법은 예금주의 이름만을 확인하는 것으로, 이체하려는 계좌의 예금주와 공격자의 이름이 같을 경우 약점이 될 수 있다. 이러한 문제를 해결하기 위해 계좌번호의 일부나 이체금액을 모두 캡차의 형태로서 확인 하도록 해야 할 필요가 있다. 그러나 편리성과 보안성의 상호 교환(trade-off) 관계는 흔히 이러한 연구에 있어서 중요하게 고려되어야할 부분이므로 이 제안에서는 예금주의 이름만 확인하는 것으로 한다.

3.3 스마트워치를 이용하여 캡차 기반의 OTP를 안전하게 입력하는 방법

맹영재 등은 모바일 뱅킹을 위해 OTP를 안전하게 입력하는 방법으로 비밀 퍼즐을 만들어 이체 확인을 하는 방법들에 대해서 제안하였다[12]. 이 논문

(a) example



(b) procedure

Fig.3. Transmission procedure and protocol of CAPTCHA based transaction scheme using smartwatch

에서는 제안한 방법을 기반으로 스마트폰과 스마트워치에서 동작하는 기법을 구현하였다. 이 기법에서는 사용자가 이체정보를 확인하기 위해서 예금주의 이름을 캡차로 만들어 스마트폰에서 보여준다. 여러 가능한 이름을 무작위로 보여주고, OTP번호에 해당하는 번호를 이체 계좌의 예금주 이름(또는 글자)과 매칭시켜야 한다. 은행 측은 예금주의 이름에 해당하는 캡차가 어디 있는지 알고 있으므로, 이로부터 OTP를 추출하여 비교할 수 있다. 사용자가 입력한 OTP가 옳다면, 사용자는 캡차를 제대로 읽었으며, OTP 생성기를 가지고 있음을 의미한다. 만약 입력된 OTP가 틀리다면, OTP 생성기가 없거나, 사용자가 캡차를 정상적으로 읽지 못하였거나, 자신의 원하는 이름이 없는 것 중에 하나이므로 이체를 수행하면 안 된다.

스마트워치는 OTP 생성기를 대체할 수 있을 것으로 생각된다. 이는 현재 스마트폰이 일부 OTP 생성기를 대체하고 있는 것과 비슷하다. Fig. 3(a)는 스마트폰과 스마트워치의 프로그램의 화면을 보여준다. 왼쪽 그림에서 입금계좌 예금주 이름은 “최진춘”으로 지정하였다. 이후에 스마트워치 표면에서 손가락으로 상하 좌우 정보를 입력하여 지정한 이름을 찾아 OTP 번호를 입력하게 된다. 오른쪽의 그림에서 이체 화면을 보여주며, 스마트워치의 OTP는 “233219”를 지정하였다. 각 숫자는 한 줄의 이름이 대응한다. 이제 스마트폰에서 맞는 이름을 찾는다. 우선 “최”를 찾는다. 스마트폰의 첫 번째 줄에서 일치하는 이름이 없기 때문에 “2”를 빈 칸으로 매칭한다. 두 번째와 세 번째 줄에서도 이름이 없어서 각자의 숫자가 빈 칸으로 매칭한다. 네 번째 줄에서 “최”를 찾아서 “2”로 매칭할 수 있으며, 다섯 번째 줄에서 “진”을 “1”로 매칭한다. 마지막으로 여섯 번째 줄에서 “춘”을 “9”로 매칭한 뒤 다음 버튼을 누름으로써 OTP 입력을 완료한다.

Fig. 3(b)는 캡차 기반 거래 연동 OTP를 이용한 과정을 나타낸다. 사용자는 계좌 이체 정보(transaction information)를 입력 한 후 은행으로부터 받은 랜덤 캡차(random CAPTCHA)를 스마트폰으로 확인하고 스마트워치에 뜬 OTP 번호를 보면서 스마트워치를 조작해 스마트폰에 OTP를 입력한다. 스마트폰에는 OTP 번호의 길이와 동일하게 총 6줄의 캡차 밑에 0부터 9까지의 번호가 배열되어 있으며, 사용자는 이체 대상의 이름을 한 글자씩 OTP 번호와 매치하도록 번호를 배열한다. 이름은 6줄에 걸쳐서 차례대로 배치되어 있으며, 이름에 해당하는 글자가 없다면 빈칸을 선택한다. 스마트폰은 조작 정보(control information)를 은행에 전송하고, 은행은 OTP 벤더에 자신이 추출한 OTP 번호를 확인받는다.

3.3.1 보안성 분석

이러한 방식은 사실 OTP의 보안성을 약화시킨다. 왜냐하면 총 6개줄 중 이름의 길이를 뺀 줄에서 빈칸을 선택하기 때문이다. 6개중 3개를 선택할 때, 이게 맞을 확률은 1/20이므로 나머지 3자리에 의한 1/1000만 맞추면 된다. 즉, 원래는 1/1000000이었던 OTP 번호의 보안성이 1/20000로 줄어들게 된다. 이는 최종 응답을 보고 OTP 값이 무엇인지 알고자하는 공격자에 대한 확률이다. OTP를 입력하려고하는 공격자에게는 여전히 1/1000000확률의 어려움을 갖는다.

또한 이 방법은 스마트폰 화면에 출력된 캡차를 풀어야 하는데, 캡차의 난이도가 올라갈수록 안전해지만 그에 비례하여 사용성은 하락하게 되다. 이름이 한꺼번에 출력되는 것이 아니고, 글자가 하나하나 출력되기 때문에 각각을 찾는 것도 사용성을 불편하게 하는 중요한 요소 중에 하나이다.

이 방법은 스마트폰이 악성 코드에 의해 감염되었을 때뿐만 아니라 스마트워치가 감염되었을 때에도 안전성을 갖는다. 둘 모두가 악성 코드로 감염되었을 때에는 캡차의 난이도만큼의 보안성을 갖는다.

IV. 스마트워치를 이용한 이체의 실용성 분석

이 논문에서 제안하는 실험을 위해 스마트워치로는 Sony smartwatch 2(1.0.B.5.28/1.0.A.4.11)를 사용하였으며, 이는 스마트폰 확장형으로 동작한다. 앞서 이야기한 바와 같이 보안성을 확보하기 위해서는 스마트폰 확장형 스마트워치의 사용을 배제하는 것이 좋으나, 이 논문에서는 사용자 실험과 개발의 용이성 등의 이유로 스마트폰 확장형 스마트워치를 사용하였다. 스마트폰으로는 Google사의 레퍼런스 모델인 Galaxy Nexus(Android 4.0.2)를 사용하였다. 또한 실험에 사용한 어플리케이션 개발을 위해 Eclipse Sony Add-on SDK v 2.6을 사용하였다.

또한 사용자 10명을 대상으로 각각 실험마다 5회

씩 반복하여 실험을 수행하였다.

4.1 스마트워치를 이용한 거래 내역 확인과 캡차 기반 거래 내역 확인의 사용자 실험

이 절에서는 3.1 및 3.2절에서 제시한 방법에 대한 사용자 실험의 결과를 보인다. 3.1절의 사용자 실험 중에 50번의 데이터를 받았고, 상세한 데이터 분포는 Fig. 4에서 확인할 수 있다. 총 38번의 데이터는 3초~7초 사이에 1회의 작업을 완료함으로 전체의 76%를 차지하고, 실험 수행에 평균 소요시간이 6276.6(ms)임을 보였다. 또한 이 실험에서는 사용자가 공격을 당해 스마트워치 화면에 이체금액이 바뀔 수 있다는 가정을 하여 사용자가 대응할 수 있는지 실험하였다. 총 50번 실험 중에 27번의 경우 이러한 공격이 있다고 가정하여 실험하였을 때, 전체 27번의 실험 중에 3번의 경우만 이체 과정을 계속했

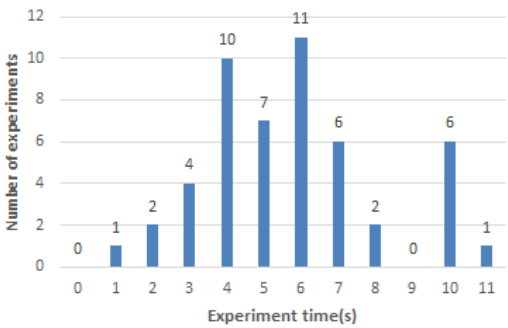


Fig. 4. Number of complete verifications in a second(based on smartwatch)

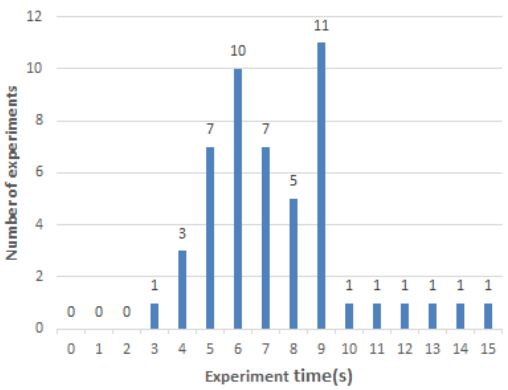


Fig. 5. Number of complete verifications in a second(using contents based CAPTCHA in smartwatch)

고, 나머지 24번 경우는 이체 과정을 취소했다. 즉, 이 실험을 통해 직관적인 공격에 대해 대부분의 사용자는 효과적인 조치를 취할 수 있음을 알 수 있다.

3.2절의 사용자 실험 중에 50번의 데이터를 받았고 그에 관한 상세한 데이터분포를 Fig. 5에서 확인할 수 있다. 이 실험에서 총 40번의 경우 5초~9초 사이에 1회의 작업을 끝냈으며, 전체의 80%를 차지하고 평균 소요시간이 8784.6 (ms)임을 보였다.

위 두 방법은 간편하고 빠르게 조작을 할 수 있는 장점이 있다. 향후 다른 방법과 혼합하여 사용한다면 이체거래에서 안전성을 더욱 높일 수 있을 것으로 생각된다.

4.2 스마트워치의 OTP를 안전하게 스마트폰에 입력하는 방법의 사용자 실험

3.3절에 제시한 방법에 대한 실험데이터는 Fig. 6과 같다. 이번 실험에서는 50번의 실험 데이터가 나왔으며, 사용자가 1회의 실험을 수행하는데 필요한 시간을 Fig. 6에서 확인할 수 있다. 20초~30초 사이에 2번의 데이터가 있으며, 30초~40초 사이에서는 21번, 40초~50초 사이에서는 19번, 50초~60초 사이에 8번의 데이터가 있음을 알 수 있다. 대부분의 작업은 30초~50초 사이에 완료되며, 이 구간에는 총 40번의 데이터가 존재한다. 또한 사용자가 실험에 적응할수록 실험시간이 상대적으로 줄어드는 것을 알 수 있었다. 전체 50번의 실험 중에 8번은 정상적인 실험의 수행에 실패했고('다음' 버튼을 누르고 '이체실패' 메시지가 뜰 때), 정확도는 84%이었다. 또한 이 방법은 스마트폰 화면에 출력된 캡차를 풀어야 하는데, 캡차의 난이도에 따라 수

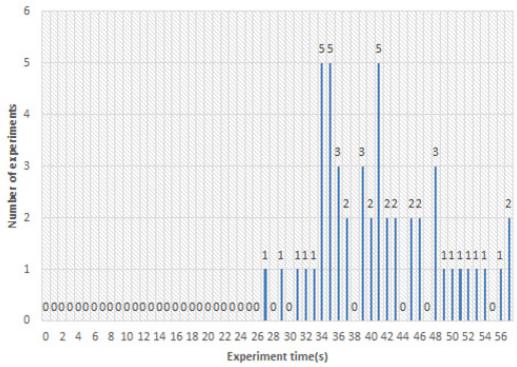


Fig. 6. Experiment results of CAPTCHA based transaction OTP scheme using smartwatch

행 시간과 정확도는 증가하거나 줄어들 수 있다[5].

Fig. 7과 Fig. 8을 같이 보면 첫 줄을 수행하는데 소요시간이 제일 길었는데, 이는 대부분의 사용자가 실험 화면에 들어갈 때 전체적으로 캡차와 대응된 이름을 확인하고 나서 실험을 시작하는 경향이 있기 때문이다. 마지막 줄은 소요시간이 제일 짧게 나왔는데, 이는 마지막 줄이 이름의 마지막 글자이거나 빈 칸이기 때문에 소요시간이 제일 적음을 알 수 있었다. Fig. 8의 추세 그래프를 통해 각 줄마다의 소요시간이 줄어든 것을 확인 할 수 있다. 사용자가 익숙해질수록 각 줄의 작업 시간이 감소하게 된다.

스마트워치의 OTP 사용은 기존의 OTP 입력방법에 비해 소요시간이 상대적으로 길다. 하지만 이후에 스마트폰과 스마트워치의 발전과 입력 방법이 보완된다면 이 논문에서 제시한 방법은 충분히 실행할 만하다고 볼 수 있다. 또한 대부분 사용자는 이 방법이 흥미롭고 긍정적이라는 의견을 표현했다.

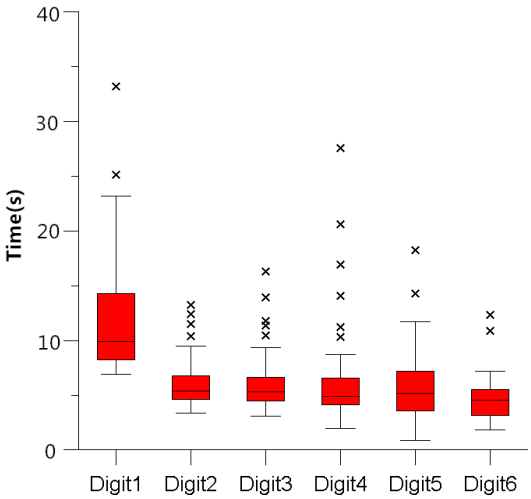


Fig. 7. Box plot of input time spending on each digit of OTP using CAPTCHA with smartwatch

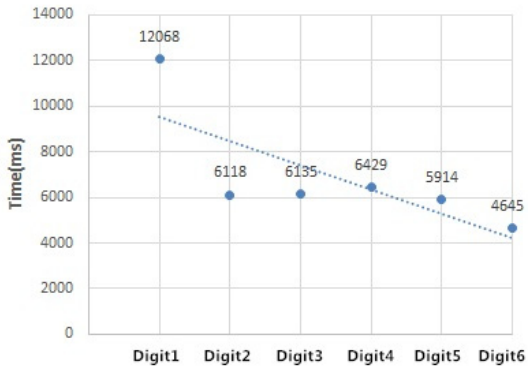


Fig. 8. Trend line of input time spending on each digit of OTP using CAPTCHA with smartwatch

4.3 스마트워치와 스마트폰의 통신시간

이 논문에서는 스마트폰에 스마트워치를 블루투스로 연결하여 실험했다. 각각의 실험에서 스마트폰에 스마트워치를 연결하는데 소요시간을 기록하였다. 3.1절의 제안에서 50번의 평균 연결시간이 842.9(ms)이고, 3.2절의 제안에서 50번의 평균 연결시간이 661.9(ms)로 나타났으며, 3.3절의 제안에서 50번의 경우 평균 연결시간이 1283.2(ms)이었다. 스마트폰에 스마트워치를 연결하는데 소요시간은 스마트폰, 및 스마트워치의 CPU, RAM, 그리고 소프트웨어 최적화 등에 영향을 받는다.

4.4 실험 결과에 대한 분석

이 절에서는 이 논문에서 수행한 실험들의 결과를 CDF를 통해 보이고, 그에 대한 분석을 수행한다. Fig. 9는 앞서 실험한 세 가지 기법들에 대해 사용자의 입력이 완료되는 시간을 CDF로 표현하였다. 이 그래프에서 볼 수 있듯 스마트워치에 표시된 거래내역을 확인하고, 확인/거절을 선택하는 기법과 스마트워치에 콘텐츠 캡차 기반의 기법의 경우 대부분의 사용자가 10초 이내에 빠르게 동작을 완료하는 것을 확인할 수 있으며, 스마트워치를 이용한 캡차 기반의 OTP 방식은 사용자의 절반 이상이 40초 이상의 시간을 사용하는 것을 알 수 있다. 다만 사용자의 거래내역을 확인하는 기법에서는 하나의 기기가 감염되는

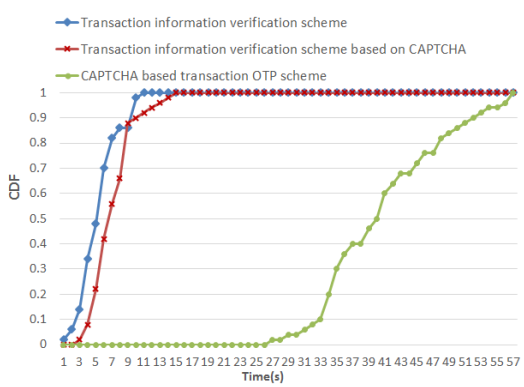


Fig. 9. CDF in three transaction scheme

Table. 2. Comparison of transaction information verification schemes

		Transaction information verification scheme	Transaction information verification scheme based on CAPTCHA	CAPTCHA based transaction OTP scheme
Secret		Signing Key	Signing Key	OTP
Additional Secret		-	CAPTCHA	CAPTCHA
Device to sign		smartwatch	smartwatch or smartphone	-
Security (when compromised)	smartphone	depend on the security of the digital signature	depend on number and difficulty of CAPTCHAs	1/20000
	smartwatch	secure iff smartphone check signature		depend on difficulty of CAPTCHA
	both	not secure		
Usability		good	reasonable	bad
ETC		-	-	communication with vendor is required

경우 그 보안성이 떨어지는 정도가 스마트워치를 이용한 캡차 기반의 OTP 방식과 차이가 있다. Table. 2에서는 이 논문에서 구현하여 실험한 세 가지 기법들에 대해 정리하였다. 이 표에서 알 수 있듯이 비밀을 어떤 기기가 가지고 있는지에 따라 스마트워치나 스마트폰이 악성코드로 감염되었을 때의 안전성이 달라진다. 즉, 하나의 기기가 비밀을 가지고 있는 경우, 그 기기가 감염되면 거래 자체가 불안전해질 수 있으며, 기기를 사용하는 것이 사람이기 때문에 사용자가 기기를 분실할 가능성도 존재한다. 이러한 경우 거래를 안전하게 하기 위해서는 기기의 언락을 위한 PIN입력이나 스마트폰에 저장된 공개키 인증서의 비밀키를 암호화하는 패스워드를 사용자로부터 입력받는 방법이 있다. 사용자의 편의를 위해서는 이러한 기법보다는 스마트워치에 존재하는 다양한 센서들을 이용하여 인증된 사용자를 대상으로만 전자거래를 수행하게 하는 등의 방법으로 전자거래를 안전하게 할 수 있는 연구가 필요할 것이다.

V. 결 론

이 논문에서는 스마트워치를 이용해 스마트폰을 안전하게 사용하는 방법을 실험하였다. 스마트워치를 이용한 거래 안전을 확보하기 위한 방법으로 스마트워치를 이용하여 거래 내역을 확인하고 서명하는 기법, 악성 코드를 막기 위해 캡차 기반의 거래 내역 확인 기법, 스마트폰을 위한 캡차 기반 거래 연동 OTP 입력 기법을 스마트워치에 적용하여 실험하였다.

각각의 기법들을 사용자들을 대상으로 하여 실험한 결과는 다음과 같다. 스마트워치를 이용한 거래내역 확인 기법에서는 사용자가 스마트워치를 보고 자신이 입력한 거래내용이 맞는지 확인한 후 거래를 계속 진행시켰다. 이 실험에서는 임의로 공격자가 존재하여 사용자의 이체 금액을 바꾸는 경우를 가정하였는데, 대부분의 사용자가 이러한 공격에 대해 효과적인 조치를 취하는 모습을 확인할 수 있었다.

캡차 기반의 거래내역 확인 기법의 경우 캡차를 사용하지 않은 기법과 비슷한 수행시간을 보임을 알 수 있었다. 이는 사용자가 알고 있는 지식을 이용한 콘텐츠 기반의 캡차를 사용하기 때문에 캡차의 난이도에 비해 사용자가 빠르게 해당 동작을 수행하는 것으로 보인다.

캡차 기반의 거래 연동 OTP 입력 기법은 사용자가 스마트워치를 이용하여 거래 정보와 관련된 캡차를 확인하고 OTP를 입력하는 데 걸리는 시간을 측정하였는데, 이를 통해 사용자들이 OTP를 입력 할 때의 경향성을 알 수 있었다.

또한 인터넷 뱅킹에서 OTP와 전자 서명을 함께 사용하여 높은 보안성을 유지하듯, 스마트워치와 스마트폰에서도 OTP와 전자 서명 기법을 사용하게 할 수 있다. 캡차 기반 거래 연동 OTP와 캡차 기반의 거래 내역 확인기법을 혼합하여 사용하는 방법으로 스마트워치나 스마트폰이 공격자에 의해 감염 되었을 때에도 안전성을 보장할 수 있을 것이다.

이후 연구에서는 이 논문에서 수행한 실험들을 바탕으로 하여 스마트워치를 활용한 스마트폰에서의 안

전한 거래방법을 제안할 때 안전성뿐만 아니라 사용자들이 실제 사용하면서 느끼는 사용성적인 측면도 충분히 반영하여야 할 것이다. 특히 캡차를 활용한 방법을 사용하는 경우, [5]의 연구에서와 같이 사용자가 불편함을 느끼지 않는 시간동안 해결할 수 있는 적절한 캡차의 난이도 설정 방법에 대한 고찰이 필요할 것이다.

References

[1] Korea Naeil Shinmoon, "IT industry catches the quick payment market! 'Contention of a Hundred Schools of Thought'." Aug. 2014.

[2] Von Ahn, L., Blum, M., Hopper, N. J., & Langford, J., "CAPTCHA: Using hard AI problems for security." In Advances in Cryptology/EUROCRYPT , pp. 294-311, 2003.

[3] YoungJae Maeng and DaeHun Nyang, "OTP with Transaction uses of complementary color," Magazine of The Korea Institute of information Security&Cryptology, 21(7), pp. 38-52, Nov. 2011.

[4] Financial Security Institute, "Considerations of Electronic financial environment about transaction signature authentication technology trends and implementation," vol. 2, Apr. 2014.

[5] Sang-ho Lee, Sung-ho Kim, Jeon-il Kang, Je-sung Byun, Dae-hun Nyang and Kyung-hee Lee, "A Method of Enhancing Security of internet Banking Service using Contents Based CAPTCHA," Journal of The Korea Institute of information Security&Cryptology, 23 (4), pp. 571-583, Aug. 2013.

[6] Korea CCTV News, "First quarter of 2014, Smartphone malicious codes have a total of 435122…2-fold increase year on year." Apr. 2014.

[7] Seung-Hyeon Seo and Gil-Su Jeon, "Smartphone Security Threat and Countermeasure," TTA Journal(2010), No. 132, pp. 44-48.

[8] Won-Tae Sim, Jong-Myoung Kim, Jae-Cheol Ryou and Bong-Nam Noh, "Android Application Analysis Method for Malicious Activity Detection," Korea Institute of Information Security & Cryptology Journal(2011), 21(1), pp. 213-219.

[9] Financial Security Institute, "Electronic banking services in the Smartphone Security Guide," vol. 6, Jul. 2014.

[10] Korea Yonhap News, "7 out of 10 smartwatches are Samsung gear series." Aug. 2014.

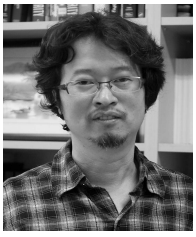
[11] Korea MK News," 'Smartwatch' seven times growth in this year…8 out of 10 Samsung products." Feb. 2014

[12] YoungJae Maeng, DaeHun Nyang and KyungHee Lee, "Password Authentication and Transaction Confirmation Method Using Secret Puzzle on Mobile Banking," Jonornal of The Korea Institute of information Security&Cryptology, 21 (1), pp. 187-199, Feb. 2011.

〈저자소개〉

주 군(Jun Zhou) 학생회원
2013년 8월: 인하대학교 전자 공학과 졸업
2014년 3월~현재: 인하대학교 컴퓨터 정보공학과 석사 과정
〈관심분야〉 네트워크 보안, 무선 인터넷 보안

최 진 춘 (JinChun Choi) 학생회원
2011년 2월: 인하대학교 컴퓨터 정보공학과 졸업
2014년 2월: 인하대학교 컴퓨터 정보공학과 석사
2014년 3월~현재: 인하대학교 컴퓨터 정보공학과 박사과정
〈관심분야〉 네트워크 보안, WSN 보안



양 대 헌 (DaeHun Nyang) 종신회원
1994년 2월: 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업
1996년 2월: 연세대학교 컴퓨터 과학과 석사
2000년 8월: 연세대학교 컴퓨터 과학과 박사
2000년 9월~2003년 2월: 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재: 인하대학교 컴퓨터정보공학과 부교수
〈관심분야〉 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안

이 경 희 (KyungHee Lee) 정회원
1993년 2월: 연세대학교 컴퓨터과학과 학사
1998년 8월: 연세대학교 컴퓨터과학과 석사
2004년 2월: 연세대학교 컴퓨터과학과 박사
1993년 1월~1996년 5월: LG소프트(주) 연구원
2000년 12월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재:수원대학교 전기공학과 부교수
〈관심분야〉 바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식