디지털산업정보학회 논문지 제11권 제2호-2015년 6월
http://dx.doi.org/10.17662/ksdim.2015.11.2.023

NFC를 이용한 스마트폰 상의 사회 공학적 공격 방지 기법 연구*

서 장 원** · 이 은 영***

A Study of Preventing Social Engineering Attack on Smartphone with Using NFC

Suh Jangwon · Lee Eunyoung

〈Abstract〉

When people stands near someone's mobile device, it can easily be seen by others. To rephrase this, attackers use human psychology to earn personal information or credit information or other. People are exposed by social engineering attacks. It is certain that we need more than just recommendation for the security to avoid social engineering attacks. This is why I proposed this paper.

In this paper, I proposed an authentication technique using NFC and Hash function to stand against social engineering attack. Proposed technique result is showing that it could prevent shoulder surfing, touch event information, spyware attack using screen capture and smudge attack which relies on detecting the oily smudges left behind by user's fingers.

Besides smart phone, IPad, Galaxy tab, Galaxy note and more mobile devices has released and releasing. And also, these mobile devices usage rate is increasing widely. We need to attend these matters and study in depth.

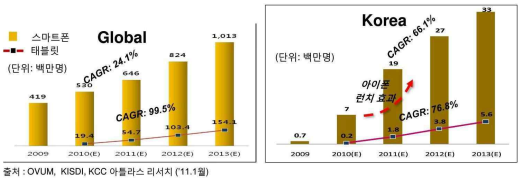
Key Words : NFC, Hash, Smartphone

Ⅰ. 서론

최근 사용이 급증하고 있는 스마트 폰은 3G망은 물론 Wi-Fi, WiBro 등 다양한 인터페이스를 통해 시간과 장소의 제약 없이 인터넷을 이용할 수 있을 뿐만 아니라, 사용자의 요구에 따라 애플리케이션의 설치 및 삭제가 가능하다는 장점을 내세워 그 인기를 더해가고 있다. 최근에는 스마트폰을 이용하여 업무를 처리하는 스마트워크 및 스마트오피스가 주목 받고 있으며, 하나의 콘텐츠를 여러 개의 스크린으로 이용할 수 있는 N 스크린 시대를 위한 서비스 연동 연구가 활발히 진행되는 등 스마트폰은 사회 전반에 걸쳐 큰 관심을 불러일으키고 있다. <그림 1>은 스마트폰의 사용률을 보여주고 있다. 이렇듯 스마트폰의 보급이 급성장하면서 스마트폰 사용이 늘어남에 따라 스마트폰과 관련한 보안 취약점 및 사고도 급속히 증가하고 있다.

스마트폰 사용자가 늘어남에 따라 스마트폰을 이용한 다양한 서비스들이 제공되고 있으며, 이를 이용

* 이 논문은 2014년도 동서울대학교 산학협력단 부설 연구지원센터의 지원에 의하여 연구되었음
** 동서울대학교 컴퓨터소프트웨어과 부교수(교신저자)
*** 동국대학교 대학원 컴퓨터공학과 박사과정



출처 : OVUM, KISDI, KCC 아틀라스 리서치 ('11.1월)

<그림 1> 스마트폰 사용률

하기 위해 필요한 개인정보들이 스마트폰에 저장되고 있다. 즉 개인 프라이버시와 밀접한 관계가 있고 또한, 물리적으로 작아서 일시적 점유 이탈, 분실, 도난 등의 이유로 허락 받지 않은 제 삼자에게 노출되기 쉽다. 이러한 개인정보 유출 공격이 발생하기 시작한 것은 이미 오래전이다. 이런 공격은 고도의 기술을 이용하여 사용자가 인지하지 못한 상황에서 시도되는 경우도 있었으나, 대부분의 경우, 정보보호에 대한 상식이 부족한 일반인들을 대상으로 자신의 중요 정보를 직접 제공하게 만드는 사회공학적인 공격 방법이 주류를 이루었다. 이러한 사회 공학 공격 방법은 비록 매우 허술해 보이지만, 아직까지도 가장 쉽게 정보를 획득할 수 있는 방법으로 인식되고 있어, 적절한 수준의 사용자 인증을 제공하는 것은 중요한 문제이다. 하지만, 기존의 텍스트 기반, 패스워드들은 사회공학 공격 즉, 피싱(Phishing), 파밍(Pharming), 훔쳐보기(Shoulder-surfing), 스파이웨이 등의 공격에 취약하며 모바일 환경에서는 더욱 심각한 문제이다. 이러한 취약점을 보완하기 위한 하나의 대안으로 문자나 숫자로 이루어진 패스워드를 직접 입력하는 대신 이미지를 사용하는 그래피컬 패스워드가 연구되고 있다. 하지만 그래피컬 패스워드는 전통적인 텍스트 패스워드 보다 오히려 훔쳐보기 공격과 스머지(지문 및 흔적 추적하기)공격에 취약하다는 잠재적인 문제점을 가지고 있다[1]. 훔쳐보기 공격은 패스워드에 대한 대표적인 공격방법 중 하나로서, 공격자는 로그인 과정을 직접 관찰하거나 사용자의 인증 과정을 녹화하는 방식으로 패스워드에 대한 정보를 얻을 수 있다. 스머지 공격은 지문 등의 흔적이 남아 육안으로도 패턴을 확인하여 사용자 인증 락을 해지 할 수 있다.

Ⅱ. 관련연구

2.1 사회 공학적 공격의 정의

사회 공학적 공격 기법이란, 고도의 기술이 접목된 해킹기술과는 전혀 무관한 것으로, 기술적인 방법을 이용하는 것이 아니라, 인간의 심리저인 면을 이용하여 개인 정보 또는 신용 정보와 같은 중요한 정보를 획득하거나, 타인스스로가 악의적인 결과를 발생하는 행위를 하도록 유도하는 것을 말한다[7]. 사회공학적인 공격은 단순한 정보획득의 차원뿐만 아니라, 악성 소프트웨어의 실행을 유도하는 데에도 널리 사용되어져 왔다. 최근 가장 큰 문제가 되고 있는 피싱, 그리고 바이러스 유포를 위한 악의적인 행동 유도 등이 이에 포함 될수 있다. 성적인 내용이나, 관리자를 사칭한 메일, 유용한 소프트웨어인 것으로 위장한 첨부 파일, 믿을 만한 업체를 사칭한 메일, 사용자 개인과의 친분을 이용 등 다양한 방법을 통해 사회 공학적인 공격 방법은 공격을 당하는 피해자가, 이와 같은 공격 형태에 대한 지식이 없는 경우, 쉽게 당할 수 있으며, 실제로 아직도 많이 활용되고 있는 공격 방법이다.

2.2 공격 기법

2.1.1 숄더 서핑(Shoulder Surfing)

어깨너머 훔쳐보기 공격(Shoulder-Surfing Attack)

은 사용자의 지식기반 인증수단에서 패스워드, PIN, 개인정보 등의 획득을 위해 누군가의 어깨 디에서 지켜보는 것과 같은 직접적이 관찰을 통한 공격을 말한다[3]. 어깨너머 훔쳐보기 공격은 비단 어깨 뒤에서만이 아니라, 카메라, 타자치는 소리, 디스플레이에서 나오는 전자기적 출력 등을 통해 원거리에서도 이루어 질 수 있다. 이러한 관찰을 통한 사용자의 패스워드 접근 방법은 아무리 잘 설계된 사용자 인증 프로토콜도 간단히 무력화 시킨다. 이러한 측면에서 일련의 보안 과정 중 가장 취약한 부분은 사용자의 패스워드 입력 부분이다.

2.2.2 스머지 공격

스머지 공격(Smudge Attack)은 터치패널을 사용하는 기기에서 가능한 공격으로 터치패널 위헤 남아있는 지문찌꺼기로 사용자 의 움직임을 파악하여 패스워드를 유추하는 공격이다[7]. 자주 터치 되는 영역은 지문찌꺼기가 남아 있게 되고 이것은 패스워드 누출을 가져온다. 특히 안드로이드 폰에서 사용자 인증으로 사용 되고 있는 패턴락은 스머지 공격에 매우 취약하다. <그림 2>는 스머지 공격의 예를 보여준다.

<그림 2> 자산관리 시스템 구성도

2.2.3 레코딩 공격

레코딩 공격은 어깨너머 훔쳐보기 공격의 진화형으로 카메라나 기타 녹화장치를 통하여 사용자 몰래 인증 화면 전체를 녹화하여 패스워드를 알아내는 방법이다. 일반적인 어깨너머 훔쳐보기 공격과 달리 녹화장치를 이용하기 때문에 인증 시 발생하는 모든 정복 공격자에게 노출된다. 공격자는 획득한 정보를 분석하여 패스워드를 쉽게 탈취할 수 있다. 현재까지 기억에 의존하는 어깨너머 훔쳐보기 공격을 방지하는 기술들은 많이 등장하였지만, 레코딩 공격까지 완벽하게 방지하는 기술은 많지 않았다. 이러한 레코딩 공격이 스파이웨어 형태로 동작한다면 사용자는 자신이 눈치 채지 못하는 사이에 패스워드를 탈취 당할 수 있다.

2.2.4 전수 조사 공격(Brute Force Attack)

전수 조사 공격은 공격자가 패스워드를 구성하는 문자 또는 이미지 등의 집합에서 패스워드를 만들 수 있는 모든 조합을 하나하나 입력하여 패스워드를 알아내는 방법이다. 대부분의 인증 기술들은 이론적으로 충분한 시간이 있으면 무작위 대입 공격으로 패스워드를 알아 낼 수 있다. 하지만, 패스워드의 모든 조합을 대입하는 시간과 비용이 많이 들어가 실용적이지 못하다. 일반적으로 무작위 대입 공격을 막기 위해 패스워드 길이를 늘려 패스워드를 구성하는 조합의 개수를 늘린다. 패스워드를 구성하는 조합의 개수가 늘어남에 따라 공격 시간과 비용이 늘어가는 것으로 방지한다.

2.2.5 피싱(Phishing)

피싱은 사회공학적인 방법으로 해당 정보를 보유

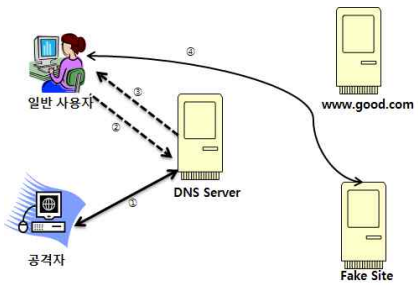
하고 있는 사람을 속여 중요한 정보등르 획득하기 위한 공격 행위를 의미한다. 여기서 피싱(Phishing)이라는 단어는 “비밀을 탐지하다”, “비밀을 찾아내다”라는 의미의 “fish”라는 단어와 전화 해킹을 의미하는 “Phreaking”이라는 단어가 통합되어 만들어진 단어로서, 해커들 사이에서는 이미 오랜전부터 사용되던 단어이다. 현재 가장 널리 사용되는 피싱 공격은 일반적으로 사용자가 특정 웹페이지로 이동하여 해당 웹사이트의 접속을 위한 ID 및 비밀번호를 입력할 때 중요 정보를 획득하는 방식을 택하고 있다. 가장 일반적인 Man-in the-Middle 공격으로는 허위 프락시 서버를 사용하는 것으로 일반 사용자가 특정 웹사이트에 접속하고자 할 때, 정당한 웹페이지를 직접 접속하지 않고, 해커가 운영하는 프락시 서버를 거쳐서 접속되도록 하는 방식을 의미한다.

<그림 3> 피싱 공격의 예

또한 URL 속이기 (Obfuscation)공격 방법이 있는데, 이는 메시지에 포함되어 있는 URL이 실제 보이는 것과는 다른 곳으로 연결되도록 만드는 공격 방식을 말한다. 이러한 피싱은 단순한 기술적인 요소를 이용한 해킹이 아니라, 사회공학적인 공격 방법을 활용하고 있다는 점에서 더 큰 위협이 되고 있다. 일반적으로 시스템 관리를 아무리 잘하더라도, 이러한 사회공학적인 방법을 통하여 해킹이 가능하기 때문에 이에 대한 대응책 개발이 매우 어렵다.

2.2.6 파밍(Pharming)

파밍은 피싱이 사용자에 의해 쉽게 탐지될 수 있는 점을 극복할 수 있는 공격 기법이다. 파밍은 다양한 방법을 통해 정당한 사용자가 특정 도메인명데 대한 IP주소 확인 요구 시, 해커가 장학하고 있는 악의적인 웹 사이트의 주소를 제공하도록 하여 해당 사이트로 접속되도록 유도하는 공격 기법을 의미한다.



<그림 4> DNS 내용 변경을 통한 Fake Site접속유도

2.3 기존 인증 기법 분석

사용자 인증을 위협하는 공격 기법이 소개되면서 이러한 공격 기법을 방지하는 다양한 사용자 인증 기술이 등장하고 있다. 여기서는 기존에 개발되어진 사용자 인증 기술들을 소개한다.

2.3.1 M.TransKey

M.TransKey는 스마트폰 환경에서 터치로그 방지하기 위한 가상 키패드 기술이다. 쿼티 형식의 키보드에 사용시 마다 무작위로 공백을 추가하여 매번 다른 위치에 키가 배열된다. 사용자가 키를 입력 시 매번 다른 위치를 입력하기 때문에 터치로그로 인하여 좌표 값이 노출되더라도 공격자는 입력된 키가 어떤 것인지 알 수 없다. 또한 알파뉴메릭을 입력 가능하

기 때문에 기존에 사용되고 있던 시스템에 적용할 수 있다. 하지만 어깨너머 훔쳐보기 공격으로 인증화면을 지켜본다면 쉽게 패스워드가 노출되며, 더피로그 뿐만 아니라 화면까지 유출되는 스파이웨어의 경우에도 안전하지 못하다. 다음 <그림 5>는 M.TransKey의 사용자 인증 예를 보여준다.

<그림 5> M.TransKey의 사용자 인증 화면

2.3.2 Passfaces

Passfaces는 해외에서 상용화 된 기술로 숫자나 문자가 아닌 사람의 얼굴 이미지를 패스워드 사용한다. 숫자나 문자 보다 이미지를 기억하는 것이 더 쉽고, 이미지 중에서도 사람의 얼굴이 기억하기 하기 쉽다는 이론에 근거하여 개발되었다. 사용자는 시스템이 제공하는 얼굴 이미지 중에서 자신이 패스워드로 사용할 얼굴 이미지를 선택한다. 이후 자신의 패스워드를 확실히 기억하기 위해 각각의 얼굴 이미지를 몇 초간 지켜보는 친숙한 과정을 진행한다. 사용자 인증 시 9개의 이미지가 출력 되는데 이중 8개는 더미 이미지이고 1개는 자신이 설정한 패스워드 이미지이다. 자신이 설정한 패스워드 이미지를 선택하고 동일한 과정을 패스워드 길이만큼 반복한다. 모든 입력이 끝나고 자신의 패스워드와 선택한 얼굴이미지 동일하면 인증에 성공한다. 이 기술은 사람의 얼굴 이미지가 멀리서 지켜볼 때 비슷하게 보인다는 것을 가지고 어깨너머 훔쳐보기 공격을 방지한다. 또한 공격자에게 혼란을 주기 위하여, 사용자 인증 시 출력되는 더미 이미지를 패스워드로 설정한 얼굴 이미지와 동일한 성별 또는 비슷한 얼굴로 구성하여 출력한다. 하지만 가까이서 지켜보거나 만원경이 등의 도구를 이용하여 자세히 관찰한다면 패스워드 이미지를 정확히 확인 할 수 있으며, 레코딩 공격에 취약하다는 문제점을 가지고 있다. 다음 <그림 6>은 Passfaces의 사용자 인증 화면을 나타낸다.

<그림 6> Passface의 사용자 인증 예

2.2.3 DAS

DAS(Dynamic Authentication System)는 어깨너머 훔쳐보기 공격을 방지하는 PIN 기반 가상 키패드 기법이다. 이 기법은 터치스크린을 사용하는 스마트폰이나 은행 ATM 머신에서 무작위로 배치된 가상 숫자 키패드를 사용하여 입력하는 기법이다. <그림 7>

은 DAS의 가상 키패드 화면을 보여준다. 사용자는 보기 버튼을 누른 상태에서 키패드를 보고 패스워드의 위치를 기억한 다음 보기 버튼에서 손을 떼 키패드 위에 숫자가 사라지면 기억한 숫자를 선택 한다. 입력 후 키패드의 배열은 무작위로 재배열 된다. 키패드의 숫자가 사라진 상태에서 입력하기 때문에 일시적인 어깨 너머 훔쳐보기 공격에는 안전하지만 지속적인 어깨 너머 훔쳐보기 공격에는 안전하지 못하다.

<그림 7> DAS의 사용자 인증 화면

2.4 NFC의 개요

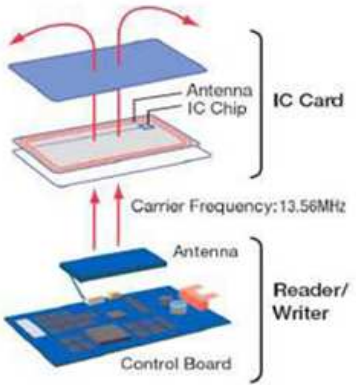
NFC는 Near Field Communication의 약자로 근접거리 무선 통신기기의 표준 기술을 의미한다. NFC는 RFID 처럼 단지 읽기만 하는 수동적인 기능 이 아니라 서로 능동적으로 상호 통신하도록 한 것으로, 기술적인 측면보다는 사용자 측면으로의 접근한 기술로 볼 수 있다[2]. NFC는 13.56MHz의 주파수를 사용하고 있으며, 42Kbps의 전송속도로 약 10cm 거리에서 단말기 간 데이터를 주고받을 수 있다. 사용자는 NFC 폰에 NFC 유심을 장착해 이용할 수 있으며 휴대폰 하나로 스마트카드와 RFID Reader/Write를 하나로 합쳐 놓은 것 같은 기능을 수행할 수 있다. 통신사의 네트워크를 통하지 않고 기기 간 직접 커뮤니케이션 하는 기능 과 더불어 정보의 Encryption으로 타 RFID 보다 보안성이 뛰어나다.

2.4.1 NFC 기술 특징

RFID 종류 중 하나로 13.56MHz 주파수 대역에서 비 접촉식으로 근접거리(10cm)내의 단말기 간 데이터 교환 기술로써, 통신사의 네트워크를 통하지 않고 기기 간 직접 Communication 기능과 NFC가 정보의 읽기 뿐 아니라 쓰기도 가능한 양방향 통신을 지원한다. RFID 기술의 발달로 PassiveType과 Active Type을 포함해서 최대 900m 까지 사용 거리가 늘어났으며 리더와 태그 개념을 적용해 비즈니스 모델에 따라 활용 범위가 크게 확대 될 것이라고 전망된다. 실생활과 연계된 복잡한 정보활동에 대한 해결책으로, 모든 타입의 사용자 장치에 대한 'Touch-and-Start' 조작으로 접촉과 실행에 대한 직관적 접속 편의성을 제공하여 보안 처리가 내장된 (Built-Insecurity) 지불/재정 등의 응용을 사용자들이 쉽게 사용할 수 있게 하였으며 휴대전화, AV(Audio Visual)장비, 디지털 카메라, PDA, 세트 탑 박스 등과 컴퓨터를 직관적으로 접속하게 하여, 전화번호, 그림, 티켓, MP3, 파일, 북마크 등의 모든 컨텐츠를 용이하게 동작 시킬 수 있다. NFC의 기술은 능동모드 혹은 수동모드에서 운영될 수 있어 비 접촉 스마트카드나 RF 태그 와 같은 다양한 소동형 장치와 폭넓게 통신할 수 있다. 무선 단거리 통신기술, 13.56MHz RFID 기술 기반, 10cm 이상의 운영거리, 비접촉식 RFID 기술과 호환 가능하며 최대 424 Kilobits/s 의 데이터 교환 속도의 특징을 갖는다.

2.4.2 NFC 기술 장점

읽기와 쓰기 등의 카드-판독기 사이의 트랜잭션은 간단하게 카드를 판독기 가까이 가져감으로써 가능해진다. 카드는 IC 칩과 안테나를 내장하며 배터리를 가지고 있지 않아 유지비용이 거의 들지 않는다[11].



<그림 8> 무선 단거리 통신의 구성도

(2) 처리 속도

본 연구를 통해서 카드를 인식하여 인증하고 데이터를 읽고 쓰는 모든 처리 과정이 0.1초 이내에 이루어지며, <그림 8>에서 무선 단거리 통신의 실행 과정을 나타내었다. 212Kbps의 데이터 전송 속도는 다른 스마트카드가 낼 수 있는 최대 속도의 거의 2배에 달한다. 이로 인하여 사용자가 단순 데이터를 NFC 카드를 통해서 입력 받을 때 정확도가 높아진다.

2.4.3 NFC 운영모드

NFC 기술은 다양한 근거리 무선 통신들의 다양한 성질들을 결합하여 단말기의 ON/OFF와 관계없이 항상 리더기를 통해 인식이 가능한 카드 에뮬레이션 모드, NFC 활성화 상태에서 RFID Tag 정보를 인식하여 휴대폰이 카드 리더기로서 작동하는 리더/라이터 모드, 두 대의 NFC 휴대폰이 카드 리더기로서 작동하여 데이터를 상호간에 전송할 수 있는 P2P 모드로 작동 가능하다. 이 모드들은 RFID와 같이 데이터를 읽고 수정할 수 있는 모드, 블루투스 등과 연결하여 데이터 통신 서비스 가능 모드, 카드에 탑재되어 비접촉식 카드의 성질을 지원하면서 스마트카드의 정확하고 빠른 응답속도를 기반으로 하는 안전한 서비스들이 지원 가능하다. <그림 9>에서 NFC 세 가지 운영모드를 나타낸다.

<그림 9> NFC 운영 모드

(1) Peer-to-Peer(P2P)모드

P2P 운영모드(ISO 18092)는 두 개의 NFC 디바이스 간의 링크 수준의 통신을 지원한다. 블루투스 페어링 절차를 NFC 기술로 대체 하여 연결 초기절차를 단순화 한다. 연결확립을 위해 클라이언트(NFC Peer-to-Peer Initiator)는 호스트(NFC Peer-to-PeerTarget)를 검색하고 NDEF(NFC DataExchange Format) 메시지 형식을 통해 데이터를 전송한다.두 대의 NFC 휴대폰이 카드리더기로서 작동하여 데이터를 상호간에 전송 할 수 있는 모드이며, 또한 능동 모드로서 데이터 전송을 위해 독자적인RF필드를 생성해야 하므로 전력 소모가 크다.

(2) Reader/Writer모드

NFC 디바이스는 NFC 트랜스폰더에 저장된 데이터를 읽고 수정할 수 있다. 사용자는 통제 관리 대상의 NFC 태그 정보와 같이 NFC 디바이스가 태그를 읽어 정보를 조회할 수 있는 기술이다. URL 주소가 저장되어 있는 태그에서 NFC 모바일 디바이스를 터치하면 URL 주소를 읽고 그 주소의 웹 사이트에 접근을 지원한다.

(3) Card Emulation 모드

NFC 디바이스가 스마트카드(ISO 14443)처럼 동작하는 모드이기 때문에 외부 NFC 리더기는 스마트카드와 NFC 디바이스를 구분할 수 없다. 이 모드에서는 비 접촉식 지불, 티켓팅 서비스가 가능하다. 실시간 범위 통제 시스템에서는 모바일 NFC 리더기의 태그 정보 서버 측에 전송하여 인증을 진행하여 보다 안전하고 편리한 로그인 절차를 수행할 수 있다.

2.4.4 NFC와 WPAN 통신 기술의 비교

NFC 기술은 다른 PAN 영역의 무선 통신과 비교하면 매울 짧은 거리에서의 통신 기술이다. 스마트카드 표준인 ISO 14443을 기반으로 약 10cm 정도의 거리에서의 통신 방법을 지원하며, 이러한 기술은 사용자가 모든 행위에 주체가 되는 사용자 중심의 서비스가 가능할 수 있다는 특징을 가지게 됨으로써 새로운 차원의 'Touch-and-Go'의 편리성을 추구할 수 있다. <표 1>는 NFC 기술과 단거리 무선 통신과의 기술의 비교이다. 표에서 사용자 중심의 기술이 발전되는 것을 확인 할 수 있다.

<표 1> NFC 기술과 단거리 무선 통신과의 기술의 비교

구분	NFC	RFID	IrDa	Bluetooth
설정 시간	<0.1 ms	<0.1 ms	~0.5ms	~6ms
사용성	사람중심 쉽고 편리 직관적이며 빠름	아이템 편리 쉽고 편리	데이터 중심 쉽고 편리	데이터 중심 다소 편리
USE CASE	지불 액세스공유 서비스준비 편리한설정	아이템 추적	데이터 제어 및 교환	데이터교환 헤드셋용 네트워크
소비자 경험	터치 간단한연결	정보획득 필요	쉽게 사용	구성필요

2.5 Hash 함수

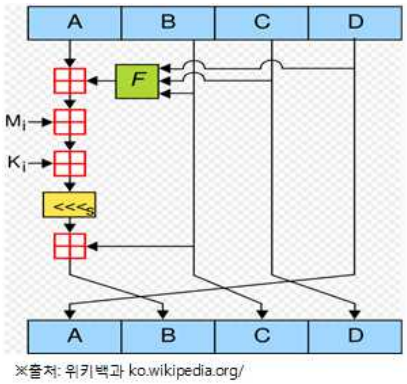
2.5.1 Hash 함수의 개요

해쉬 함수는 임의의 길이를 갖는 메시지를 입력 받아 고정된 길이의 해쉬 값을 출력하는 함수이다. 암호 알고리즘에는 키가 사용되지만, 해쉬 함수는 키를 사용하지 않으므로 같은 입력에 대해서는 항상 같은 출력이 나오게 된다. 이러한 함수를 사용하는 목적은 입력 메시지에 대한 변경할 수 없는 증거 값을 뽑아냄으로서 메시지의 오류나 변조를 탐지할 수 있는 무결성을 제공하는 목적으로 주로 사용된다.

2.5.2 MD5

MD5(Message-Digest algorithm 5)는 128비트 암호화 해시 함수이다. RFC 1321로 지정되어 있으며, 주로 프로그램이나 파일이 원본 그대로인지를 확인하는 무결성 검사 등에 사용된다. 1991년에 로널드 라이베스트가 예전에 쓰이던 MD4를 대체하기 위해 고안했다. 1996년에 MD5의 설계상 결함이 발견되었다. 이것은 매우 치명적인 결함은 아니었지만, 암호학자들은 해시 용도로 SHA-1와 같이 다른 안전한 알고리즘을 사용할 것을 권장하기 시작했다. 2004년에는 더욱 심한 암호화 결함이 발견되었고. 2006년에는 노트북 컴퓨터 한 대의 계산 능력으로 1분 내에 해시 충돌을 찾을 정도로 빠른 알고리즘이 발표되기도 하였다. 현재는 MD5 알고리즘을 보안 관련 용도로 쓰는 것은 권장하지 않으며, 심각한 보안 문제를 야기할 수도 있다. 2008년 12월에는 MD5의 결함을 이용해 SSL 인증서를 변조하는 것이 가능하다는 것이 발표되었다.

<그림 10> 단일 MD5 연산, MD5에서는 이 단일 연산을 64번 실행한다. 16개의 연산을 그룹화한 4라



<그림 10> One MD5 Operation

운드로 묶인다. F는 각 라운드에서 사용하는 비선형 함수를 가리키며, 각 라운드에서는 각각 다른 함수를 사용한다. Mi는 입력 메시지의 32-비트 블록을 의미한다. <<<s는 s칸 만큼의 레프트로테이션을 가리키며, s는 각 연산 후 값이 변한다. ⊞은 모듈로 232덧셈을 말한다.

2.5.3 SHA

Secure Hash Algorithm(SHA)은 national Institute of Standards and Technology(NIST)에서 개발한 표준으로서 FIP1) 180으로 출판되었다. 이것을 보통 Secure Hash Standard(SHS)이라고도 부른다. 이 표준은 MD5를 기초로 해서 만들어졌다. 이표준은 1995년에 FIP180-1로 개정되었는데 이 안에 SHA-1이 포함되어 있다. 이 표준은 FIP180-2로 한 번 더 개정되었고 여기에서 SHA-224, SHA-256, SHA-384와 SHA-512 네 개의 버전이 포함되어 있다. <표 2>에 이들에 대한 특성을 나타내었다.

이 버전들은 모두 다 동일한 구조를 가지고 있다.

<표 2> 안전 해쉬 알고리즘(SHA)의 특성

Characteristics	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Maximum Message size	2^{64}-1	2^{64}-1	2^{64}-1	2^{128}-1	2^{128}-1
Block size	512	512	512	1024	1024
Message digest size	160	224	256	384	512
Number of rounds	80	64	64	80	80
Word size	32	32	32	64	64

Ⅲ. NFC와 해시함수를 이용한 기법 제안

3.1 제안한 인증 전체 구성도

다음 <그림 11>은 본 논문에서 제안하는 NFC와 해시함수를 이용한 인증 방법에 대한 전체 구성도로서 단계별 설명은 다음과 같다.

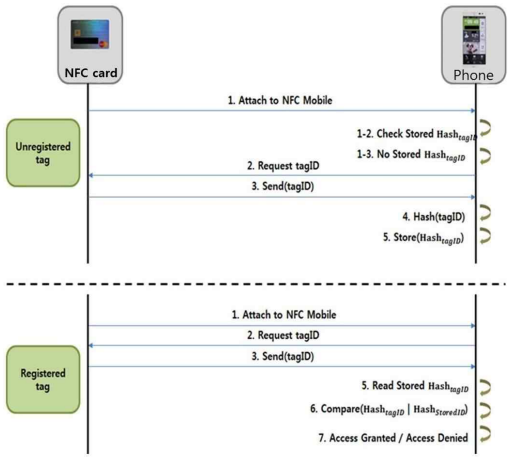
<그림 11> 제안 인증 구성도

다음 <그림 11>은 본 논문에서 제안하는 NFC와 해시함수를 이용한 인증 방법에 대한 전체 구성도로서 단계별 설명은 다음과 같다.

스마트폰의 기존 인증 구성도는 스마트폰에 내장되어있는 NFC를 읽어 들일수 있는 리더기를 통해 비

밀번호나 패턴을 이용해서 인증을 시도하는 방법이라면[6] 제안 방법은 <그림 11>에 나타나있듯이 사전에 등록된 카드의 해쉬 값과 스마트폰에 접촉할 때 카드의 해쉬 값들 비교하여 인증하는 방법을 제시하였다.

3.2 제안한 인증 상세 프로토콜



<그림 12> 제안 인증 프로토몰

○ 최초 등록

1. NFC카드는 최초로 Mobile에 접촉을 시도한다.

1-2. 이때 Mobile에 접촉된 NFC카드는 사전에 등록된 HAshtagID 여부를 체크해야 한다.

1-3. Mobile은 사전에 등록되어진 HAshtagID가 없음을 확인한다.

2. Mobile은 사전 등록하기 위하여 NFC 카드로부터 tagID를 요청한다.

3. NFC카드는 Mobile로부터 요청되어진 tagID를 Mobile로 tagID를 보낸다.

4. Mobile은 NFC카드 tagID를 SHA-512를 이용하여 Hash하여 Hash값을 만들어 낸다.

5. SHA-512를 이용하여 만든 Hash값, 즉 HAshtagID를 저장 한다.

○ 사전 등록 시 비교

1. NFC카드는 Mobile에 접촉을 시도한다.

2. Mobile은 NFC카드에 사전에 등록된 tagID를 요청한다.

3. NFC.카드는 Mobile로부터 요청되어진 tagID를 Mobile로 tagID를 보낸다.

4. Mobile은 사전 등록된 즉, 저장된 HAshtagID을 read한다.

5. 이 때, read한 HAshtagID와 사전에 등록된 즉, HAshstoredID를 비교 한다.

6. HAshtagID와 HAshstoredID비교에 따라 접근 허용 또는 접근 금지라는 결과가 나타나게 된다.

NFC.카드는 Mobile로부터 요청되어진 tagID를 Mobile로 tagID를 보낸다.

Mobile은 사전 등록된 즉, 저장된 HAshtagID을 read한다.

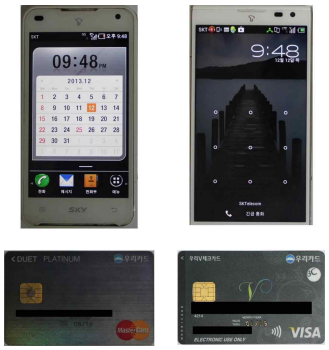
이 때, read한 HAshtagID와 사전에 등록된 즉, HAshstoredID를비교 한다.

HAshtagID와 HAshstoredID비교에 따라 접근 허용 또는 접근 금지라는 결과가 나타나게 된다.

3.3 실험 및 결과

3.3.1 실험 환경

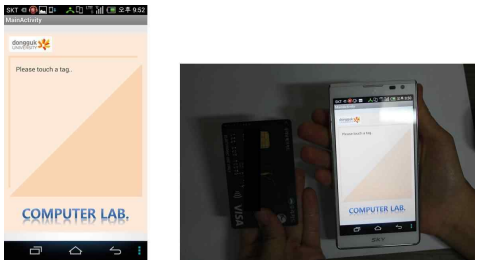
본 논문에서는 기존 논문에서 사용한 수식을 이용하여 통합개발환경 (IDE : Integrated Development Environment)과 안드로이드 소프트웨어 개발 킷 그리고 운영체제 윈도우를 이용하여 개발 하였다.



<그림 13> 실험 기기 및 카드

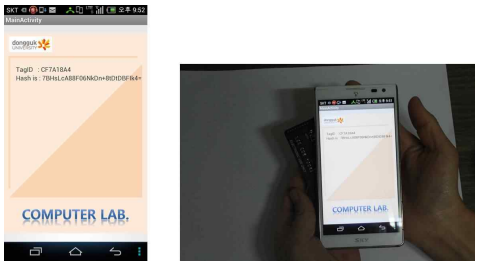
<그림 13>는 본 논문에서 사용하는 개발도구로는 베가S5, 베가레이서이고, 종류가 다른 두 개의 체크카드를 사용하였다.

3.3.1 실험 결과



<그림 14> 실험 결과1

<그림 14>의 실험 결과1은 사전에 제안 실험 환경이 Android developer tools를 실행시켜 둔다. 그리고 Mobile 베가S5의 디바이스를 설치 한 후 Android developer tool과 Mobile 베가 S5를 연결하여 제안한 실험 코딩을 Run as하면 실행되면서 화면에 please touch a tag.. 라고 보여주게 된다. 그리고 제안한 개발 환경인 카드를 Mobile 베가 S5에 접촉하기 위해 Mobile 뒷면에 카드를 갖다 댄다.



<그림 15> 실험 결과2

<그림 15>의 실험 결과2는 Mobile 베가 S5에 제안한 실험 환경인 카드를 접촉하는 순간 Mobile은 카드에 고유번호 값을 읽어 온다. Mobile은 카드로부터 읽어 온 고유의 값을 tagID로 화면에 보여준다. 그리고 tagID 즉, 카드의 고유 값을 SHA-1를 사용하여 16진수로 카드의 해쉬 값을 Hash is로 화면에 보여주고 있다.

Ⅳ. 결론

스마트폰 사용자들의 급증하고 있는 사회공학 공격, 훔쳐보기(Shoulder-surfing)등에 의하여 발생할 수 있는 보안 문제를 강화 방법을 제안 하였다. 공격에 취약한 모바일 환경에 더욱 심각한 문제이기 때문에 취약점을 보완하기 위한 대안으로 문자나 숫자로 이루어진 패스워드를 직접 입력하는 대신 이미지를 사용하는 그래피컬 패스워드가 사용되고 있지만 오히려 훔쳐보기 공격에 취약하다는 잠재적인 문제점을 가지고 있다. 현재는 스마트폰으로 뱅킹, 비즈니스 업무, 행정, 건강 등 여러 가지 많은 중요한 일들을 일부 수행하고 있고 또한 그 범위는 더욱 커지고 있다. 이렇듯 빠르게 변하는 스마트폰, 태블릿 세상에서 보안에 대해서 실질적인 해결책을 간구해야 한다. 따라서 본 논문은 누구나 가지고 있는 카드로 NFC와 해쉬함수를 이용하여 스마트 폰의 사회공학적 공격

으로 부터의 보안 강화를 제안하였다. 추후의 연구는 카드의 고유번호의 값과 스마트폰 단말기의 고유번호를 해쉬 하여 2Factor 인증으로 발전시키는 연구가 필요할 것이며, 특정 개인적인 컨텐츠에 NFC와 해쉬 함수를 이용하여 인증 할 수 있는 연구 또한 필요할 것이며, 단기간의 발전 가능성으로는 앱을 개발하여 Play 스토어에 배포 또한 가능할 것이다.

참고문헌

[1] 김기언, 조성제, “스마트폰 보안 취약점 동향,” 한국정보과학회논문지, 제37권, 제2호(B), 2010, pp. 90-94.

[2] 김형준, “NFC 기술이 적용된 모바일 환경에서의 취약점을 이용한 피싱 공격 연구,” 세종대학교대학원 석사학위논문, 2013, pp. 27-29.

[3] 김시원, “어깨너머 훔쳐보기 공격에 견고한 더미 키 기반 패스워드 인증 기법,” 연세대학교대학원 석사학위논문, 2012, pp. 16-18.

[4] 김종우, 김성환, 김광휘, 조환규, “훔쳐보기 공격에 견고한 그리드 기반 패스워드 시스템의 개선,” 정보과학회논문지, 제17권, 제4호, 2011, pp. 264-268.

[5] 박경현, 김애영, 이상호, “스머지 및 훔쳐보기 공격에 강한 이중 링 구조 기반의 그래픽 패스워드 기법,” 한국정보과학회논문지, 제39권, 제1호, 2012, pp. 312-313.

[6] 송정은, 김진복, 이문규, “진동을 이용한 스마트 디바이스 사용자 인증 방법,” 한국차세대컴퓨팅학회논문지, 제10권, 제1호, 2014, pp. 6-21.

[7] 최양서, 서동일 “사회공학적 공격방법을 통한 개인정보 유출기술 및 대응방안 분석,” 한국정보보호학회논문지, 제16권, 제1호, 2006, pp. 40-48.

[8] 김현진, 서화정, 이연철, 박태환, 김호원 “어깨 넘어 훔쳐보기에 저항성을 가진 가상금융키패드의 구현,” 한국정보학회논문지, 제23권, 제6호, 2013, pp. 21-29.

[9] 이재식, 김형주, 유한나, 박태성, 전문석, “NFC 환경에서 개인정보보호를 위한 취약점 분석 및 대책 수립 방법론,” 정보보호학회논문지, 제22권, 제2호, 2012, pp. 357-365.

[10] 이민구, 김동완, 손진수, “NFC를 활용한 능동형 인증 방법,” 한국통신학회논문지, 제37권, 제2호, 2012, pp. 149-156.

[11] 최창열, 한수범, “모바일 3. 0과 NFC 기반에서의 e-비즈니스 모델,” e-비즈니스, 제12권, 제3호, 2011, pp. 269-292.

■ 저자소개 ■

서 장 원
Suh Jangwon

2001년 9월~현재 동서울대학교 컴퓨터소프트웨어과 부교수
2000년 8월 숭실대학교 대학원 컴퓨터학과 (공학박사)
1996년 2월 숭실대학교 대학원 컴퓨터학과 (공학석사)
1992년 2월 서울과학기술대학교 컴퓨터공학과 (공학사)

관심분야 : 정보보호, 암호 알고리즘, 암호학
E-mail : jwsuh@dsc.ac.kr

이 은 영
Lee Eunyoung

2014년 3월~현재 동국대학교 대학원 컴퓨터공학과 박사과정
2014년 2월 동국대학교 대학원 컴퓨터공학과 (공학석사)
2011년 2월 평생교육진흥원 전자계산학과 (이학사)
2010년 2월 동서울대학교 컴퓨터소프트웨어과 졸업 (공업 전문학사)

관심분야 : 보안, 랩리듀스, 데이터마이닝, 모바일컴퓨팅
E-mail : jwoil79@naver.com

논문접수일: 2015년 5월 20일
수 정 일: 2015년 6월 1일
게재확정일: 2015년 6월 5일