정 보 보 호 학 회 지
제25권 제6호, 2015. 12

위치 정보 기반의 모바일 장치 보안 시스템 제안 (잠금 기능 중심으로)

박 재 혁*, 지 선 학**

요 약

최근에 모바일 장치 관련 정보 유출과 더불어 유출된 정보를 악용한 범죄가 빈번하게 일어남에 따라 정보호호에 대한 관심과 중요성이 높아지고 있다. 국내 모바일 장치 관련 사용자 수도 해를 거듭할수록 기하급수적으로 증가하고 있는 추세이며, 이에 따른 모바일 장치의 보안에 대한 중요성 역시 대두되고 있다. 그 중에서도 사용자 측의 모바일 잠금 기술인 비밀번호, PIN, 얼굴 인식 등의 기능을 활용하여 사용자 모바일 장치에 대한 암호 보안 기술을 적용하고 있다. 또한 사용자들의 개인정보를 다루는 서비스 이용이 증가함에 따라 모바일 장치 자체의 보안에 대한 안전한 처리 문제, 편리성, 효율성 등을 고려한 문제점이 대두되고 있다.

본 지에서는 사용자 모바일 장치 잠금 관련 동향을 분석하고, 이와 관련된 모바일 장치 잠금 어플리케이션의 한계점에 대해서 살펴본다. 또한 현 모바일 장치 잠금 시스템이 직면하는 보안성과 편의성의 한계점을 보완하기 위한 위치 정보 기반의 모바일 장치 보안 시스템을 제안한다.

Ⅰ. 서 론

기존의 모바일 장치 잠금 어플리케이션들의 경우에는 단순히 어플리케이션의 비활성화나, 개인정보 파일, 사진 등과 같은 특정 어플리케이션에 대한 잠금을 수행하는 어플리케이션들이 다수이다. 일반적으로 사용자의 가정이나 개인의 공간에서는(보안 위협이 적은 곳) 사용자 모바일 장치 보안이 필요 없는 경우가 있고, 공공장소나 여러 사람들이 교류하는 곳(보안 위협이 많은 곳)에서는 사용자 모바일 장치 보안이 필요하게 된다. 예를 들어, 사용자의 개인정보를 보호하기 위하여 주소록 관련 어플리케이션에 암호 잠금을 수행하였는데, 공공장소나 다수가 모여 있는 공간에서는 필요한 조치일 수 있으나, 사적인 공간이나 가정집에 위치하였을 때는 일반적으로 본인만이 모바일 장치를 제어하기 때문에 어플리케이션에 대한 암호 잠금이 필요하지 않다.

일반적인 모바일 장치 사용자들은 자신의 개인정보가 중요시 된다고 생각하면 장소에 관계없이 어플리케이션에 대한 암호 잠금 기능을 활성화 한다. 반대로 정보보호가 중요시 되지만, 사용자 편의성이나 효율성 측면에서 암호 잠금 기능을 비활성화 하는 경우가 있다. 이는 정보호호 관점에서는 모바일 장치에 대한 취약성이 증가하는 결과를 갖는다.

정보보호 측면의 암호 잠금 기능과 잠금 해제의 편의성을 아우르면서 사용자들의 요구 사항을 충족시킬 수 있는 어플리케이션은 현 시점에는 전무한 상태이며, 위와 같은 한계점에 대한 새로운 제안을 하고자 한다. 본 제안에서는 GPS, 데이터 네트워크 혹은 Wi-Fi를 활용하여 사용자의 위치를 수집한 후, 사용자가 정의하였던 보안 단계를 설정한다. 이후 사용자의 위치 별로 차등적 보안 단계를 적용하여 모바일 장치 잠금을 편리하고, 효율적으로 활성화 할 수 있는 방안에 대해서 제안하고자 한다.

Ⅱ. 기존의 유사 어플리케이션 현황 분석

분석에 활용할 어플리케이션의 범위는 안드로이드 어플리케이션으로 하며, 구글의 ’플레이스토어(안드로

* 동국대학교 국제정보대학원 정보보호학과(pjhw119@naver.com)
** 동국대학교 국제정보대학원 정보보호학과(jshag90@naver.com)

이드 어플리케이션 마켓)‘에 판매 중인 어플리케이션들에 대해서 분석한다. 분석에 대한 범위는 잠금 기능 관련, 위치 기반 관련, 잠금 및 위치 기반 관련 어플리케이션이다. 분석을 통하여 본 지에서 제안하고자 하는 시스템과 유사한 기존의 어플리케이션들의 현황을 파악해 본다.

2.1. 잠금 기능 관련 어플리케이션

‘Smart App Protector’ 어플리케이션은 모바일 장치에 설치된 어플리케이션에 대해서 비밀번호나 패턴으로 잠금을 수행하여 사용자가 잠금을 지정한 어플리케이션에 대해서 실행하지 못하게 하는 어플리케이션이다. 또한 잠금 해제 실패 시에는 잠금 실패를 적용하여 접근을 실패한 사람의 얼굴을 전면 카메라 촬영을 통해 얼굴 사진을 확보해서 사용자의 이메일로 전송하는 시스템을 갖추고 있다. 추가적으로 사용자가 지정한 시간에만 어플리케이션 잠금 기능을 사용한 시간별 차등 잠금 기능이 있다.

‘사진 잠금(스마트 갤러리)’ 어플리케이션은 잠금 기능에서 멀티미디어 정보만 선별적으로 잠금 기능을 사용하여 사용자의 사진이나 동영상 등을 보호할 수 있는 기능을 갖추고 있다. 잠금 방법으로 폴더별, 파일별로 차등적으로 잠금 기능을 수행할 수 있다.

2.2. 위치 기반 관련 어플리케이션

‘딩동’이라는 어플리케이션은 위치 기반 시스템에서 사용자의 위치에 따른 주변 매장들의 e-쿠폰을 ‘딩동몰‘에서 할인 구매할 수 있다. 또한 사용자가 위치한 주변의 제휴된 매장들의 정보를 지도와 리스트로 확인하여 사용자가 매장 정보를 조회 시에 포인트가 적립되고 이를 ‘딩동몰’이라는 어플리케이션 자체 상점을 통하여 상품권이나 할인 쿠폰 등을 구매하여 사용할 수 있다.

‘B자녀 스마트폰 관리’ 어플리케이션은 사용자 부모의 자녀에 대한 위치 정보를 확인하여 실시간으로 자녀의 위치를 확인할 수 있는 어플리케이션이다. 자녀의 위치 정보를 통하여 납치, 유괴 등의 범죄로부터 자녀를 보호할 수 있고, 긴급 상황 시에 자녀가 긴급 상황 기능을 활용하여 부모에게 현재 위치에 대한 정보를 SMS로 전송하는 방식의 안심 자녀 관리 시스템을 갖추고 있다.

2.3. 잠금 및 위치 기반 관련 어플리케이션

‘여기요’ 어플리케이션은 사용자의 모바일 장치를 분실하였을 시에, 타인의 모바일 장치로 사용자가 지정한 비밀번호와 함께 특수 문자를 전송하게 되면, 타인의 모바일 장치로 분실 장치의 위치를 전송 받게 된다. 또한 패스워드와 함께 ‘!’문자를 전송하게 되면 분실 장치에서 무음 모드 상태에서도 사이렌 알림이 약 15초간 작동하게 되고, ‘?’와 함께 패스워드를 전송하게 되면 사용자가 설정하였던 비밀번호로 분실 장치가 원격으로 잠금 기능이 활성화 되게 된다.

‘안드로이드 기기 관리자‘는 구글의 기본 어플리케이션인 안드로이드 기기 관리자이다. 사용자의 모바일 장치를 분실하였을 경우에 분실된 기기의 위치를 찾을 수 있게 해주며, 기기와 데이터를 안전하게 보호할 수 있는 어플리케이션이다. 사용자의 단말기를 분실하게 되면, 구글 웹사이트에서 사용자의 단말기에 연결된 구글 계정에 따라서 기기의 위치를 찾고, 기기의 화면 잠금 및 PIN 잠금 기능을 수행하게 된다. 또한 최후의 방법으로 모바일 장치의 모든 데이터를 초기화 할 수 있는 기능을 제공한다.

2.4. 잠금 기능 관련 어플리케이션의 한계점

잠금 관련 어플리케이션들의 경우에는 어플리케이션 자체에 대한 잠금 기능 활성화라든지, 민감한 사용자의 개인정보를 보호하기 위한 수단으로서의 단순한 잠금 및 암호 설정 기능이 많다. 잠금 자체에 대한 기능을 중점으로 비밀번호 입력 방식, PIN 방식, 패턴 매칭 등 잠금 해제에 대한 방법이 다를 뿐 기본적으로 잠금 자체의 기능에 대한 잠금 방법의 차이만 존재한다.

2.5. 위치 기반 어플리케이션의 한계점

기존의 위치 기반 어플리케이션들의 경우에는 어플리케이션의 잠금과 위치(일반적으로 GPS 방식) 기반을 활용한 사용자의 위치를 파악하는 데에 중점을 두고 있다. 대표적인 사례로는 지정한 위치에서 벗어나거나, 위치 추적이 불가능해질 경우에 알림 경고를 발생시키는 등의 사용자의 위치 파악 중점의 어플리케이션들이 사용되어지고 있다. 추가적으로 위치 기반 시스템을 활용

해서 사용자가 위치한 주변의 상점에 대한 할인 쿠폰 발행이나 마켓의 새로운 정보를 알려주는 등의 정보 제공 측면에서의 활용이 많다.

Ⅲ. 제안 방법

3.1. 구동 프로세스

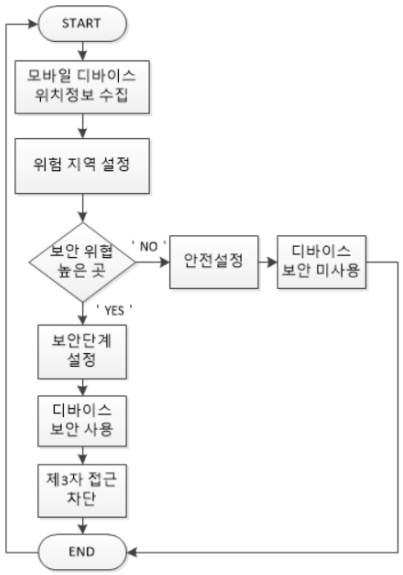
본 제안은 사용자의 모바일 장치의 위치 기반을 바탕으로 선택적으로 보안 단계를 변화시켜 모바일 장치 잠금을 수행하는 어플리케이션이다. 사용자가 모바일 장치를 통하여 위치 정보를 수집하는 방식은 다음과 같은 방식을 이용한다.

첫 번째로 장치 자체에 내장된 GPS를 이용하여 위성으로부터 좌표를 수신 받는다. 현 모바일 장치에서 가장 보편적이고 실외에서 비교적 정확한 위치 정보를 송수신 하는 방식이다. 두 번째로 Wi-Fi를 통한 무선 통신을 이용하는 방법이다. 실내에 위치한 무선 AP의 하드웨어 주소(MAC : Media Access Control)를 활용하여 통신하기 때문에 이 방법을 이용할 경우 실내에 사람이 위치할 경우에도 비교적 정확하게 위치를 파악할 수 있다는 장점이 있다. 세 번째로는 데이터 네트워크를 이용하여 모바일 장치의 위치를 파악하는 방법이다. 이 방법은 모바일 장치가 기지국(기지국 내의 GPS활용)과 데이터 통신을 통하여 기지국에서 위치 정보를 전송받는다. 이 방법은 기지국을 이용하여 위치가 알 수 있기 때문에 대략적인 사용자의 위치를 파악하게 된다.

여기서 언급하는 위치 기반은 사용자가 있는 위치의 보안 위협 정도에 따라서 보안 단계가 변화된다는 것이다. 인구 밀도가 높은 공공장소나 번화가에서는 보안 위협이 많기 때문에 위협도가 상승하게 된다. 그에 따라서 모바일 장치 자체에서 보안 단계를 상승하게끔 한다.

반면에, 사용자의 집이나 스스로 보안 위협이 낮다고 판단되는 장소에서는 장치 자체의 보안 단계를 최저로 낮추게 한다. 이후에 사용자가 해당 위치에 접근할 경우 자체적으로 보안 단계가 낮아지게 된다. 본 시스템을 적용하게 될 경우, 사용자는 기존에 장치 잠금 기능 등을 따로 해제하지 않고도 스마트폰을 이용하며 보안이 확보된 장소에서 모바일 장치를 사용하게 된다.

아래의 ‘그림 1’과 같이 본 제안의 프로세스는 최초에 사용자가 어플리케이션을 실행하게 되면 모바일 장치 위치 정보 수집 기능을 수행하면서 사용자의 현재 위치 정보를 불러온다. 이 후에 사용자의 위치 근방의 지도에서 자신이 보안 설정을 하고 싶은 곳의 지역(좌표)을 화면에서 선택하고, 안전한 지역인지 위험한 지역인지 선택하게 된다. 선택한 지역을 안전한 지역으로 설정하면, 보안 단계는 자동으로 최하 단계로 설정된다. 이후에는 안전한 지역으로 접근하게 되면 보안 암호 잠금 기능 없이 모바일 장치를 이용할 수 있게 된다.



〔그림 1〕 위치 정보 기반의 모바일 장치 보안 시스템 프로세스

이와는 반대로 선택한 지역을 위험한 지역으로 설정하게 되면 1단계에서 4단계의 모바일 장치 보안 잠금 설정을 거치게 된다. 위험 지역에 대한 사용자의 보안 단계 설정을 마친 후, 사용자가 위험 설정 지역에 접근하게 되면 암호 잠금을 해제해야지만 모바일 장치를 이용할 수 있게 된다.

추가적으로 지속적인 사용자의 위치 정보를 수신할 수 있도록 어플리케이션에서 사용자 위치 정보 수집에 대한 동의를 받아서 사용자의 위치에 따른 암호 잠금 기능이 자동으로 수행될 수 있도록 한다. 동의를 얻지 않는다면 사용자가 수동으로 위치 정보를 전송함으로써 어플리케이션을 이용하게끔 한다.

3.2. 메인 화면 구성

아래의 ‘그림 2‘는 본 제안 시스템의 어플리케이션 메인 화면이다. 최초에 어플리케이션을 실행하게 되면

〔그림 2〕 메인 화면 구성 화면

사용자 위치 정보에 대한 설정하기 메뉴가 나오게 되고, 위치 정보 수집을 허용하면 GPS, 데이터 망, Wi-Fi 순으로 사용자의 위치 정보를 수집하게 된다. 위치 정보를 바탕으로 사용자가 보안 단계를 설정하게 된다. 수집한 위치 정보를 기반으로 사용자가 위치한 곳으로 화면에 지도의 좌표를 위치시킨다. 사용자는 자신의 주변 지도를 바탕으로 위험 지역이나 안전 지역을 선택하여 지역(좌표) 별로 보안 단계를 설정할 수 있다. 추가적으로 지속적인 사용자의 위치 정보를 수신할 수 있도록 어플리케이션에서 사용자 위치 정보 수집에 대한 동의를 받아서 사용자의 위치에 따른 암호 잠금 기능이 자동으로 수행될 수 있도록 한다. 동의를 얻지 않는다면 사용자가 수동으로 위치 정보를 전송함으로써 어플리케이션을 이용하게끔 한다.

3.3. 보안 위협에 따른 모바일 장치 보안 단계 설정

보안 위협에 따른 모바일 장치 보안 단계 변화는 다음과 같다. 보안 위협이 높은 곳에서 최상의 보안 단계가 필요하다. 높은 보안 단계의 패턴, PIN번호, 얼굴/지문 인식 등의 조합을 통하여 제3자가 스마트폰에 접근할 수 없도록 하는 것이다. 반면에, 보안 위협이 적은 집이나 개인 장소에서는 높은 보안 단계가 필요 없게 된다. 오히려 사용자의 불편함을 더하게 된다. 본 제안에서는 자동으로 보안 단계가 최하위로 설정되어서 보안 기능 없이 모바일 장치를 이용하게 된다. 보안 단계

〔그림 3〕 보안 위협에 따른 모바일 장치 보안 단계 설정 화면

설정은 '그림 3'과 같이 사용자가 위험 지역인지 안전 지역인지를 등록하기 위해 잠금 설정 할 위치(좌표)를 선택한다. 총 4단계로 이루어져 있으며 단계가 높을수록 여러 요소를 조합하여 모바일 장치 보안을 강화하며 이는 다음과 같다.

매우 높음 단계에서는 패턴, PIN, 얼굴 혹은 지문 인식으로 모바일 장치 잠금 기능이 실행된다. 얼굴이나 지문 인식은 모바일 장치에 따라서 적용이 된다. 기본적으로 이 단계는 사람이 가장 많은 공공장소와 같이 보안 위협이 많이 존재하는 곳에서 동작이 되도록 한다. 보통 단계에서는 패턴, PIN을 조합하여 보안 단계를 설정한다. 기본은 매우 높음으로 설정되어 있지만 사용자가 불편함을 느낄 경우 하위 단계로도 설정이 가능하다. 약간 낮음 단계에서는 PIN 혹은 패턴과 같이 한 가지의 잠금 기능 방법으로 보안 기능을 수행한다. 매우 낮음 단계는 사용자가 안전한 지역으로 설정하면 자동으로 매우 낮음 단계로 설정 되도록 되어있다. 이 단계에서는 보안 기능 없이 자신의 모바일 장치를 사용할 수 있다.

3.4. 지역별 보안 단계 설정

보안 위협이 적은 곳은 항상 집이나 개인적인 공간만 있는 것은 아니다. 사용자가 정보 유출로부터 안전하다고 판단되는 곳에 낮은 보안 단계를 설정하도록 한다.

본 기능에서는 '그림 4'와 같이 사용자가 안전한 지역이라고 생각하는 지역을 등록하게 된다. 대표적으로 자신의 집 위치를 안전 지역이라 등록하고 시작할 수 있다. 등록한 집 주소 이외에 '그림 4'의 'Config' 메뉴를 통해 보안 위협이 적거나 안전한 지역 혹은 위치 정보를 등록할 수 있다. 예를 들어 학교와 같은 보안 위협이 많은 곳은 안전하지 않은 곳이기 때문에 지도에서

〔그림 4〕 지역별 보안 단계 설정 화면

학교를 선택을 하고 ‘unsafe’를 선택을 하면 단계 별로 보안 단계를 설정할 수 있고, ‘safe’이면 추가적인 보안 단계 설정 없이 보안 기능을 비활성화 시킨다.

3.5. 사용자 지정 지역 잠금 설정

사용자가 이미 지정한 장소별 잠금 보안 설정을 수정할 수 있는 화면이다. ‘그림 4’와 같이 메인 페이지에서 ‘Config’ 버튼을 선택하면 ‘그림 5’ 화면처럼 사용자가 지정하였던 장소들의 목록이 나오게 된다. 기존에 보안 단계를 설정하였던 장소들을 선택하면 안전 지역인 ‘매우 낮음’ 단계부터 위험 지역인 1단계에서 4단계의 보안 단계를 재설정할 수 있다. 재설정 이후에는 ‘Back’ 버튼을 통해서 초기 화면으로 되돌아 갈 수 있다.

〔그림 5〕 사용자 지정 지역 잠금 설정 화면

3.6. 구동 예시 시나리오

보안 단계 적용 시를 가정했을 때, 사용자는 사람이 많은 공공장소나 인원이 많은 장소에 위치하게 된다. 사용자의 모바일 장치에는 본 제안의 어플리케이션이 설치되어 있어서 사용자가 서비스를 실행함과 동시에 사용자의 위치 정보를 GPS, Wi-Fi, 데이터 망 등을 이용해서 수집한다. 보안 위험 지역에 근접하였을 때, 어플리케이션에 사용자가 미리 설정한 보안 위협 데이터베이스를 바탕으로 사용자가 위치한 곳이 보안 위협이 있다고 판단한 후에, 사용자의 모바일 장치 보안 단계를 자동으로 매우 높음 단계로 설정하게 된다. 이에 따라 매우 높음 보안 단계가 설정된 모바일 장치를 분실하더라도 모바일 장치의 보안 수준이 매우 높음 단계이므로 패턴, PIN, 얼굴 및 지문 인식 과정을 거쳐야만 모바일 장치를 사용할 수 있게 되고 결국 제3자가 사용자의 모바일 장치에 접근하기 어렵게 된다. 만약 사용자가 보안 위협이 많은 곳에서 매우 높음 단계의 사용의 불편하다고 느끼면 보안 단계 설정 메뉴를 통하여 임의로 단계 설정을 변경할 수 있도록 하였다.

보안 단계 미적용 시를 가정한다. 사용자는 항상 보안 위협이 거의 없는 자신의 집으로 이동한다. 이 경우에도 사용자의 모바일 장치가 위치 정보를 수집하게 된다. 사용자가 위치한 곳은 사용자의 집으로, 사전에 사용자가 집을 안전 지역으로 설정한 곳이다. 그에 따라서 모바일 장치의 보안 단계는 매우 낮음 단계로 자동 전환되고 스마트폰의 모든 잠금 기능도 해제 된다. 사용자는 사람이 없고, 보안 위협이 없는 장소에서 편안하게 자신의 모바일 장치를 사용할 수 있게 된다. ‘그림 4’와 같이 안전 지역 등록 메뉴를 통하여 사용자는 자신의 집뿐만 아니라 자신이 안전 지역이라고 생각하는 지역을 어플리케이션 서비스에 등록하여 사용자의 집에 적용한 보안 수준과 동일한 수준으로 적용시킬 수 있다. 사용자가 안전 지역으로 등록한 곳을 방문할 경우 자동으로 최하 보안 단계 설정이 적용된다.

Ⅵ. 결론 및 기대효과

최근에 발생하는 정보보호 관련 사고들을 살펴보면 많은 수의 공격들이 모바일 장치를 목표로 하는 공격들

이 많아지고 있는 추세이다. 이러한 추세에 따라 정보보호 및 암호화에 대한 이슈들이 커지고 관련 산업과 기술들이 발전하고 있다. 이에 따라 본 지에서는 사용자 모바일 장치의 잠금 기능을 활용한 새로운 시스템을 제안한다.

본 제안에서 언급하는 모바일 어플리케이션은 위치 정보를 활용하여 모바일 잠금 기능을 설정한다. 모바일 장치의 GPS, Wi-Fi, 데이터 네트워크 등을 활용하여 위치 기반으로 모바일 장치 잠금 수준을 설정한다. 본 어플리케이션을 통하여 보다 편리하고 효율적인 정보보호 시스템을 구축할 수 있고, 다음과 같은 기대 효과를 예상할 수 있다.

첫째로, 일반적으로 모바일 장치 사용자들의 경우에는 자신의 모바일 장치를 보호하기 위해, 비밀번호, PIN, 패턴 잠금, 지문 인식 중 한 가지 잠금 기능을 활용한다. 또한 장소와 상관없이 설정된 기능을 지속적으로 사용해야 한다. 하지만, 본 제안은 위치 정보 기반의 잠금 시스템이므로 위치에 따라 유연하게 잠금 단계를 변경 및 제어할 수 있다.

둘째로, 효율적인 모바일 장치의 보안 기능 향상 측면이 있다. 공공장소이거나 집단이 모여 있는 장소에서는 자신의 모바일 장치가 타인에게 쉽게 노출되어 보안 위협에 취약하다. 이에 따라 본 제안 시스템을 활용하면 사용자가 지정한 보안 위협 수준에 따라서 보안 단계가 설정되기 때문에 보다 효율적으로 향상된 보안 기능이 적용된다.

마지막으로, 향상된 보안 기능을 바탕으로 편의성 향상 측면이 있다. 위치 기반으로 보안 단계가 변경되기 때문에 사용자의 가정과 같은 안전한 장소에서는 보안 단계가 최하로 설정된다. 일반적으로 급하게 모바일 장치를 사용할 상황에서 장치 잠금 기능으로 인한 불편함을 느끼고 있다. 그렇지만 본 제안에 따르면 정보 유출의 위험에서 벗어난 안전한 장소에서는 보안 기능 없이 자신의 모바일 장치에 접근이 가능하다. 본 제안은 이러한 불편함을 해소해서 향상된 보안성을 바탕으로 높은 편의성을 제공한다.

본 제안인 '위치 정보 기반의 사용자 모바일 장치 잠금' 기능을 활용한다면 위치 별로 사용자가 지정한 보안 단계에 따라서 모바일 장치가 유동적으로 사용자의 모바일 장치 잠금을 수행하게 된다. 결론적으로 잠금 기능을 기반으로 모바일 장치 정보보호의 효율성, 편의성, 보안성의 극대화를 기대할 수 있는 시스템이다.

참 고 문 헌

[1] Swapnil Waghmare, Madhumita Chatterjee, Satish L. Varma, "Authentication System for Android Smartphones", International Journal of Computer Applications, February 2014.

[2] Serge Egelman, Sakshi jain, Rebecca S.Portnoff, "Understanding User Motivations for Smartphone Locking Behaviors", University of California, International Computer Science Institute Berkeley, Google, Inc.Mountain View, November 2014.

[3] 안드로이드 2.3 프로그래밍, 위키북스, 이준호

[4] 김현홍, "스마트폰 환경에서 위치정보를 이용한 사용자 인증 기법 설계 및 구현", 숭실대학교 대학원 학위논문, December 2012.

[5] 위치 기반 서비스를 이용한 스마트폰 관광 정보 시스템, 멀티미디어 학회 논문지, 김석현, 김지욱, 김현정, 박동규

〈저 자 소 개〉

박 재 혁 (Jae-Hyeok Park)
학생회원

2014년 2월 : 고려대학교 경영정보학과 졸업
2014년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : MIS, 정보기술관리, 정보보호전략, 모바일보안

지 선 학 (Seon-Hak Ji)
학생회원

2015년 2월 : 강원대학교 정보통신공학과 졸업
2015년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 모바일보안, S/W보안, 악성코드