스마트폰 보안 기술 동향

장기헌*□이상래□염흥열**

순천향대학교 정보보호학과

목 차

Ⅰ. 서 론

스마트폰(Smartphone)은 PC와 같은 기능을 더불어 고급 기능을 제공하는 휴대 전화이다[1]. 스마트폰은 다양한 인터페이스 및 기능 등 기존 휴대폰과는 차별화된 장점을 내세워 그 인기가 높아지고 있으며, 사용자의 취향에 따라 어플리케이션의 설치 및 삭제가 가능하다. 최근에는 하나의 콘텐츠를 여러 개의 스크린으로 사용할 수 있는 엔스크린(N-Screen)서비스와 업무를 처리하기 위해 사용되는 스마트오피스가 주목을 받고 있다.

또한 스마트폰에서 이용할 수 있는 어플리케이션의 수와 종류가 급속이 증가하고 있다. iPhone에서 서비스 하고 있는 앱 스토어의 경우 20만 가지 이상의 앱(APP : Application)이 등록되어 있다[2]. Android 마켓의 경우 2010년 11월 28일 기준 17만 가지 이상의 어플리케이션이 등록되어 있으며, 22억6천회 이상의 다운로드가 집계되었다[3]. 이러한 어플리케이션은 사용자에게 새로운 기능 및 서비스를 제공하며, 사용자는 등록된 어플리케이션 중 필요한 어플리케이션을 다운로드받아 사용 할 수 있다 [그림 1]. 그 중 스마트폰을 이용한 뱅킹 서비스를 이용하기 위해 스마트폰뱅킹(모바일뱅킹) 어플리케이션의 사용자가 늘고 있는 추세이다.

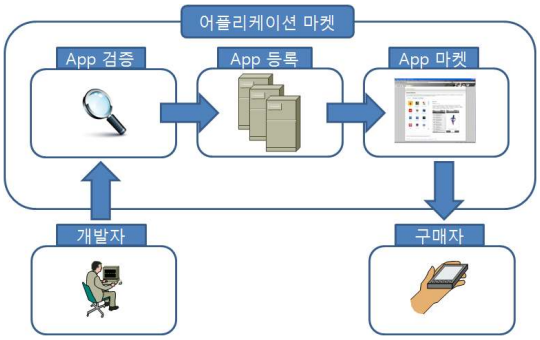

그림 1. 어플리케이션 유통 과정

이 외 에도, GPS를 통한 네비게이션 서비스, 사진을 통한 위치 확인, 재생되는 음악을 통한 음악 검색서비스 등 다양한 어플리케이션이 존재한다.

하지만 스마트폰의 사용이 모두 이로운 것만은 아니다. 스마트폰은 "하나의 작은 PC"라고 불릴정도로 성능이 높아졌으며, 기능이 다양하기 때문에 기존 PC에서 발생하던 보안 위협이 스마트폰에서도 동일하게 발생할 수 있다. 최근 보고된 대표적인 스마트폰 악성코드는 광고 메세지로 위장하여 심비안 스마트폰을 공격하는 중국발 악성코드가 있으며, 이러한 악성코드가 스마트폰에 감염되면 스마트폰 내에 저장되어 있는 전화번호부(주소록)를 통해 공격지를 선정하고 다시 전파를 하여 다른 스마트폰에 감염된다. 요금을 부과 시키거나 개인정보를 탈취하는 등의 동작을 하는 악성코드도 존재하며 이로 발생되는 문제의 심각성이 더해지고 있다.

얼마 전 어플리케이션 스토어에 등록되었던 "오빠믿지" 어플리케이션의 경우 SMS를 통해 상대 위치 정보가 노출되어 개인 프라이버시 침해 논란을 일으켰다.

이처럼 다양한 기능을 제공하는 스마트폰은 양면의 칼날처럼 사용자의 프라이버시와 보안을 위협하고 있다.

이에 따라 본 고에서는 스마트폰의 위협을 분석하고, 이를 방어할 수 있는 보안 기술을 알아본다. 2장에서는 스마트폰의 주요 위협을 살펴보고, 3장에서 이에 대한 보안

기술 동향을 알아본 후 글을 맺는다.

Ⅱ. 스마트폰 위협

보안 위협은 각각의 영역별로 다양한 위협이 발생될 수 있지만[4], 본 장에서는 스마트폰을 사용하면서 발생 할 수 있는 주요 위협에 대해 간단히 살펴본다[표 2].

2.1 악성코드

스마트폰에서 악성코드가 발생하는 이유는 표1과 같다.

표 1. 악성코드 발생 이유

	내용
악성코드 발생 이유	음성 및 인터넷 통신 가능
	초고속 무선 데이터 통신사용
	Wi-Fi, Wibro 등의 액세스 확대
	무선 브라우징 확대
	휴대폰 기기의 성능 향상
	휴대폰의 개인화 및 전자 결제 지원
	공개 플랫폼화

이러한 발생 이유들은 악성코드의 전파 확대를 가속화 시키는 주요 원인으로 작동하고 있다.

스마트폰에 악성코드가 감염되면, 감염된 스마트폰을 원격으로 제어하거나, 파일 실행 차단, 어플리케이션의 동작을 변경하여 악의적인 행동을 할 수 있으며, 불필요한 통신요금을 발생, 스마트폰에 저장된 사용자의 자료 유출 및 SMS 훔쳐보기 등의 리스크를 초래한다.

또한 스마트폰에 GPS 기능이 추가되면서 위치 추적이 가능해 졌다. 악성 코드에 의한 위치 추적으로 인해 사용자의 개인 프라이버시 침해 논란이 발생하고 있으며, 이에 대한 대응책이 필요하다.

2.2 분실 및 도난

스마트폰에서 이용할 수 있는 서비스가 다양해 지면서, 저장되는 정보의 종류와 양도 많이 지고 있다. 특히 모바일 뱅킹을 이용하기 위해 사용되는 공인인증서, 기업 기밀 정보를 담고 있는 중요 문서, 스마트폰에 저장된 사용자의 전화번호부 등의 자료는 외부로 유출 시 피싱, 주요 정보 노출, 신분도용 등의 피해로 이어질 수 있기 때문에 보안이 필요성이 높아지고 있다. 또한 대부분의 스마트폰 사용자들이 메신저, E-mail등의 서비스를 이용할 때 계정정보를 저장하여 사용하고 있는 점도 위협으로 작용할 수 있다.

주니퍼네트웍스가 KRC리서치와 시노베이트(Synovate)에 의뢰해 전세계 13개국 4,500명 이상의 스마트폰 및 테블릿 PC사용자를 대상으로 모바일 보안 인식에 대한 조사를 실시한 결과 폰/데이터 분실 및 신분도용이 가장 높은 비율을 보였다[7].

이러한 정보가 노출될 가능성이 가장 높은 위협은 분실 및 도난에 의한 노출이다. 사용자의 스마트폰이 분실 및 도난 되었다면, 이를 습득한 제 3자는 스마트폰 내부의 자료를 열람할 수 있으며, 저장되어 있는 계정정보를 이용하여 메신저, E-mail등을 열람할 수 있다.

2.3 앱 스토어를 통한 악성코드 유포

1장에서 언급하였듯이 앱 스토어는 빠르게 성장하고 있으며, 거대한 규모를 자랑한다. 이러한 앱 스토어는 앱의 개발, 유통 및 거래 중개를 통해 새로운 가치를 창출하는 수익 창출의 기회를 제공할 뿐만 아니라 위협요인을 동시에 제공 할 것으로 예상된다[5].

앱 스토어에 등록되는 어플리케이션이 악의적인 사용자에 의해 만들어져 배포될 경우 2.1절에서 언급한 피해가 발생할 수 있다.

표 2. 주요 위협 정리[4]

구분	위협
악성코드	원격제어, 파일 실행 차단, 어플리케이션 변조, 불필요한 요금 발생, 저장된 자료 유출, SMS 노출 등
분실 및 도난	저장된 자료 유출, 저장된 계정정보를 사용한 서비스 이용, 개인정보 노출
앱 스토어 악성코드 유포	악성코드 유포지로 이용가능
모바일 오피스 환경에서 기업정보 유출	기업 정보 유출
기타	WEB SITE를 통한 피싱, 어플리케이션 취약점을 이용한 악용, 데이터 스니핑 및 변조, 음성 도청, GPS위치 정보 노출, 외장 메모리를 이용한 악성코드 전파 등

2.4 모바일 오피스 환경에서의 기업정보유출

스마트폰이 확산되면서 모바일 오피스를 통한 업무 환경이 도입되고 있다. 하지만 스마트폰은 때와 장소를 가리지 않고 기업내부 정보에 접속할 수 있기 때문에 내부 정보 유출위협이 존재한다. 기업 내부 정보가 외부로 유출 될 경우 해당 기업은 큰 손해를 보게 될 것이며 이에 대한 보안 대책이 필요하다.

Ⅲ. 보안 기술 동향

스마트폰 OS는 표 3과 같이 다양한 종류가 존재하며, 다양한 보안 기능을 제공한다[4]. 하지만 이러한 보안 기능만으로는 완벽한 보안을 제공할 수 없기 때문에 추가적인 보안 기술이 필요하다[표 4]. 본 장에서는 스마트폰 보안과 관련하여 보안 강화를 위한 기술에 대해서 알아본다.

표 3. 스마트폰 OS의 종류

구분	내용
비 리눅스 기반	심비안, 윈도우 모바일, 블랙베리 OS, 아이폰 OS
리눅스 기반	Qtopia, 리모, 마에모, 모블린, 미고, 안드로이드

3.1 악성코드 보안 기술

악성코드에 대응하기 위해서는 안티바이러스 솔루션이 필요하다. 국내에서는 안철수 연구소, 하우리, NSHC 등에서 백신을 개발 하고 있으며 해외에서는 Kaspersky, McAfee, SMobile Security 등에서 개발하여 사용하고 있다. 표 3과 같이 스마트폰에 사용되는 OS의 종류는 다양하지만 아직까지 모든 스마트폰 OS에서 동작하는 안티 바이러스 솔루션은 찾기 힘든 것이 현실이다. 주로 사용자가 많이 사용하고 있는 Windows mobile, 심비안, 안드로이드, 심비안 등에서 지원하고 있으며, 스마트폰의 성능이 PC보다 현저히 떨어지기 때문에 기존의 PC 안티 바이러스 솔루션 보다 기능이 제한적이며, 경량화하여 사용하고 있다. 이러한 안티 바이러스 솔루션들은 실시간으로 파일 과 프로세스에 대한 감시를 제공하며, 악성코드를 탐지하고 차단한다. 3G, Wi-Fi등의 다양한 네트워크를 이용하여 엔진 업데이트가 가능하며 사용자가 사용하고 있는 외장 메모리 영역까지 검사가 가능하다.

일부 업체에서는 안티바이러스 솔루션에 분실 및 도난 방지 기술까지 포함하여 제공하고 있으며, 위험한 네트워크 접근을 차단하는 기능을 포함하고 있다.

3.2 분실 및 도난 방지 기술

분실 및 도난으로 발생되는 문제의 중요성이 부각되면서 이에 대한 보안 기술들이 개발되고 있다.

통신사에서 제공하는 보안 기술의 경우 스마트폰

표 4. 스마트폰 보안기술

보안 기술	내용
악성코드 보안기술	안티 바이러스 솔루션을 이용한 보호
분실 및 도난 방지기술	통신사 및 보안 솔루션 업체에서 제공하는 스마트폰 원격 제어 솔루션
앱스토어 보안기술	코드 사이닝을 통한 게시자 신원확인 및 등록된 어플리케이션의 위변조 방지
모바일 VPN	모바일 오피스 환경에서 종단간 기밀성, 무결성, 데이터 인증성을 제공하는 보안 터널 제공
위치정보보호기술	위치서버에서 수행하는 사용자 프로파일 관리, 인증 및 보안, 접근통제 등
모바일 가상화기술	모바일 가상화를 통한 안전한 실행환경 제공
스마트폰 단말보안기술	MTM을 이용하여 외부 공격으로부터 개인정보및 중요정보를 보호[8]
개인정보보호기술	DLP를 이용한 정보 유출 방지
가상키보드 보안기술	카상키보드의 패널 위치 변경 및 전달되는 입력정보를 암호화

분실 시 분실 신고가 접수되면, 원격으로 모든 스마트폰 OS에 대한 공장 초기화, 프린트 스크린 차단, 카메라 차단 등을 할 수 있다. 공장 초기화 기능이란 분실 및 도난 된 스마트폰의 저장된 모든 데이터 및 정보를 원격에서 삭제할 수 있으며, 공장에서 출하 당시의 상태로 만드는 것을 말한다. 카메라로 촬영을 할 수 없도록 하는 카메라 차단 기능과 스마트폰에 저장된 정보를 그림파일로 저장할 수 없게 하는 프린트 스크린 차단 기능이 통신사에서 제공하는 주 보안 기술이다.
보안 솔루션 업체에서 제공하는 보안 어플리케이션의 경우 종류는 다양하지만 제공하는 기능은 원격 데이터 삭제 기능과 SIM카드 보호 기능 등으로 유사하다. 원격으로 데이터를 삭제하거나 SIM카드를 암호로 보호하며, GPS를 통하여 분실된 스마트폰이 어디에 위치하고 있는지 확인이 가능하다.

3.3 앱스토어 보안 기술

앱스토어에는 사용자가 만든 어플리케이션을 업로드하고 이를 필요한 사용자가 다운로드하는 두 가지 경우가 존재하며 크게 두가지 위협이 존재한다. 하나는 게시자의 신원을 도용하는 것이고, 다른 하나는 등록된 어플리케이션의 위변조 방지와 데이터 발신지 확인이다. 이를 막기 위해 전자서명 기법 기반의 코드 사이닝 (Code Signing)을 사용하고 있다. 코드 사이닝을 위해서는 인증서가 필요하며[11-13], 사용되는 인증서는 ITU-T권고 X.509에 기반을 두고 있다[12]. 코드사인에 사용되는 인증서 발급기관으로는 Verisign(국외), 금융결제원(국내) 등이 있다.

3.4 모바일 VPN 기술

모바일 VPN은 모바일 사용자의 증가로 인한 데이터 통신에 대한 보안 요구사항의 증가와 데이터 통신의 보안을 향상할 수 있는 수단으로써 사용된다. 모바일 VPN을 사용함으로써, 네트워크 접속을 위한 끈김 없는 이동성을 보장할 수 있으며, 보안성을 보장하는 통신채널을 제공할 수 있다[그림 2]. 현재 대부분의 VPN은 IPsec기반 VPN으로 site-to-site 연결에 적합하다.

Nokia에서 제공하는 Mobile VPN의 경우 AES와 AKA 등을 사용하고 있으며, Certificate file의 format은 X509.3 ASN.1 format을 사용하고 있다[17].

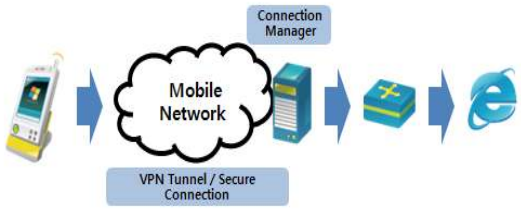

그림 2. Mobile VPN

3.5 위치정보보호 기술

스마트폰 위치 기반 서비스(Location-Based Service)는 위치 정보를 통한 응용 시스템 및 서비스를 스마트폰과 융합하여 다양한 서비스를 제공하고 있다[그림 3]. GPS 위성신호뿐만 아니라 Wi-Fi AP, 3G 기지국 ID 순으로 위치정보를 제공하여 GPS 기반 위치측위로 해결할 수 없는 도심과 실내 측위에 대해서 WLAN 기반 측위를 사용이 가능하게 하고 있다[14].

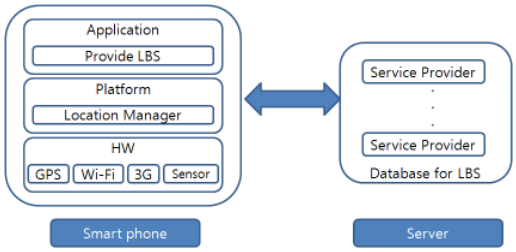

그림 3. LBS 구성 요소

하지만 개인의 위치가 실시간으로 노출될 경우 사생활 노출로 인한 프라이버시 문제 및 범죄 등에 악용될 수 있다. 위치 기반 서비스의 메시지 도청, 변조, 위조 등의 위협이 있으며 이를 위한 보안 요구사항은 표 5와 같다[15].

표 5. 위협별 보안 요구사항

보안 서비스	위협요소
기밀성	메시지 도청
무결성	메시지 변조
인증	메시지 위조
부인방지	메시지 송신 및 수신 부인
접근제어	불법적 서비스 및 정보 이용

이를 위해 위치서버(location server)는 위치 획득 서버로부터 위치를 획득하여 요청에 응답, 정보처리, 경로 추적 등의 위치중심의 처리기능을 수행해야할 뿐만 아니라 사용자 프로파일 관리, 인증 및 보안, 타사업자와의 위치정보 제공 연계, 망부하 관리, 다양한 사용의 접근통제, 통계관리 등 통신망과 연계된 기능을 수행한다[16].

3.6 모바일 가상화 기술

모바일 가상화 기술이란 실제 하드웨어 시스템은 하나이지만 가상으로 여러 가지의 가상 시스템을 제공하는 기술로써 VMWare, VirtualBox 등이 있다.

모바일 가상화 기술의 필요성은 표 6과 같다.

표 6. 모바일 가상화 기술의 필요성

구분	내용
앱 스토어	현재 사용되고 있는 각 회사별 앱스토어에는 다양한 어플리케이션이 등록되어 있지만, 이들은 스마트폰 OS별 구분이 확실히 정해져 있음 이러한 어플리케이션을 단일 스마트폰에서 동시에 구동이 가능해 짐
용도	단일 스마트폰에 여러 가지 환경을 구성하고 용도에 맞게 사용할 수 있음
보안	안전한 실행환경을 제공할 수 있음. 가상화 기능을 이용하여 사용상의 제약을 사전에 정의할 수 있음
대체	스마트폰용 도킹 스테이션을 이용하여 스마트폰에서 PC OS를 부팅해서 사용할 수 있으며, 가상화로 스마트폰 OS 역시 구동중이기 때문에 사용 중 전화도 받을 수 있음.

이러한 가상화 기술은 안전한 실행 환경을 제공할 수 있기 때문에 보안 분야에서 주목을 받고 있다[그림 4]. 예를 들면, 사용자의 정보(전화번호부 등)를 담고 있거나 중요한 어플리케이션들이 사용자가 설치한 어플리케이션이 실행되는 환경과 다르게 하고 공격을 받더라도 보안 정책이 높은 전자에는 피해가 없도록 하는 것이 가능하다[그림 5].

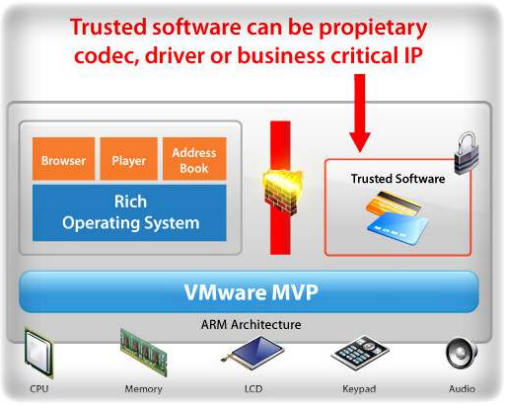

그림 4. 모바일 가상화를 통한 보안 이미지[6]

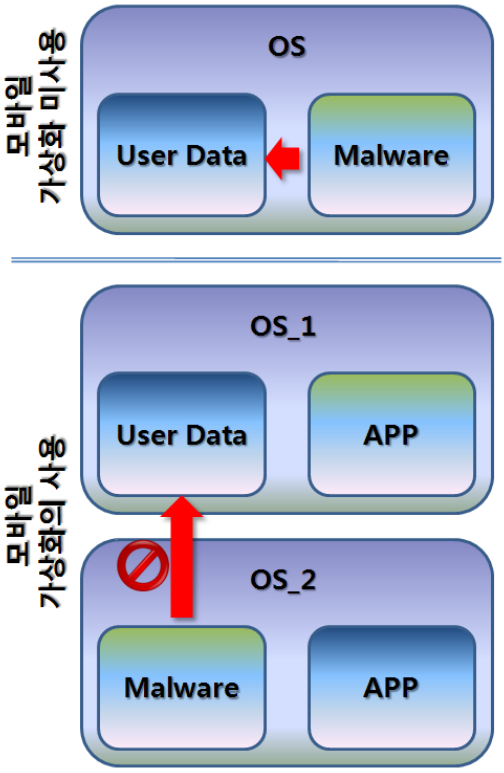

그림 5. 모바일 가상화를 통한 보안

3.7 스마트폰 단말 보안 기술

물리적 보안성을 제공해 주는 MTM (Mobile Trusted Mobile)을 이용하여 외부 공격으로부터 개인정보 및 중요 정보를 안전하게 보호할 수 있으며, 스마트폰 단말 플랫폼의 무결성 검증을 통해 악성코드의 실행을 사전에 탐지하며 이를 차단할 수 있다[8].
Root of trust 기능을 제공해주는 MTM은 tamper-resistant 컴퍼넌트로써 데이터를 안전하게 저장하는 RTS, 시스템 상태를 신뢰할 수 있는 방법으로 증명하는 RTR역활을 담당하며, 시스템의 상태를 PCR에 기록하는 RTM의 역할은 CRTM이 담당한다[8]. CRTM은 power-on시에 가장 먼저 실행되고, 항상 신뢰할 수 있는 컴포넌트로 PC의 경우 BIOS에 포함될 수 있으며, 임의로 수정할 수 없는 특징을 갖는다[8].

3.8 개인정보보호기술

스마트폰에는 다양한 개인정보가 저장되어 있고, 이러한 개인정보 유출 사건이 지속적으로 발생하면서 이를 안전하게 관리하는 것이 무엇보다 중요해 지고 있다.

개인정보유출은 외부에 의한 유출과 내부에서 발생하는 유출로 나뉘는데, 대부분의 정보 유출은 내부인에 의해 발생한다. 산업기밀보호센터에 따르면 정보유출의 약 80%가 내부자에 의해 발생한 것으로 조사 되었다[10].

2010년 11월 29일부터 30일까지 열린 ISEC2010에서 개인정보 유출 방지에 가장 효과적인 기술로 DLP (Data Loss Prevention)가 소개되었다[9].

DLP란 정보가 외부로 유출되는 것을 방지해주는 솔루션으로 접근제어 및 필터링, 사전 탐지 와 사후 분석이 가능하다. DLP는 스마트폰 단말기를 이용한 유출 방지 기술에도 사용될 수 있기 때문에 활용도가 높다. 다만, DLP 가 스마트폰에 설치된다면, 스마트폰 성능에 영향을 줄 가능성이 있어서 경량화된 DLP 솔루션 개발이 요구된다.

3.9 스마트폰 키보드 보안 기술

스마트폰 키보드 보안 기술이란 스마트폰 입력장치를 통해 입력되는 정보를 후킹을 통해 빼내 볼 수 있는데, 이를 방지하는 기술을 말한다. 특히 스마트폰의 경우 버튼 입력 방식이 아닌 터치 방식의 입력으로 이루어지기 때문에 기존 PC와는 다른, 스마트폰 OS상에서만 존재할 수 있는 후킹이 발생할 수 있다. 이러한 위협으로부터 보호하기 위해 가상키보드의 패널 위치를 변경하거나, 전달되는 입력정보를 암호화 하여 통신한다.

현재 대표적이 기술로는 소프트씨큐리티에서 상용화한 터치 보안솔루션이 있다.

Ⅳ. 결 론

본 고 에서는 스마트폰 위협을 보안할 수 있는 보안기술에 대해 알아보았다.

사용자가 많아지고 서비스가 다양해질수록 발생되는 위협은 더욱 많아질 것이며, 발전하는 해킹 기술은 스마트폰 사용자들에게 커다란 위협이 될 것이다. 안전한 스마트폰 사용 환경을 조성하기 위해 스마트폰 보안기술은 꾸준히 연구 개발 되어야 할 것이며, 지속적인 관심이 필요하다.

더불어 스마트폰 사용자들 또한 스스로 보안에 관심을 가지고 대처해야 할 것이다.

참고문헌

[1] http://ko.wikipedia.org/
[2] http://www.apple.com/kr/iphone/features/app-store.html
[3] http://www.androlib.com/appstats.aspx
[4] 장기헌, 염흥열, '스마트폰 침입 경로 및 위협 분석', 한국정보보호학회 추계학술발표대회, pp 238-244, 2010년 10월
[5] 정보통신산업진흥원, '앱스토어 현황분석'
[6] http://www.vmware.com/
[7] http://www.juniper.net/
[8] 강동호 외 6, '스마트폰 보안 위협 및 대응 기술', 전자통신동향분석 제 25권 3호, 20010년 6월
[9] http://www.isec.co.kr/
[10] http://service4.nis.go.kr/servlet/page/
[11] Microsoft, http://msdn.microsoft.com/en-us/library/

ms537361.aspx
[12] Apple, http://developer.apple.com/, 'code sihning guide', Oct 2009.
[13] Google Android, http://developer.android.com/guide/publishing/app- signing.html
[14] 정구민, '스마트폰 위치기반 서비스(LBS) 기술 동향', TTA Journal No. 130 표준기술동향
[15] 박남제 외 2명, '안전한 위치기반 서비스 제공을 위한 인증 및 보안 적용 방안', 정보보호학회, 2004년 6월
[16] 위치기반서비스 기술 동향, 전자통신동향분석 제20권 제3호, 2005년 6월
[17] 'Nokia_Mobile_VPN_Policy_Specitication', Nokia

저자소개

장기헌(Ki-hun, JANG)

2010년 2월 순천향대학교 정보보호학과 졸업
2010년 9월~현재 순천향대학교 정보보호학과 석사과정
2009년 4월~2010년 5월 SK인포섹모의해킹팀
※ 관심분야 : 정보보호, 모바일 보안, 네트워크 프로토콜

이상래(Sang-Rae LEE)

2010년 2월 순천향대학교 정보보호학과 졸업
2010년 3월~현재 순천향대학교 정보보호학과 석사과정
※ 관심분야 : 정보보호, 클라우드 컴퓨팅 보안, IPTV, 역추적

염흥열(Heung-Youl YOUM)

1981년 2월 한양대학교 전자공학과 학사 졸업
1983년 9월 한양대학교 대학원 전자공학과 석사 졸업
1990년 2월 한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월 한국전자통신연구소 선임연구원
1990년 9월~현재 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장(역), 수석부회장(현)
2005년~2008년 ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월 정보통신연구진흥원 정보보호전문위원
2009년 5월~현재 국정원 암호검증위원회 위원
2009년~현재 ITU-T SG17 부의장/SG17 WP2 의장
※관심분야 : 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜