情 報 保 護 學 會 誌
第21卷 第4號, 2011. 6

모바일 ID를 저장하여 관리 및 이용하고 있는 스마트폰의 사용자 인증 동향

나 사 랑*, 신 수 연*, 권 태 경*

요 약

스마트폰의 성능 향상과 다양한 기능 추가에 따라 스마트폰 사용자의 수는 급증하고 있으며, 모바일 인터넷 활용도가 높아짐에 따라 스마트폰을 통해 PC를 이용한 업무를 대체하는 것이 가능해졌다. 이러한 스마트폰의 성능 진화와 다양한 추가 서비스 제공은 사용자에게 편리함을 주고 있지만, 개인정보 노출, 모바일 악성 코드 등 다양한 위협에 노출될 가능성이 있다. 스마트폰에서의 사용자 인증은 스마트폰 기기를 안전하게 사용하기 위해서 필요한 기본적인 보안 기능이다. 본 논문에서는 스마트폰의 보안 위협 요소와 스마트폰의 사용자 인증 기법에 대해 알아본다. 스마트폰의 전자 지갑 애플리케이션과 해당 애플리케이션을 위해 개발된 사용자 인증 기법에 대해 알아본 후 전자 지갑 애플리케이션을 포함한 스마트폰 사용자 인증 기법의 특징, 장점, 단점 등을 비교 분석한다.

Ⅰ. 서 론

전 세계적으로 스마트폰 사용자 수는 이미 10억 명을 넘었고, 국내 휴대폰 가입자의 경우도 총 5,000만 명 중 스마트폰 사용자 수는 약 1,000만 명에 이르고 있다[16]. 다양한 버전의 스마트폰이 출시됨에 따라 향후 스마트폰 가입자 수는 더욱 증가할 것으로 예상하고 있다.

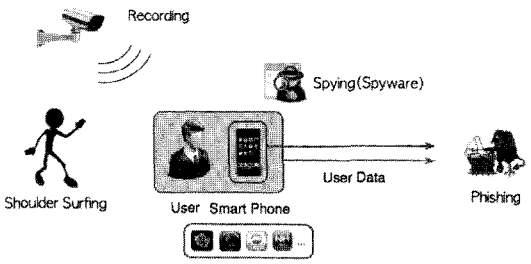
스마트폰은 기존 모바일의 전화, 문자메시지 기능을 포함해 다양한 컨텐츠를 제공한다. 모바일 인터넷을 통한 정보 검색 및 GPS 기능, 사진, 음악, 동영상의 멀티미디어 서비스, 게임, 이메일, 일정 관리, 인터넷 뱅킹, 증권, 금융 결제, 전자 지갑 등이 스마트폰으로 이용이 가능하다[17]. 스마트폰의 성능이 향상되고 기능이 다양해짐에 따라 스마트폰에 개인 정보 및 업무 관련 정보, 신용 카드 정보 등 다양한 정보를 저장할 수 있게 되었다. 스마트폰의 모바일 인터넷을 통한 다양한 서비스는 사용자에게 편리함을 제공하고 있지만 개인 혹은 기업의 민감한 정보를 담고 있으므로 다양한 프라이버시 공격에 노출될 가능성이 높다. 스마트폰에서의 사용자 인증은 이러한 공격으로부터 스마트폰과 스마트폰을 통한 서비스를 안전하게 하기 위해 기본적인 보안 요구사항이다.

사용자 인증 크게 지식 기반 인증, 소유 기반 인증, 생체인식 기반 인증으로 크게 나뉘지만 스마트폰에서는 지식 기반 인증 기법과 소유 기반 인증 기법을 많이 사용된다. 그 중에서도 텍스트 기반의 PIN (Personal Identification Number)이나 패스워드, 그래픽 기반의 패턴 락(Pattern Lock)이 대표적이다.

본 논문에서는 스마트폰의 보안 위협에 대해 알아보고, 스마트폰의 사용자 인증 기법과 전자 지갑 애플리케이션을 포함한 여러 애플리케이션에서 사용되고 있는 다양한 사용자 인증 기법에 대해서 알아본다. 또한 스마트폰의 사용자 인증 기법을 분류하고 간단히 비교 분석한다.

본 논문은 다음과 같이 전개된다. 2장에서는 사용자 인증과 스마트폰의 보안 위협 요소에 대해 정리하고, 3장에서는 스마트폰의 사용자 인증 기법에 대해 설명한다. 4장에서는 스마트폰의 애플리케이션 중에서 민감한 개인 정보를 사용하는 전자 지갑 애플리케이션을 위한 사용자 인증 기법에 대해 알아보고 5장에서는 본 논문

이 논문은 2010년도 세종대학교 미래전략연구비 지원에 의한 논문임.
* 세종대학교 컴퓨터공학과 정보보호 연구실 ({tot, shinsy80}@sju.ac.kr tkwon@sejong.ac.kr)



〔그림 1〕 보안 위협 모델

의 결론을 기술한다.

Ⅱ. 사용자 인증 및 보안 위협 요소

2.1 사용자 인증

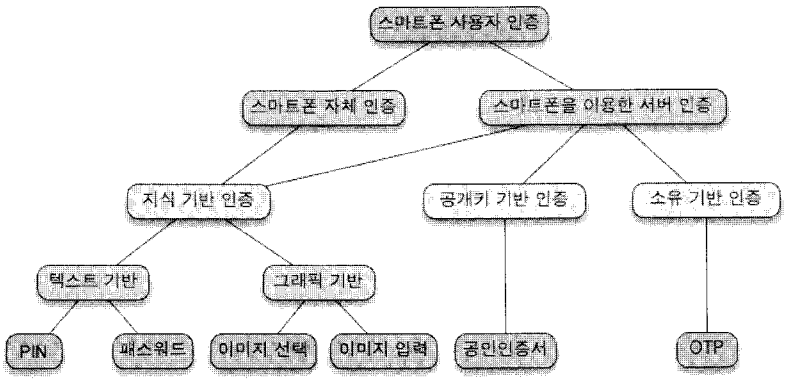
사용자 인증은 크게 지식 기반 인증, 소유 기반 인증, 생체인식 기반 인증, 세 가지로 분류할 수 있다. 첫 번째는 지식 기반 인증 방법으로 텍스트 기반 패스워드 기법과 그래픽 기반 패스워드 기법이 이에 속한다. 이 중에서도 가장 많이 사용되는 지식 기반 인증 방법은 텍스트 기반 패스워드 기법으로 본인만이 알고 있는 정보인 PIN이나 패스워드를 가지고 인증을 하는 것이다. NIST (National Institute of Standards and Technology)에서 권고한 안전한 패스워드는 길고 랜덤한 패스워드(랜덤한 12문자 패스워드)이다. 하지만 실제로 사용자는 기억하기 쉽고 짧은 패스워드를 선택하는 경향이 있기 때문에 전수조사(exhaustive search or brute force) 공격, 사전(dictionary) 공격, 숄더 서핑(shoulder surfing) 공격과 같은 다양한 공격에 취약하다. 두 번째는 소유 기반 인증 방법으로 ID 카드, 보안 토큰, 휴대폰(인증서) 등을 이용해 사용자를 인증하는 것이다. 소유 기반 인증은 안전성을 높이기 위해 지식 기반 인증과 함께 사용되는 경우가 많다. 소유 기반 인증 기법은 텍스트 기반 패스워드 기법보다 숄더 서핑 공격에는 강인하지만, 사용자가 소지하고 있어야 하는 불편함이 있으며 분실하거나 도난당할 가능성도 있다. 세 번째는 생체인식 기반 인증 방법으로 지문, 홍채와 같이 개인의 유일한 생물학적 특징을 사용하여 사용자를 인증하는 것이다. 이 기법은 복제가 어렵고 숄더 서핑 공격에 강인하다. 하지만 개인의 생물학적 특징이 한 번 노출되면 사용이 불가능하게 된다는 단점이 있다[9].

위에서 언급한 사용자 인증 기법들의 단점을 보완하기 위해 새로운 인증 기법들이 연구되고 있으며, 지식 기반 인증 기법, 소유 기반 인증 기법, 생체인식 기반 인증 기법을 혼용해서 사용하는 하이브리드 인증 기법에 대해서도 연구가 진행되고 있다.

2.2 보안 위협 요소

컴퓨터 및 스마트 기기들은 인터넷으로 연결되어 있기 때문에 공격자의 위협이 항상 존재하고 있다. 본인도 모르는 사이 컴퓨터에 악성코드가 설치되어 개인의 정보나 자료가 유출될 수 있고 혹은 컴퓨터가 마비가 되기도 한다. 또한 기술적인 보안 체계를 우회하기 위해 친구나 지인으로 위장하는 등 인간관계와 사회적 특성을 이용한 다양한 사회 공학적 공격으로 인해 피해를 입을 수 있다. 이 외에도 [그림 1]과 같이 사용자의 패스워드 입력을 녹화하는 레코딩(recording) 공격[4], 다른 사람의 컴퓨터 및 스마트폰에 잠입하여 개인 정보를 빼가는 스파이웨어(spyware)[2], 다른 사람의 로그인 과정을 관찰하여 패스워드를 가로채는 숄더 서핑 공격[3], 금융기관 등의 웹사이트로 위장하여 개인의 신용카드번호, 계좌 정보 등을 가로채는 피싱(phishing) 공격[8] 등 다양한 공격의 가능성이 있다.

스마트폰은 일반 핸드폰과는 다르게 무선 인터넷 및 외부 인터페이스를 개방하여 제공하고 있다. 이는 사용자에게 편리함을 제공해주는 반면 악성코드의 전파경로가 다양해지고 악의적인 개발자에 의해 악성코드가 내재된 애플리케이션이 등장하면서 보안적인 측면에서는 취약점으로 작용하기도 한다. 또한 스마트폰은 휴대할 수 있기 때문에 숄더 서핑 및 레코딩 공격의 대상이 될 수 있으며, 분실의 위험이 따르기도 한다. 숄더 서핑 공격의 경우 공공장소에서 그 위험이 더 크며, 스마트폰 같은 휴대기기는 경우 언제, 어디서, 누가 자신의 정보를 가로채 가는지 알 수 없기 때문에 더욱 조심해야 한다. 일반 핸드폰은 분실했을 시 전화번호, 메모, 사진 등의 정보 유출이 전부였지만, 스마트폰은 각종 개인정보, 신용카드, 인증서 및 기업의 정보 등을 저장하고 있어 프라이버시 침해, 기업 정보 유출, 금전적 피해 등을 입을 수 있다[6]. 위와 같은 스마트폰의 특징 때문에 일반 PC보다 보안에 취약할 수 있으며, 스마트폰에 대한 보안을 강화해야할 필요가 있다.



〔그림 2〕 스마트폰 사용자 인증 분류

Ⅲ. 스마트폰 사용자 인증

3.1 스마트폰 사용자 인증

스마트폰 인증은 스마트폰 자체 인증과 스마트폰을 이용한 서버 인증으로 나눌 수 있다. 스마트폰 자체 인증은 [그림 2]의 (a)와 같이 스마트폰 혹은 애플리케이션을 이용하기 위해 사용자를 인증하는 것이다. 스마트폰을 이용한 서버 인증은 [그림 2]의 (b)와 같이 스마트폰을 이용해서 웹 사이트 및 인터넷 뱅킹 등의 서버에 인증을 받는 것이다. 이 경우 웹 사이트의 기존 인증 방법과 동일한 방식으로 로그인 할 수 있으며, 아이디 및 패스워드를 스마트폰에 저장하여 사용 가능하다.

[그림 3]은 스마트폰 인증과 스마트폰을 이용한 서버 인증을 포함한 스마트폰의 사용자 인증 기법 분류를 보여준다. 스마트폰의 사용자 인증 기법은 크게 지식 기반 인증, 소유 기반 인증 및 이 둘을 동시에 이용하는 공개키 기반 인증 기법으로 분류될 수 있다. 지식 기반 인증의 텍스트 기반으로는 PIN, 패스워드를 사용하는 인증 기법이 있으며, 그래픽 기반으로는 패스페이스(Passface)[14]와 같은 이미지 선택 방식과 패턴 락과 같은 이미지 입력 방식이 있다. 소유 기반 인증 기법으로는 OTP를 사용하는 기법과 공인 인증서와 같이 공개키 암호와 전자 서명을 이용하는 인증 기법이 있다. 스마트폰을 이용한 인증은 텍스트 기반 인증 기법의 PIN이나 텍스트 패스워드가 가장 널리 사용되고 있으며, 공인 인증서와 OTP는 인터넷 뱅킹과 같은 금융 서비스에서 많이 사용되고 있다. [표 1]은 스마트폰에서 사용되고 있는 사용자 인증 기법들에 대한 특징을 장점과 단점으로 나눠서 설명하고 있다.

(a) 스마트폰 인증

(b) 스마트폰을 이용한 서버 인증

〔그림 2〕 스마트폰 사용자 인증

3.2 스마트폰의 사용자 인증 예

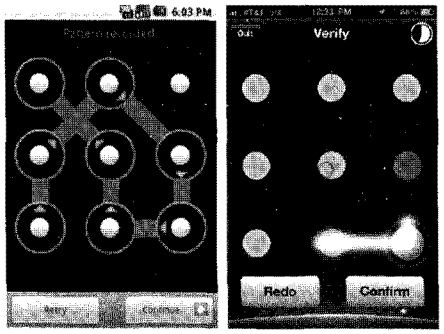
일반 핸드폰은 메인 화면, 전화, 문자메시지, 사진, 인터넷 기능마다 잠금 기능을 설정할 수 있다. 스마트폰은 일반 핸드폰처럼 메인 화면 잠금 기능은 제공하지만 문자메시지, 사진 등 각 기능 별로 잠금 설정은 제공하지 않는다. 하지만 각 애플리케이션마다 제공하는 잠금 기능을 사용할 수 있다는 점에서 일반 핸드폰과 차이가 있다. 스마트폰은 다양한 애플리케이션만큼 여러 종류의 사용자 인증 기법을 제공한다. 스마트폰에서 사용하는 사용자 인증 기법을 메인 화면 잠금을 위한 인증 기법과 메신저, 인터넷 뱅킹, 증권 등 애플리케이션 분류별 인증 기법으로 나누어 살펴본다.

〔표 1〕 스마트폰 사용자 인증 기법 비교

인증 기법	장점	단점	안전성	편의성
PIN	숫자만을 이용해 패스워드를 입력하므로 기억하기 쉽고 간단	PIN의 길이가 짧을 경우 전수조사 공격에 취약[12]	낮음	높음
패스워드	기억하기 쉽고 숫자 패스워드보다 텍스트 패스워드 선택 공간이 큼	텍스트 패스워드의 길이가 짧거나 랜덤하지 않을 경우 사전 공격에 취약 가능[7]	보통	보통
패스페이스	이미지 기반의 패스워드로 사용자에게 친숙하고 선택 가능한 이미지가 다양할 경우 패스워드 공간이 크다.	패스워드로 생성한 이미지들을 기억해야하고 라운드 수가 적을 경우 쉽게 노출 가능	보통	낮음
패턴 락	터치 입력 방식을 사용하여 비밀정보를 입력하기 편리	숫자 패스워드보다 패스워드 공간이 작고 패턴이 쉽게 노출 가능하며[20], 패턴 흔적(smudge)을 이용한 스머지 공격[1] 가능	낮음	높음
OTP	일회용 패스워드이므로 패스워드가 노출되더라도 안전[11]	OTP 생성기를 소지하고 있어야만 인증 가능	높음	낮음
공인 인증서	공인 인증서와 텍스트 패스워드를 동시에 인증하므로 스마트폰을 통해 안전한 금융 결제 가능[13]	초기 설정 시 컴퓨터나 USB에 저장되어 있는 공인 인증서를 스마트폰에 저장해야 하는 불편함 존재[18]	높음	낮음

3.2.1 메인 화면

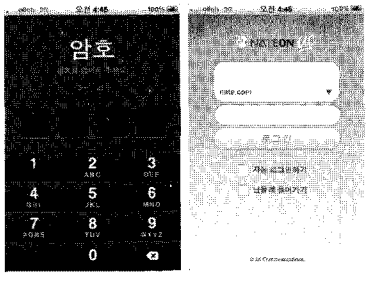
일반 핸드폰은 기본적으로 4자리 PIN을 사용해 잠금 기능을 설정하도록 되어 있는데, 스마트폰은 PIN, 텍스트 패스워드, 패턴 락 중 하나를 선택하여 사용할 수 있다. 안드로이드 폰 사용자의 경우는 패턴 락을 이용한 잠금 기능을 많이 사용하는데, 이를 기반으로 한 다양한 유형의 패턴 락 기법이 많이 등장하고 있다. [그림 4]는 스마트폰의 잠금 화면을 보여준다. 왼쪽 그림은 안드로이드의 패턴 락 화면이고 오른쪽 그림은 아이폰의 패턴 락 화면이다. 안드로이드 패턴 락은 모든 현재 안드로이드 스마트폰에 적용되어 있으며, 아이폰 패턴 락은 아직 아이폰에 적용되어 있지 않고 개발만 되어 있는 상태이다.



〔그림 4〕 패턴 락 잠금 화면

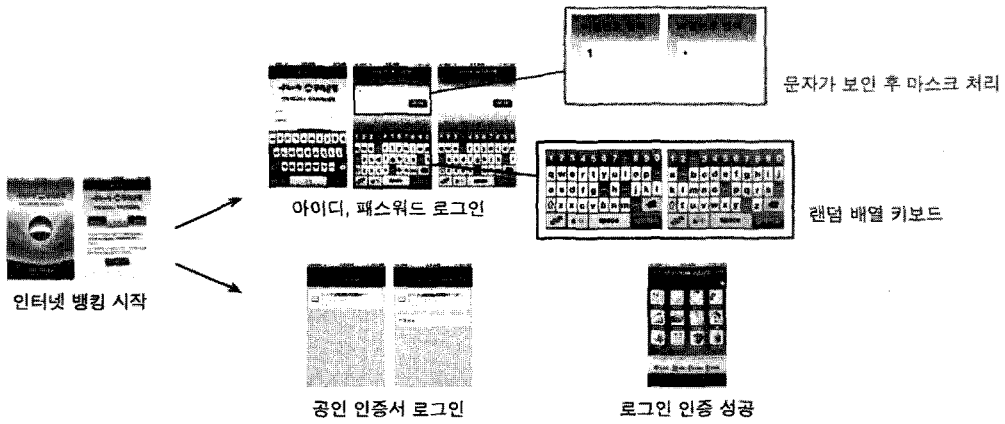
3.2.2 메신저

스마트폰은 메신저 애플리케이션을 제공하여 사용자들이 실시간으로 메시지와 데이터를 주고받을 수 있도록 해준다. 일반 컴퓨터에서 사용되는 메신저를 포함한 다양한 스마트폰 용 메신저 애플리케이션이 출시되었는데, 그 중에서도 카카오톡은 가입자 수가 1,000만 명을 넘는 스마트폰의 주요 애플리케이션으로 자리 잡았다. 스마트폰의 문자 메시지는 따로 잠금 기능을 제공해주지 않는다. 따라서 다른 사람이 자신의 메시지를 볼 수가 있는데, 이에 반해 카카오톡은 자체 잠금 기능이 있어 사용자가 필요 시 4자리 PIN을 정해서 잠금 설정을 할 수 있다. 다른 스마트폰 메신저 애플리케이션 역시 자체 잠금 기능을 제공하는데, 기존의 컴퓨터 기반에서



(a) 카카오톡 (b) 네이트온

〔그림 5〕 메신저 로그인 화면

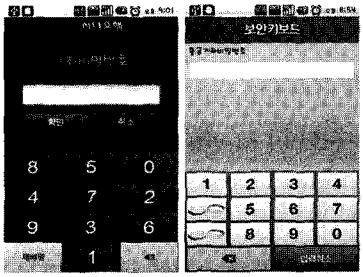


〔그림 6〕 우리은행 스마트 뱅킹 인증 실행 과정

사용했던 아이디와 텍스트 패스워드를 이용한 인증 방법을 많이 사용한다. [그림 5]의 (a)는 카카오톡의 잠금 화면이고 (b)는 네이트온의 잠금 화면이다.

3.2.3 인터넷 뱅킹

사용자가 스마트폰으로 인터넷 뱅킹을 할 수 있도록 각 은행마다 고유 애플리케이션을 제공하고 있다. 인터넷 뱅킹은 사용자의 개인 정보 및 금융 정보를 이용하기 때문에 인증을 필수로 하고 있다. 애플리케이션의 로그인 시 기본적으로 아이디와 패스워드 사용 혹은 공인 인증서를 이용한 인증 기법이 많이 사용되고 레코딩 공격에 강인하게 하기 위해 패스워드 키패드를 랜덤하게 배열해 주는 형태로 제공하고 있다. 패스워드 입력 시 랜덤 공백 배열을 이용한 특수 키패드가 제공되는데, 아이디 입력 시에도 패스워드 입력 시와 동일한 키패드가 사용되거나 일반 키패드가 사용되기도 한다. [그림 6]은 우리은행 인터넷 뱅킹의 로그인 과정을 보여준다. 아이디, 패스워드 혹은 공인 인증서 로그인 기법을 선택하여 로그인 할 수 있다. 두 방식 모두 텍스트 패스워드를 이용하여 인증하게 되는데, 이 때 랜덤 배열 키패드가 제공된다. 왼쪽 하단의 재배열 키를 누르면 QWERTY 키패드와 알파벳 순서 키패드를 번갈아가며 랜덤하게 키패드의 문자 배열을 바꿔준다. 랜덤 배열 키패드는 레코딩 공격엔 안전하지만 숄더 서핑 공격에는 안전하지 못하고, 패스워드를 입력 할 경우 패스워드가 바로 마스크 처리되지 않고, 패스워드를 보여준 다음 마스크 되는 단점이 있다.



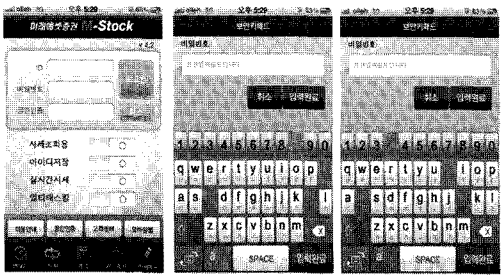
(a) 하나은행 (b) 우체국 뱅킹

〔그림 7〕 PIN 입력 화면

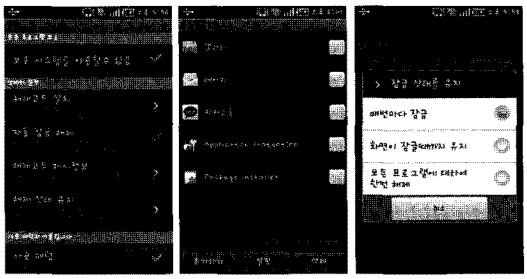
인터넷 뱅킹 이용 시 해당 계좌에 대한 4자리 PIN을 입력해야 한다. PIN을 입력할 때 랜덤 숫자 키패드를 이용하게 되어 있는데, 랜덤 숫자 키패드는 [그림 7]의 (a)와 같이 공백을 사용하지 않고 단순히 숫자들의 배열을 랜덤하게 바꿔주는 형태로 제공되거나 [그림 7]의 (b)와 같이 문자 키패드와 비슷한 방법으로 공백을 임의의 위치에 넣어주는 형태로 제공된다.

3.2.4 증권

스마트폰 증권 애플리케이션은 기본적으로 아이디와 패스워드를 이용하여 사용자를 인증하는데, 인터넷 뱅킹과 유사한 방법으로 아이디는 일반 키패드, 패스워드는 랜덤 공백 배열을 이용한 키패드를 제공한다. 하지만 증권 애플리케이션은 시세조회용 로그인이 아닐 경우 아이디, 패스워드와 함께 공인인증서를 추가적으로 인증해 주어야 한다. 공인인증서의 비밀번호 입력 키패드는 패스워드 입력 키패드와 동일한 랜덤 키패드가 제공



〔그림 8〕 미래에셋 증권 로그인 화면



〔그림 9〕 Application Protection(안드로이드)

된다. [그림 8]는 미래에셋 증권의 로그인 화면이다. 아이디, 패스워드, 공인인증서를 모두 인증해야 하며 입력 키패드는 랜덤 키패드가 제공된다.

3.2.5 기능별 잠금 애플리케이션

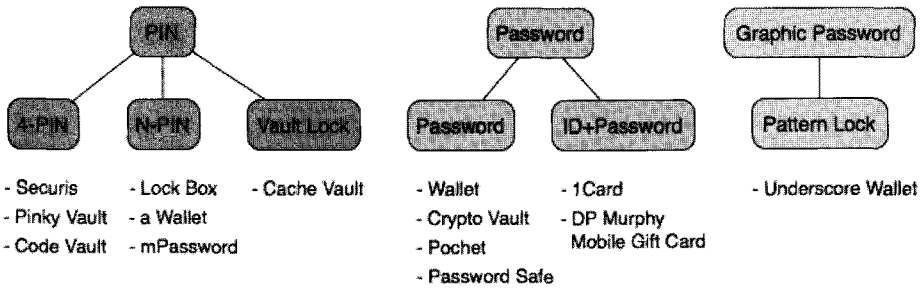
스마트폰은 전체 잠금이나 애플리케이션 자체 잠금 기능은 있지만 전화, 문자메시지, 사진 등과 같은 기본 프로그램들을 기능별로 잠글 수 없다. 하지만 사용자의 편의를 위해 기능별 잠금을 설정할 수 있게 해주는 잠금 애플리케이션들이 나오면서 기본 프로그램들도 따로 관리할 수 있게 되었다. [그림 9]은 안드로이드 용 잠금 애플리케이션인 'Application Protection'으로 이 애플리케이션은 환경 설정을 통해 기본 프로그램을 포함해서 여러 응용 프로그램들을 잠금 기능을 설정할 수 있다. 또한 텍스트 패스워드나 패턴 락을 사용하여 프로그램들을 보호하고, 잠금 상태 유지 설정을 통해 각 프로그램들을 매번 잠글 것인지 한번만 잠글 것인지 등을 설정할 수 있다[19]. 아이폰의 경우는 환경 설정을 통해 각 프로그램들의 잠금 설정을 할 수 없다. 잠금 설정이 가능한 동일한 기능의 애플리케이션을 제공하긴 하지만 기존 프로그램에서 데이터를 가져와야하는 불편함이 있다.

Ⅳ. 스마트폰 전자 지갑 사용자 인증

4.1 전자 지갑

전자 지갑은 전자상거래에서 사용되는 전자 지불 시스템의 일종으로 컴퓨터, 스마트 기기 등에 화폐가치를 저장해 지갑처럼 사용하면서 전자상거래시 대금을 결제할 수 있는 소프트웨어를 말한다. 인터넷 사이트를 통해 물품이나 서비스를 구매할 경우 소비자는 자신의 신용카드 번호나 ID 확인 등으로 물품구매가 즉시 이루어져 모든 구체적인 정보를 입력해야 하는 불편을 해소시킨다. 또한 각 인터넷 사이트 간 고유한 인증체계에 대해 사용자가 최소한의 인증만을 수행하고, 사용자 인증 정보의 통합 관리 및 사용자에게 편리하고 일관된 인터페이스를 제공한다[5].

컴퓨터를 이용한 전자 지갑은 사용 범위가 제한적이나 스마트폰을 이용한 전자 지갑은 휴대할 수 있어 저장할 수 있는 정보의 종류도 다양하다. 신용카드, 멤버십 카드, 은행 보안카드, 통장 정보, 보험, 신분증, 운전면허, 여권, 명함 등의 정보를 저장함으로 여러 장의 카드가 필요 없이 스마트 폰 하나만으로 사용이 가능하고 인터넷 계정의 ID 및 패스워드를 저장할 수 있어 사이



〔그림 10〕 전자 지갑 사용자 인증 기법 분류

트에 쉽게 인증을 받을 수 있게 해준다. 또한 사진, 중요메모 및 각종 패스워드를 저장할 수 있다[10].

전자 지갑은 사용자의 개인 정보 및 금융 정보, 패스워드와 같은 중요한 정보를 저장하고 있다. 따라서 전자 지갑에 대한 사용자 인증은 필수적이며, 인증에 대한 안전성 역시 강화되어야 한다. 다음으로 전자 지갑 애플리케이션에서 사용되고 있는 인증 기법에 대해서 살펴본다.

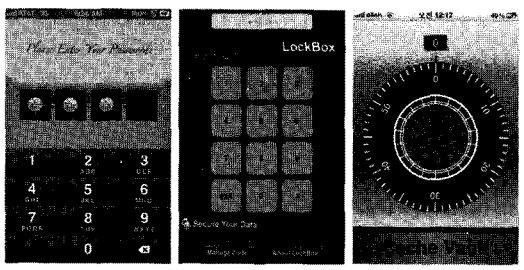
4.2 전자 지갑 사용자 인증 기법

스마트폰 전자 지갑은 기본적으로 PIN과 텍스트 패스워드를 이용한 사용자 인증 기법을 많이 사용한다. 또한 스마트폰의 사용자 인터페이스를 이용한 그래픽 기반의 패스워드 인증 기법이 사용되기도 한다. 전자 지갑 애플리케이션의 사용자 인증 기법은 크게 PIN, 텍스트 패스워드, 그래픽 패스워드로 분류할 수 있는데, PIN은 4자리 PIN과 N자리 PIN으로, 텍스트 패스워드는 아이디와 패스워드 둘 다 입력하는 방법과 패스워드만 입력하는 방법으로 나눌 수 있다. [그림 10]는 전자 지갑의 사용자 인증 기법을 분류하고 각각에 해당하는 애플리케이션을 보여 준다.

4.2.1 PIN

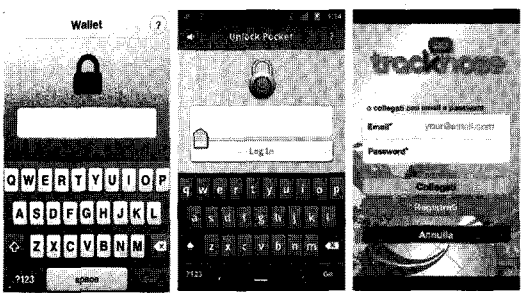
4자리 PIN은 [그림 11]의 (a)와 같이 0부터 9의 숫자 4개를 선택하여 PIN을 만들어 인증하는 방법으로 ATM, 은행 계좌 패스워드 등 여러 사용자 인증에서 가장 많이 사용된다. 4-PIN은 자리수가 짧고 숫자만을 이용하기 때문에 간단하고 기억하기 쉽지만 PIN의 길이가 짧을 경우 전수조사 공격에 취약할 수 있다.

N-PIN은 4-PIN과 거의 유사하지만 사용자가 임의로 PIN의 자리 수를 선택할 수 있다. 하지만 PIN의 길이가 너무 짧으면 외부에 쉽게 노출될 수 있기 때문에 4자리 이상의 PIN을 사용할 것을 권장하고 있다. [그림 11]의 (b)는 N자리의 PIN을 사용하는 예를 보여주고 있다.



(a) Pinky Vault (b) Lock Box (c) a Wallet

〔그림 11〕 전자 지갑에서의 PIN 사용자 인증 기법



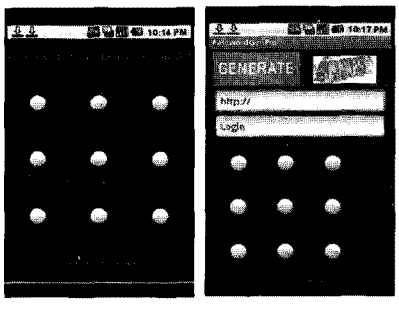
(a) Wallet (b) Pocket (c) 1Card

〔그림 12〕 전자 지갑에서의 텍스트 패스워드 사용자 인증 기법

[그림 11]의 (c)는 'Cache Vault' 애플리케이션으로 금고의 자물쇠 원리를 이용한 사용자 인증 기법을 사용한다. 0에서 59까지의 숫자를 가지고 4자리 패스워드를 설정한다. 첫 번째 번호는 시계반대방향으로 두 번째 번호는 시계방향으로 자물쇠를 돌린다. 앞의 과정을 번갈아가면서 4자리 패스워드를 모두 찾은 다음 'Cache Vault'를 터치하면 인증이 된다.

4.2.2 텍스트 패스워드

웹 사이트에 로그인 시 일반적으로 아이디(혹은 이메일 정보)와 함께 패스워드를 입력받아 사용자를 인증한다. 전자 지갑 애플리케이션도 아이디와 패스워드를 이용하여 사용자를 인증하는데 단순히 패스워드만을 요구하는 경우도 있다. [그림 12]의 (a),(b)는 패스워드만을 이용한 인증 화면이고 (c)는 이메일과 패스워드 둘 다를 이용한 인증 화면이다.

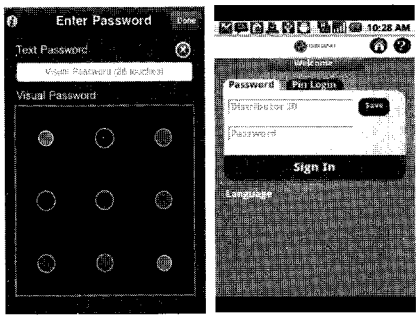


〔그림 13〕 Password Gen Pro

4.2.3 그래픽 패스워드

스마트폰에서 가장 많이 사용되는 그래픽 패스워드인 패턴 락은 전자 지갑 애플리케이션에서도 사용되고 있다. [그림 13]은 'Password Gen Pro'의 애플리케이션 인증 화면이다. 'Password Gen Pro'은 일반적인 패턴 락의 작동 원리를 이용한 사용자 인증 방식을 사용한다. 웹사이트의 주소 및 계정 정보를 저장해 두면 초기에 생성한 마스터 패턴(master pattern)만을 이용하여 인증받을 수 있다[15].

일반적인 패턴 락은 한 번 지나간 점은 거쳐서 가지



(a) Underscore Wallet (b) My OG Wallet

〔그림 14〕 멀티 인증 기법

〔표 2〕 전자 지갑, 인터넷 뱅킹, 증권 애플리케이션의 비교

분 류	사용자 인증 분류	애플리케이션	특 징
전자 지갑	텍스트 기반 (PIN)	Pinky Vault (아이폰)	4자리 PIN 인증, 사진, 동영상 잠금 기능 및 신용카드, 은행, 웹 사이트 아이디, 패스워드 등의 정보를 저장
		Crypto Cards (아이폰)	4자리 PIN 인증, 운전 면허증, 학생증, 멤버십 카드 등의 ID카드를 저장
		Lock Box (아이폰)	N자리 PIN 인증, 신용카드, 은행 계좌, PIN, 패스워드 등의 정보를 저장 및 비밀 노트 기능 제공
		a Wallet (안드로이드)	N자리 PIN 인증, 은행 계좌, 시리얼 번호, 노트 등의 정보를 저장
		Cache Vault (아이폰)	금고 자물쇠 원리를 이용한 4자리 PIN인증, 신용카드, 은행 계좌, Identifications, 멤버십 정보, ATM PIN, 여권, 웹 사이트 계정 등의 정보를 저장
	텍스트 기반 (패스워드)	Wallet (아이폰)	텍스트 패스워드 인증, 신용카드, 멤버십 카드, 운전 면허 번호, 여권 번호, 웹 사이트 아이디, 패스워드 등의 정보를 저장
		Pocket (안드로이드)	텍스트 패스워드 인증, 신용카드, 은행 계좌, 라이센스, 멤버십, 보험, 세금, 여권, 이메일 계정 등의 정보를 저장
		1Card	아이디, 패스워드 인증, 로얄티 카드, 기프트 카드, 모바일 쿠폰 등의 정보를 저장
		UNIQPass (안드로이드)	아이디, 패스워드 인증, 신용카드, 인터넷 뱅킹, 여권, 멤버십 카드, Social Security 번호 등의 정보를 저장
	그래픽 기반	Underscore Wallet(아이폰)	텍스트 패스워드, 패턴 락 두 개의 인증 방법을 제공, 패스워드, 사진, 음성 메모, 신용카드, 은행 계좌, 웹 사이트 및 이메일 계정 아이디, 패스워드 등의 정보를 저장
인터넷 뱅킹	텍스트 기반 / 공개키 기반 인증	우리은행 (아이폰)	ID, 패스워드 혹은 공인 인증서 로그인, 패스워드 입력 시 QWERTY 키패드와 알파벳 순서 키패드를 번갈아가며 랜덤 배열 키패드를 제공
		새마을금고	ID, 패스워드 혹은 공인 인증서 로그인, 아이디와 패스워드 입력 시 랜덤 배열 QWERTY 키패드를 제공
	공개키 기반 인증	국민은행 (아이폰)	공인 인증서 로그인, 랜덤 배열 QWERTY 키패드를 제공
		기업은행	공인 인증서 로그인, QWERTY 키패드와 알파벳 순서 키패드를 번갈아가며 랜덤 배열 키패드를 제공
		농협	공인 인증서 로그인, 랜덤 배열 QWERTY 키패드를 제공
		우체국 뱅킹	공인 인증서 로그인, QWERTY 키패드와 알파벳 순서 키패드를 번갈아가며 랜덤 배열 키패드를 제공
증권	공개키 기반 인증	미래에셋증권	ID, 패스워드, 공인 인증서 로그인, 패스워드 입력 시 랜덤 배열 QWERTY 키패드를 제공
		대신증권	ID, 패스워드, 공인 인증서 로그인, 패스워드 입력 시 랜덤 배열 QWERTY 키패드를 제공
		키움증권	ID, 패스워드, 공인 인증서 로그인, 패스워드 입력 시 랜덤 배열 QWERTY 키패드를 제공
		현대증권	ID, 패스워드, 공인 인증서 로그인, 패스워드 입력 시 QWERTY 키패드와 알파벳 순서 키패드를 번갈아가며 랜덤 배열 키패드를 제공
		삼성증권	ID, 패스워드, 공인 인증서 로그인, 패스워드 입력 시 랜덤 배열 QWERTY 키패드를 제공
		동양증권	ID, 패스워드, 공인 인증서 로그인, 패스워드 입력 시 QWERTY 키패드와 알파벳 순서 키패드를 번갈아가며 랜덤 배열 키패드를 제공

않는 이상 다시 지나갈 수 없다. 하지만 [그림 14]의 (a)의 'Underscore Wallet'은 이전에 지나간 점을 다시 지나갈 수 있어서 일반 패턴 락에 비해 패턴의 패스워드 공간이 크다. 또한 대부분의 전자 지갑 애플리케이션은 시작 시 한 번의 인증으로 이용이 가능하지만 'Underscore Wallet' 은 애플리케이션 시작 시 인증하지 않고 정보를 담고 있는 각 항목에 접근할 때마다 인증을 요구한다.

4.2.4 멀티 인증 기법

어떤 전자 지갑 애플리케이션은 로그인 방식을 선택할 수 있다. [그림 14]의 (a)와 같이 텍스트 패스워드나 패턴 락 이 중 하나를 이용하거나 [그림 14]의 (b)와 같이 PIN 또는 텍스트 패스워드를 선택하여 인증 받을 수 있다. 'Underscore Wallet'의 경우 'Text Password' 와 'Visual Password' 중 하나를 선택해서 로그인할 수 있다. 'Text Password'는 기존의 텍스트 패스워드 입력과 동일한 인증 방식이고 'Visual Password'는 패턴 락의 작동 원리를 이용한 인증 방법이다. 사전에 패스워드를 등록하였다면 등록된 패스워드 방식으로만 인증할 수 있다.

V. 결 론

본 논문에서는 스마트폰 기반으로 사용되는 다양한 사용자 인증 기법들에 대해서 살펴보았다. 스마트폰은 기존의 사용자 인증 기법과 함께 스마트폰의 터치 입력 방식을 이용한 패턴 락과 같은 그래픽 기반의 새로운 인증 기법이나 랜덤 배열 키패드를 사용할 수 있다. [표 2]는 전자 지갑, 인터넷 뱅킹, 증권 애플리케이션의 사용자 인증 기법 및 각 애플리케이션에 대한 특징을 예로 들어 설명하고 있다. 인터넷 뱅킹, 증권 같은 금융 서비스를 제공하는 애플리케이션들은 키 입력의 안전성을 높이기 위해 랜덤 배열 키패드나 공개키 기반의 인증 기법을 사용한다. 이에 반해 전자 지갑은 간단한 PIN, 텍스트 패스워드 인증 기법을 사용하는 경우가 대부분이고 그래픽 기반 패스워드 기법을 사용하는 전자 지갑도 있지만 소수에 불과하다. 다양한 개인 정보를 저장하고 있는 전자 지갑에 대한 보안을 강화해야 할 필요가 있으며, 안전하면서도 사용자에게 편리함을 주는 사용자 인증 기법에 대한 연구가 필요하다.

이와 같은 연구 개발 분야는 향후 더욱 많은 관심을 받을 것이며, 참고로 2010년에 숄더 서핑 공격에 저항하는 전자 지갑 인증 기법으로 한국전자통신연구원과 세종대학교에서 SPIN(Secure PIN) 기법을 개발한 바 있다.

참 고 문 헌

[1] Adam J. Aviv, K. Gibson, E. Mossop, M Blaze and J.M. Smith, "Smudge attacks on smartphone touch screens," In Proc. of Woot'10, Aug. 2010.

[2] K. Fujita and Y. Hirakawa, "A study of password authentication method against observing attacks," Intelligent Systems and Informatics IEEE SISY, Nov. 2008.

[3] V. Roth, K. Richter and R. Freidinger, "A PIN-Entry method resilient against shoulder surfing," CCS Proc. of the 11th ACM Conf. on Computer and communications security, pp. 236-245, Oct. 2004.

[4] G. Shaw, "Spyware & Adware: the risks facing businesses," Elsevier Network Security, pp. 12-14, Sep. 2003.

[5] Tanaka and Tatsuo, "Possible economic consequences of digital cash," First Moday Vol. 1, no. 2-5, Aug. 1996.

[6] 강동호, 한진희, 이윤경, 조영섭, 한승완, 김정녀, 조현숙, "스마트폰 보안 위협 및 대응 기술," *전자통신동향분석* 25(3), pp. 73-75, 2010 6월.

[7] 김창순, "엿보기 공격에 내성을 지닌 편리한 패스워드 입력 방법," 공학석사학위 청구논문, 인하대학교, 2010 2월.

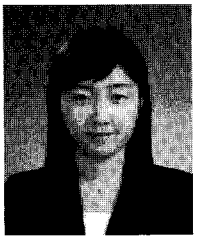
[8] 박대우, 서정만, "Phishing, Vishing, SMiShing 공격에서 공인인증을 통한 정보침해 방지 연구," *한국컴퓨터정보학회논문지*, 12(2,46), pp. 171-180, 2007 5월.

[9] 신수연, 권태경, "개인정보보호를 고려한 HCI 기술에 대한 고찰," *정보과학회지* 27(12), pp. 68-77, 2009 12월.

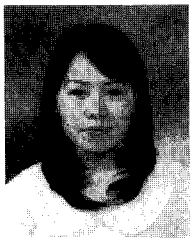
[10] 조영섭, 진승헌, "사용자 중심 ID 관리 기능을 제공하는 전자 ID 지갑 시스템," *전자통신동향분석* 23(4), pp. 11-14, 2008 8월.

[11] 최동현, 김승주, 원동호, "일회용 패스워드(OTP: One-Time Password) 기술 분석 및 표준화 동향," *정보보호학회지* 17(3), pp. 12-17, 2007 6월.
[12] Advantages and Disadvantages of Different Authentication Tools http://www.theiia.org/download.cfm?file=29264
[13] OTP와 공인증서 방식의 비교 http://blog.naver.com/smgrl
[14] PassfacesTM http://www.realuser.com
[15] PasswordGenPro application Info http://kr.androlib.com/android.application.innovate-android-passwordgenpro-ziAzp.aspx
[16] 스마트폰 사용자 1,000만 시대 http://it.donga.com/newsbookmark/5053
[17] 스마트폰의 기능, 위키백과 http://ko.wikipedia.org/wiki/스마트폰
[18] 아이폰4 공인인증서 이용 방법 http://272it.com/10094527497
[19] 안드로이드 잠금 어플 Application Protection http://yae0829.blog.me/40122909780
[20] 패스워드와 패턴 락의 보안성 http://blog.naver.com/playtouch

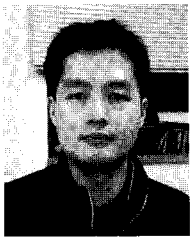
〈著者紹介〉



나 사 랑 (Sarang Na)
학생회원
2011년 2월 : 세종대학교 컴퓨터공학과 학사
2011년 3월 ~ 현재 : 세종대학교 컴퓨터공학과 석사과정
관심분야 : 시스템 보안, 네트워크 보안, 암호프로토콜, HCI 보안 등



신 수 연 (Sooyeon Shin)
학생회원
2004년 2월 : 세종대학교 컴퓨터공학과 학사
2006년 2월 : 세종대학교 컴퓨터공학과 석사
2006년 9월 ~ 현재 : 세종대학교 컴퓨터공학과 박사과정
관심분야 : 프라이버시 보호기술, 익명성 기술, 센서네트워크 보안, HCI 보안 등



권 태 경 (Taekyoung Kwon)
종신회원
1992년 2월 : 연세대학교 컴퓨터과학과 학사
1995년 2월 : 연세대학교 컴퓨터과학과 석사
1999년 8월 : 연세대학교 컴퓨터과학과 박사
1999년 ~ 2000년 : U.C. Berkely Post-Doc.
2001년 ~ 현재 : 세종대학교 컴퓨터공학과 부교수, 정보보호학회 이사 및 편집위원
2007년 ~ 2008년: Univ. Maryland at College Park 교환교수
관심분야 : 암호프로토콜, 네트워크 프로토콜, 센서네트워크 보안, 프라이버시 보호, HCI 보안 등