韓國컴퓨터情報學會 論文誌
第16卷 第2號, 2011. 2.

2011-16-2-3-7

스마트폰 보안위협과 대응기술 분석

전 웅 렬*, 김 지 연*, 이 영 숙**, 원 동 호*

Analysis of Threats and Countermeasures on Mobile Smartphone

Woongryul Jeon*, Jeeyeon Kim*, Youngsook Lee**, Dongho Won*

요 약

스마트폰은 일반폰보다 진보한 성능을 지닌, PC와 유사한 기능의 모바일 단말을 의미한다. 최근 아이폰 및 안드로이드폰의 성장을 바탕으로 세계적으로 모바일 시장에서 시장 점유율이 급격히 증가하고 있는 추세이며, 국내 역시 2010년을 기점으로 스마트폰이 본격적으로 활성화 될 것으로 기대된다. 스마트폰은 휴대폰의 통화 및 메시지 기능 뿐만 아니라 강력한 컴퓨팅 성능을 바탕으로 이메일, 일정관리, 문서작업, 게임 등 다양한 서비스를 제공한다. 또, 서비스를 제공하기 위해 스마트폰은 무선네트워크를 통해 정보를 외부로 전송되기도 한다. 이를 위해 스마트폰은 다양한 정보를 집적하여 저장하고 있다. 스마트폰은 분실이 쉬운 휴대폰의 특성을 그대로 지니고 있기 때문에 분실할 경우에 대비한 내부에 저장된 정보의 보안이 매우 중요하다. 또 무선네트워크를 통해 전송되는 정보의 보안도 중요하다. 현재 스마트폰의 보안과 관련하여 다양한 분야에서 연구가 진행되고 있다. 그러나 스마트폰의 위협이 무엇인지, 대응하는 방법은 또 무엇인지 아직 명확하게 정의되지 않아 안전한 스마트폰 활용이 어렵다. 본 논문은 스마트폰의 사용환경 분석을 통해 스마트폰에 존재하는 다양한 위협들을 도출하고 대응기술을 설명한다. 본 논문의 연구결과는 향후 이어질 스마트폰의 다양한 보안기술 연구 및 스마트폰 보안기준 마련 등에 활용될 수 있을 것이다.

▸ Keyword : 스마트폰, 스마트폰 위협, 보안, 위협 대응기술

Abstract

Smartphone is a mobile device which can perform better than feature phone. Recently, growth in demand for advanced mobile devices boasting powerful performance, market share of smartphone is increasing rapidly in mobile device market, for example, iphone and android phone. Smartphone can provide many functionalities, e-mail, scheduler, word-processing, 3D-game, and etc, based on its powerful performance. Thus, various secret information is integrated in smartphone. To provide service, sometimes, smartphone transmits informations to outside via wireless network. Because smartphone is a mobile device, user can lose his/her smartphone, easily, and losing smartphone can cause serious security threats, because of integrated information in

• 제1저자 : 전웅렬 교신저자 : 원동호
• 투고일 : 2010. 08. 21, 심사일 : 2010. 09. 16, 게재확정일 : 2010. 09. 29.
* 성균관대학교 정보통신공학부(Sungkyunkwan University)
** 호원대학교 사이버수사경찰학부(Howon University)
※ 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2010-0011279).

smartphone. Also data which is transmitted in wireless network can be protected for privacy. Thus, in present, it is very important to keep secure smartphone. In this paper, we analyze threats and vulnerabilities of smartphone based on its environments and describe countermeasures against threats and vulnerabilities.

▸ Keyword : Smartphone, Threats of Smartphone, Security, Countermeasure

Ⅰ. 서 론

스마트폰은 일반폰보다 진보한 성능을 지닌, PC와 유사한 기능의 모바일 단말을 의미한다. 최근 아이폰 및 안드로이드 폰의 성장을 바탕으로 세계적으로 모바일 시장에서 시장 점유율이 급격히 증가하고 있는 추세이며, 국내 역시 2010년을 기점으로 스마트폰이 본격적으로 활성화 될 것으로 기대된다.

시장조사업체 SA(Strategy Analytics)가 최근 발표한 보고서에 따르면 2009년 4분기 전 세계 스마트폰의 출하대수는 전년대비 30% 성장한 5300만대로 이에 힘입어 2009년 연간규모는 1억 7380만대로 확대되었음을 확인할 수 있다. 이는 전년 판대매수 1억 5110만대에 비해 약 15% 증가한 수치이다. 2010년 2분기 현재 스마트폰의 판매량은 예년보다 훨씬 증가한 3억 2천만대 수준으로 확장되었다.

스마트폰은 PC와 유사한 수준의 강력한 성능을 바탕으로 사용자에게 다양한 서비스를 제공할 수 있다. 기본적으로 사용자는 스마트폰을 사용하여 일반 휴대폰과 마찬가지로 음성통화, 문자메시지(SMS), 멀티미디어 메시지(MMS) 등의 기능을 사용할 수 있으며, 그 외 스마트폰의 다양한 응용 프로그램을 바탕으로 여러 가지 서비스를 부가적으로 사용할 수 있다. 대표적인 예로 이메일 송수신, PC와 연동한 일정관리, 오피스를 비롯한 각종 문서작업, 게임 등을 들 수 있다. 최근에는 응용 프로그램을 공유하는 앱스토어가 등장하면서 전 세계 개발자들이 사용자의 요구를 반영한 다양한 응용 프로그램을 출시하고 있으며, 그 개수는 아이폰의 경우 16만여개에 달하며, 안드로이드 역시 5만개여개에 달한다. 이처럼 다양한 응용 프로그램은 스마트폰의 활용용도를 PMP(Portable Media Player), MP3 Player, 전자사전, 지도 등으로 확장시키고 있다. 즉, 스마트폰은 다양한 모바일 기기의 융합 형태로 발전하고 있다.

다른 모바일 기기의 융합은 바꾸어 말하면, 그만큼 다양한 정보가 스마트폰에 집적된다는 것을 의미한다. 예를 들어 스마트폰으로 지도나 길찾기 기능을 사용하는 경우, 스마트폰은 GPS와 연동하여 사용자의 위치정보를 사용한다. 체력관리 프로그램을 통해 운동을 하는 경우 스마트폰은 사용자가 운동한 거리, 운동방법, 사용자의 키, 사용자의 몸무게 등의 정보를 사용한다. 일정관리나 문자메시지, 통화 등의 기능은 사용자의 전화번호, 사용자의 주소록, 사용자의 개인일정 등을 저장하고 있다. 이처럼 스마트폰에는 여러 기기에 흩어져있던 다양한 개인정보들이 집적되어 있다. 특히 스마트폰은 휴대용 기기로서 분실의 우려가 높고, 통화, 문자메시지, 무선네트워크 접속 등의 서비스는 과금과 직접적으로 연결되어 있기 때문에 스마트폰의 취약성은 정보의 손실뿐만 아니라 즉각적인 금전적 피해도 야기할 수 있다.

따라서 스마트폰의 보안이 최근 중요한 이슈로 부각되고 있다. 그러나 연구동향을 살펴보면 스마트폰의 악성코드에 의한 취약성 분석, 스마트폰 플랫폼의 취약성 분석 등 단편적인 주제에 대한 연구는 활발하게 진행되고 있으나, 스마트폰의 총체적인 보안위협과 그에 대한 대응기술에 대한 정의가 명확하지 않은 실정이다. 이에 본 논문은 스마트폰의 사용환경을 중심으로 위협을 도출하고 이에 대응하는 기술을 설명한다. 본 논문의 연구결과는 스마트폰의 향후 보안기술 연구 및 스마트폰의 보안기준 개발에 활용될 수 있을 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트폰을 정의하고 스마트폰의 특징 및 시장현황에 대해 설명한다. 3장에서는 스마트폰의 자산과 사용환경을 분석하고, 스마트폰의 위협을 도출한다. 4장에서는 스마트폰의 보안목적을 정의하고, 3장에서 도출한 위협에 대한 대응기술에 대해 설명한다. 5장에서는 결론을 설명한다.

Ⅱ. 스마트폰

2.1 스마트폰 개요

스마트폰(smartphone)은 PC와 유사한 기능을 제공하는 휴대전화이다. 스마트폰에 대한 산업 표준은 아직 정의된 바 없다. 스마트폰은 응용 프로그램 개발자를 위한 표준화된 인터페이스와 플랫폼을 제공하며, 전화라는 본래의 기능을 가지고 있으며, 전자 우편, 인터넷, 전자책 읽기 기능, 내장형 키보드나 외장 USB 키보드 등 다양한 기능을 포함하고 있다.

즉 전화 기능이 있는 소형 컴퓨터를 스마트폰이라 한다. 정보통신 기술의 발달에 따라 핸드헬드 장치(hand-held device)와 휴대전화가 급속도로 확산되었으며, 이에 따라 고급 휴대기기들에 대한 수요 역시 증가하였다. 최근 출시되고 있는 휴대전화는 높은 성능의 CPU, 대용량 메모리, 넓은 화면, 개방형 운영 체제를 탑재하고 있다.

PDA를 개발하던 업체에서 이동통신 모듈을 추가하여 전화 기능이 되는 PDA폰을 시작한 것과 같이, 이동통신 단말기를 개발하던 업체에서 PDA 기능을 휴대전화 안으로 포함시켜 이를 스마트폰이라 불렀다. 대체로 PDA폰과 비슷하며, 휴대전화 기능에 부가 기능 탑재로 덩치는 큰 편이었다. 하지만 점차 PDA폰과 스마트폰의 경계가 허물어지면서 이 둘을 통칭하여 스마트폰으로 통칭하고 있다.

최초의 스마트폰은 시몬(Simon)이었다. IBM사가 1992년에 설계하여 그 해에 미국 네바다 주의 라스베이거스에서 열린 컴덱스에서 컨셉 제품으로 전시되었다.

그림 1. 최초의 스마트폰
Fig. 1. The First Smartphone

최초의 스마트폰은 휴대 전화의 기능 뿐만 아니라 계산기, 주소록, 세계 시각, 계산기, 메모장, 전자 우편, 팩스 송수신, 게임 기능까지 포함하고 있었다. 전화번호를 누르기 위한 물리적인 단추는 없었지만 터치스크린을 사용하여 손가락으로 전화번호를 입력할 수 있었다. 또, 팩시밀리와 메모를 수행하기 위해 부가적인 스타일러스 펜을 사용할 수 있었다. 오늘날의 기준으로 살펴보면 시몬이 제공하는 기능을 일반적인 수준으로 평가할 수 있으나, 당시에는 혁신적인 기술로 주목을 받았다.

스마트폰의 활성화는 노키아가 주도하였다. 노키아 커뮤니케이터 라인은 1996년에 노키아 9000을 시작으로 노키아의 첫 스마트폰을 출시하였다. 이 스마트폰은 당시 노키아의 베스트셀러였던 휴대전화와 휴렛패커드 초기 PDA 모델의 협동결과로 탄생한 것이었다. 노키아 9210은 최초의 컬러 스크린 커뮤니케이터 모델이면서 개방형 운영 체제를 가진 최초의 진정한 스마트폰이었다. 9500 커뮤니케이터 또한 노키아의 첫 카메라폰이었고 다른 제조사의 제품보다도 20%~40% 정도 더 비쌌다.

그림 2. 현대의 스마트폰
Fig 2. Modern smartphones

2.2 스마트폰 시장현황

시장조사업체 SA(Strategy Analytics)가 최근 발표한 보고서에 따르면 2009년 4분기 전 세계 스마트폰의 출하대수는 전년대비 30% 성장한 5300만대로 이에 힘입어 2009년 연간규모는 1억 7380만대로 확대되었음을 확인할 수 있다. 이는 전년 판대매수 1억 5110만대에 비해 약 15% 증가한 수치이다. 아래 표는 2009년 4분기 현재 전 세계의 스마트폰 판매량을 나타낸다.

표 1. 스마트폰 판매량(출처 : SA)
Table 1. Sales of Smartphone

구분	세계 스마트폰 판매(백만)		스마트폰 시장점유율(%)	
	2009년 4분기	2009년 전체	2009년 4분기	2009년 전체
노키아	20.8	67.8	39.20%	39.00%
RIM	10.7	34.5	20.20%	19.80%
애플	8.7	25.1	16.40%	14.40%
그 외	12.8	46.4	24.20%	26.70%
계	53	173.8	100.00%	100.00%

국내 스마트폰 시장은 해외 시장에 비해 아직까지는 미미한 상황이다. 이는 플랫폼의 폐쇄적 운영정책에 의한 것으로 플랫폼이 개방되면서 아이폰을 비롯한 다수의 안드로이드폰이 휴대폰 제조사를 통해 경쟁적으로 출시되고 있다. 비즈니스 컨설팅 기관인 이노사이트 그룹의 2010년 1월 9일 “The Future of Smartphone in Korea”라는 보고서에 따르면 2011년 국내 스마트폰 이용자 수는 174만 명이 될 것으로 예측하고 있다. 이노사이트 그룹은 올해 말을 기준으로 국내 스마트폰 사용자가 73만명으로 약 1.5%의 점유율에 그치지만, 2011년에는 사용자 수와 점유율이 두 배 이상 급증해 174만명에 3.7%의 점유율을 전망하고 있다.

특히 지난 2007년, 구글이 안드로이드(Android)라는 새로운 모바일 플랫폼을 발표하면서 스마트폰 시장에 비약적인 성장을 예고하였다. 삼성전자나 모토로라, LG전자 등 세계 유수의 휴대폰 제조업체들이 안드로이드 기반 스마트폰의 개발을 경쟁적으로 발표하고 있으며, 휴대폰뿐만 아닌 다른 여러 임베디드 장비에도 안드로이드를 탑재하여 상용 플랫폼으로 사용하겠다는 움직임이 활발하게 일어나고 있다.

안드로이드는 2007년 11월에 구글이 모바일 관련 여러 플레이어가 참여하는 OHA(Open Handset Alliance)라는 모임을 통해 발표되었다. 그 이후로 전 세계의 모든 휴대폰 제조사나 통신사업자들, 그리고 일반 사용자들의 뜨거운 관심을 끌었고, 2008년 11월 대만의 제조업체 HTC가 G1이라는 이름으로 미국의 T-Mobile 이동통신사를 통해 최초의 안드로이드 단말을 출시함으로써 세상에 등장한다.

안드로이드를 간단히 표현하자면 운영체제(OS, Operating System)부터 미들웨어, 그리고 자바(Java) 언어로 개발되는 중요 애플리케이션까지를 모두 포괄하고 있는 "모바일 단말을 위한 소프트웨어 스택"이라 할 수 있다. 즉, 안드로이드는 단말기에서 하드웨어를 제외한 나머지 모든 소프트웨어의 계층을 다 포함하고 있다.

안드로이드의 가장 큰 특징은 개방형 플랫폼이라는 것이다. 구글은 대부분의 안드로이드 소스 코드를 완전 개방하였고, 따라서 누구든지 안드로이드를 이용하여 제한 없이 안드로이드 기반의 스마트폰 및 응용 프로그램을 개발할 수 있다.

2009년 10월 Gatner에서 발표한 자료에 따르면 2009년 1분기 현재 안드로이드 운영체제의 스마트폰 시장 점유율은 1.6%에 불과하지만 2012년에 이르면 아이폰을 제치고 심비안에 이어 두 번째 점유율을 차지할 것으로 예측되었다.

표 2. 안드로이드 스마트폰의 성장(출처 : Gatner)
Table 2. Growth of Android Smartphone

운영체제	2009년 1분기	2012년 4분기	판매량 (백만)	성장률 (%)
심비안	49.3%	39.0%	203.58	-10.3
안드로이드	1.6%	14.5%	75.69	+12.9
아이폰 OS	10.8%	13.7%	71.51	+2.9
윈도우 모바일	10.3%	12.8%	66.82	+2.5
림 OS	19.9%	12.5%	65.25	-7.4
리눅스	7.0%	5.4%	28.19	-1.6
Web OS	0.0%	2.1%	10.96	+2.1

III. 스마트폰 보안위협

3.1 보호대상

스마트폰의 이용 확대는 모바일 네트워크 개방 및 오픈 플랫폼 적용을 가져왔지만, 다음과 같은 이유로 보안 위협이 증가하는 결과를 초래하고 있다.

첫째, 개방형 운영체제 기반의 다양한 응용 프로그램 공유로 인하여 보안 위협이 증대되고 있다. 이는 리눅스 기반의 개방형 운영체제인 안드로이드나 리모를 통해 잘 알 수 있다. 둘째, PC와 같이 다양한 멀티미디어 서비스 기능 및 인터페이스 지원으로 인한 Wireless Attack, Virus, Worm 등의 보안 위협이 증가하였다. 셋째, 장치 간 융합으로 인하여 새로운 모바일 위협에 노출되어 있다. 이러한 새로운 위협에는 모바일 이용료를 과다하게 부과하게 만드는 Overcharging 공격 (SMS/MMS 공격, Cross-service 공격) 및 장치의 가용성을 떨어뜨리는 DoS 공격 (배터리 소모 공격) 등이 있다. 넷째, 모바일 기기 제조사가 아닌 제삼자에 의한 3rd party application 시장의 활성화로 인하여 보안 위협이 증대하고 있다. 애플의 경우 응용 프로그램에 대해 자체 검증을 하고 있으나, 구글의 경우 기본적인 검증 수준 등으로 모바일 단말 사용자의 보안 위협 노출은 심각한 수준이다.

스마트폰은 다양한 모바일 기기들이 융합된 형태라고 볼 수 있다. 다양한 전자기기의 융합은 즉, 다양한 정보들이 융합되어 있음을 의미한다. 따라서 스마트폰의 분실, 도난 및 스마트폰의 보안에 대한 위협은 개인의 다양한 정보에 대한 위협이며, 앞서 언급한 바와 같이 스마트폰의 경우 과금 및 결제와 직접적으로 연관되어 있기 때문에 다른 모바일 기기와는 비교할 수 없는 피해를 초래할 수 있다.

아래 표는 스마트폰의 보안위협 분석에 앞서 위협으로부터 보호되어야 하는 대상인 자산을 분류하고 있다[1]. 자산은 크게 스마트폰 기기 자체와 스마트폰 내에 저장된 중요 정보로 분류할 수 있다.

표 3. 스마트폰의 자산
Table 3. Assets of Smartphone

자산	설명
중요 정보	- 주소록, 통화기록, 위치정보, 수첩 및 일정, 이메일, 웹 브라우저 캐쉬 파일, 웹에서 사용하는 비밀번호 등 스마트폰에 저장되어 있는 개인정보 - 업무에 사용되는 경우 스마트폰에 저장되어 있는 고객정보 및 기업 내부정보가 포함될 수 있음
스마트폰	- 스마트폰 기기 자체

스마트폰에서는 우선 일반 휴대폰과 동일한 개인정보들이 저장된다. 통화기록, 주소록, 문자메시지, 사용자가 촬영한 혹은 다운받은 사진, 사용자의 메모 등이 바로 이러한 개인정보이다. 스마트폰은 여기에 사용자의 일정 정보, 사용자의 이메일, 웹브라우저와 관련된 캐시파일, 웹에서 사용하는 비밀번호 등을 덧붙일 수 있다. 이러한 개인정보들은 바로 스마트폰이 보유하고 있는 자산으로서 위협으로부터 보호해야 하는 대상이 된다. 그리고 스마트폰 자체 역시 자산이 될 수 있다. 스마트폰은 휴대폰처럼 과금 및 결제와 밀접하게 연관되어 있기 때문에 스마트폰의 분실은 분실로 인한 타인의 사용 등으로 인해 즉각적인 금전적 손실을 유발할 수 있다. 물론 스마트폰의 도난은 개인정보의 유출로도 이어지기 때문에 경계해야 한다.

스마트폰은 쿼티 자판 또는 터치스크린을 입력 장치로 제공을 하는데, 사실 모바일 기기의 3~4인치에 불과하기 때문에 입력이 용이하지는 않다. 따라서 인증 서비스를 제공하는 대부분의 응용 프로그램들은 사용자 ID 및 비밀번호를 저장하는 기능을 갖추고 있다. 최초 프로그램의 사용 시 사용자 인증을 수행하고 이후에는 저장해놓은 이전 인증정보를 사용하여 인증을 완료하는 방법이다. 실제 PC 환경에서 접속하는 네이버는 아이디 저장기능만 제공하고 있지만, 모바일 버전의 네이버는 아이디뿐만 아니라 비밀번호 역시 저장할 수 있다. 이는 사용자의 편의를 위한 것이지만, 만일 스마트폰을 분실하거나 도난당할 경우 타인이 사용자의 개인정보를 인증과정 없이 확인할 가능성이 있기 때문에 위험하다.

3.2 스마트폰 사용환경

앞서 스마트폰의 자산에 대해 살펴보았다. 본 절에서는 스마트폰 보안위협을 도출한다. 위협을 도출하기 위해 스마트폰의 사용환경을 구체적으로 살펴본다. 아래 그림은 스마트폰 사용환경을 나타낸다.

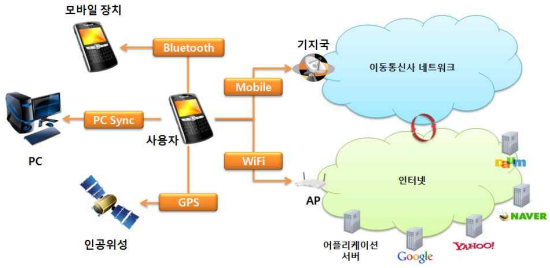

그림 3. 스마트폰 사용환경
Fig 3. Environments of Smartphone

스마트폰은 위 그림과 같은 환경에서 다른 네트워크 혹은 장비와 연결되어 사용된다. 각각의 환경에 대해 살펴보면 다음과 같다.

사용자는 스마트폰을 직접 사용하는 일인칭 환경을 의미한다. 사용자는 스마트폰을 직접 휴대하고 다니면서 통화, 문자메시지 등의 기본적인 통신서비스와 무선네트워크 서비스 그리고 일정관리 및 기타 등의 스마트폰이 제공하는 기능을 필요로 한다.

기지국은 사용자에게 통화와 문자메시지 등의 통신서비스와 함께 3G망을 통한 무선네트워크 접속환경을 제공한다. 3G망을 통한 무선네트워크 접속은 데이터 요금을 필요로 한다.

AP는 WiFi(Wireless Fidelity) 기술을 바탕으로 통해 사용자에게 무선네트워크 서비스를 제공한다. 이때에는 별도의 과금이 부과되지 않는다. 단, 통신사에서 설치한 AP의 경우에는 특정 요금제를 요구하는 경우도 있다.

인공위성은 스마트폰이 필요로 하는 경우 GPS를 활용한 위치정보를 제공한다. 위치정보는 스마트폰의 각종 응용 프로그램에 의해 스마트폰에서 또는 응용 프로그램 서버에서 적절히 가공되어 사용자에게 서비스로서 제공된다.

PC는 스마트폰과 케이블을 통해 직접 연결되거나, 무선네트워크를 통해 연결될 수 있는데, 데이터의 백업, 스마트폰 업데이트, 스마트폰 충전 등이 가능하다.

3.3 스마트폰 보안위협

위협은 보호대상이 어떤 환경에서 어떤 방법으로 인해 훼손될 수 있는지를 의미한다. 따라서 본 절에서는 스마트폰의 위협을 앞서 언급한 사용환경과 보호대상을 중심으로 도출한다.

각각의 위협을 도출하기에 앞서 스마트폰의 자산이 훼손될 수 있는 경로를 사용환경을 중심으로 서술하면 아래와 같다.

첫째, 공격자는 무선 네트워크에서 전송되는 데이터를 도청하거나 위변조 할 수 있다. 공격자는 무선 네트워크에 대해 알려진 여러 가지 공격방법들을 적용하여 전송되는 데이터를

중간에 가로채거나 위변조를 시도할 수 있다. 사용자는 스마트폰을 사용하여 온라인 뱅킹을 이용할 수 있는데 이때에는 무선 네트워크상으로 사용자의 주요 개인정보들이 전송되게 된다. 이 경우 공격자는 무선 네트워크 상에서의 일반적인 공격방법을 적용하여 정보의 도청, 위변조 등을 시도하여 사용자에게 심각한 피해를 초래할 수 있다.

둘째, 공격자는 스마트폰의 가용성을 훼손하기 위해 DOS 공격을 시도할 수 있다. 공격자는 네트워크에 존재하는 다양한 서버뿐만 아니라 기지국에 대해서도 DOS 공격을 시도할 수 있다.

셋째, 공격자는 서버를 공격하여 서버에 저장되어 있는 정보를 획득하거나 서버를 통해 악성코드를 유포할 수 있다. 특정 응용 프로그램의 경우 무선 네트워크에 접속하여 서버와 정보를 주고받으면서 사용자에게 서비스를 제공하는데, 이 때 공격자가 해당 서버를 공격하면 사용자와 관련된 정보를 획득할 수 있다. 대표적인 예로는 위치정보를 사용하는 응용 프로그램을 들 수 있다. 공격자는 서버를 공격하기 위해 서버 OS의 취약성, 서버 응용 프로그램의 취약성 등 다양한 공격기법을 사용할 수 있다. 또, 공격자는 악성 코드를 삽입한 응용 프로그램을 앱스토어에 업로드 함으로써 악성코드를 유포할 수 있다. 또는 악성코드가 포함된 콘텐츠를 서버를 통해 사용자에게 제공함으로써 악성코드를 유포할 수 있다. 악성코드에 감염된 사용자는 무선 네트워크뿐만 아니라 블루투스 등 다양한 경로를 통해 악성코드를 재유포할 수 있다. 특히 블루투스를 이용하는 악성코드는 블루투스를 통해 스마트폰의 주요 정보들을 외부로 유출하는 형식, 악성코드를 주변의 블루투스로 연결된 기기에 유포하는 형식, 그리고 지속적으로 통신을 유발하여 배터리를 소모시키는 형식 등이 알려져 있다.

넷째, 공격자는 PC를 통해 스마트폰을 공격할 수 있다. 악성코드를 PC에 심어두고 스마트폰이 PC와 연결되는 경우 스마트폰의 주요 정보들을 획득할 수 있다. 또 PC의 악성코드를 스마트폰으로 전이할 수도 있다.

다섯째, 공격자는 스마트폰을 직접 공격할 수도 있다. 공격자는 스마트폰을 훔쳐 스마트폰에 저장되어 있는 주요 정보를 획득하거나, 불법적으로 사용하여 과금을 유발할 수 있다.

이처럼 스마트폰은 스마트폰의 여러 외부 환경과 데이터를 주고받으며 사용자에게 서비스를 제공한다. 따라서 위협요소는 공격자의 공격 포인트에 따라 크게 스마트폰 내부에 대한 공격과 스마트폰 외부환경에 대한 공격으로 구분할 수 있다.

스마트폰 내부에 대한 공격은 다시 스마트폰의 응용 프로그램 레벨에서의 공격, 스마트폰 플랫폼 레벨에서의 공격 그리고 스마트폰의 기기에 대한 공격으로 구분할 수 있고, 스마트폰 외부에 대한 공격은 스마트폰과 통신하는 웹서버, 기지국, PC, 그리고 다른 모바일 기기에 대한 공격으로 구분할 수 있다. 단, 다른 모바일 기기에 대한 공격은 스마트폰 내부에 대한 공격과 중복되므로 스마트폰 내부에 대한 공격으로 갈음하고자 한다.

본 절에서는 위와 같은 스마트폰의 특징을 기반으로 스마트폰의 보안위협을 도출한다.

아래 표는 스마트폰의 위협요소를 나타낸 것이다. T는 위협(Threat)의 약자를 나타낸다.

표 4. 스마트폰의 위협요소
Table 4. Threats of Smartphone

구분		설명
스마트폰 내부 (응용 프로그램)	T1	- 악성코드 감염으로 인해 스마트폰에 저장되어 있는 정보가 위변조 또는 유출될 수 있음
	T2	- 스마트폰이 악성코드에 의해 DOS 공격의 숙주가 되거나 SPAM 발송자가 되어 불필요한 과금이 유발될 수 있음[1-2]
	T3	- 배터리 소모 공격 등을 시도하는 악성코드 감염으로 인하여 스마트폰 가용성이 훼손될 수 있음[1]
	T4	- 도청 프로그램을 통해 사용자의 통화내용 및 문자메시지가 외부로 유출될 수 있음[2]
	T5	- 응용 프로그램의 취약성으로 인해 스마트폰에 저장되어 있는 정보가 위변조 또는 유출될 수 있음
	T6	- 응용 프로그램의 오류로 인하여 스마트폰 가용성이 훼손될 수 있음
	T7	- 응용 프로그램과 응용 프로그램 간의 호환성 문제로 인하여 가용성이 훼손될 수 있음[3]
	T8	- 응용 프로그램과 플랫폼 간의 호환성 문제로 인하여 가용성이 훼손될 수 있음[3]
스마트폰 내부 (플랫폼)	T9	- 스마트폰 플랫폼의 취약성으로 인해 스마트폰의 정보가 위변조 및 유출될 수 있음[4]
	T10	- 플랫폼 취약성으로 인하여 가용성이 훼손될 수 있음[4]
	T11	- 플랫폼과 응용 프로그램의 비호환성으로 인하여 가용성이 훼손될 수 있음[3]
	T12	- 스마트폰 탈옥(Jail Breaking) 등의 플랫폼의 위변조를 통해 기존 방화벽이 풀리면서 악성코드에 노출될 위험이 있음[5]
스마트폰 내부 (스마트폰 기기)	T13	- 스마트폰의 분실, 도난 및 재사용으로 인해 개인정보가 유출되거나 불법적인 과금이 유발될 수 있음[1]
	T14	- GPS가 장착된 스마트폰의 경우 위치정보가 불법적으로 유출될 수 있음[6]
	T15	- 전자기파 간섭 및 방해로 인해 스마트폰의 가용성이 훼손될 수 있음[7]
스마트폰 외부 (네트워크)	T16	- 무선 네트워크에 대한 공격으로 인해 사용자 정보가 위변조 및 유출될 수 있음[2]
	T17	- 무선 네트워크상에서 man in the middle attack을 시도할 수 있음[8]

스마트폰 외부 (서버 및 기지국)	T18	- 서버에 대한 DOS 공격으로 인하여 스마트폰 사용자의 가용성이 훼손될 수 있음[1]
	T19	- 기지국에 대한 DOS 공격으로 인하여 스마트폰 사용자의 가용성이 훼손될 수 있음[1-2]
	T20	- 서버 OS의 취약성으로 인하여 정보가 위변조 및 유출될 수 있음
	T21	- 서버 응용 프로그램의 취약성으로 인하여 정보가 위변조 및 유출될 수 있음
	T22	- 피싱 웹사이트에 접속하는 경우 사용자의 정보가 유출될 수 있음[2]
	T23	- 악의적인 AP 등을 통해 사용자의 정보가 유출될 수 있음[2]
	T24	- 서버가 악성코드에 감염된 콘텐츠를 제공함으로써 사용자에게 악성코드를 전파할 수 있음[1-2]
	T25	- 서버가 사용자의 스마트폰에 SPAM 메일 및 문자를 대량으로 전송할 수 있음[1-2]
	T26	- 서버에 저장된 사용자의 위치정보가 유출될 수 있음
스마트폰 외부 (PC)	T27	- 스마트폰이 악성코드에 감염된 PC에 접속하는 경우 사용자 정보가 외부로 유출될 수 있음[2]

IV. 스마트폰 보안위협 대응기술

4.1 보안목적

본 절에서는 스마트폰의 보안목적을 정의한다. 스마트폰은 다양한 사용환경에서 공격자의 여러 가지 위협에 노출이 되어 있다. 이러한 보안위협들로부터 스마트폰을 안전하게 관리하기 위해서는 아래와 같은 보안목적이 선행되어야 한다.

아래 표는 스마트폰 보안목적을 나타낸다.

표 5. 스마트폰 보안목적
Table 5. Security Objectives of Smartphone

보안목적	설명
O1.기밀성	- 스마트폰 외부로 전송되는 데이터들은 공격자의 위변조로부터 안전해야 함
O2.무결성	- 스마트폰 내부에 저장된 개인정보 및 외부로 전송되는 데이터들은 무결성을 유지해야 함
O3.가용성	- 스마트폰은 기능의 실패 또는 DOS 공격 등으로부터 가용성을 확보해야 함
O4.식별 및 인증	- 스마트폰은 사용자 인증 기능을 제공하여 인증된 사용자에게만 스마트폰의 기능을 사용할 수 있게 해야 함
O5.접근제어	- 스마트폰은 접근제어 기능을 제공하여 신뢰되지 않은 사용자의 스마트폰에 대한 접근을 차단할 수 있어야 함

스마트폰은 다양한 위협으로부터 정보의 위변조 및 유출을 방지하기 위해 기밀성과 무결성을 유지해야 한다. 또 스마트폰은 가용성을 보장함으로써 사용자의 편의를 도모해야 한다. 그리고 스마트폰은 개인정보 및 과금체계와 밀접하게 연관이 되어 있으므로, 분실이나 도난, 재사용 등에 의한 피해를 방지하기 위해 식별 및 인증과 접근제어를 제공해야 한다. 아래 [표 6]은 보안목적과 보안위협과의 관계를 나타낸다. 각각의 대응관계는 위협과 직접적으로 연관되는 보안목적을 나타낸다. 예를 들어, T1의 경우 기밀성, 무결성, 식별 및 인증, 접근제어와 연관관계를 맺고 있는데, 이는 악성코드가 스마트폰의 정보를 위변조하거나 유출시킴으로써 기밀성과 무결성을 훼손하고, 이러한 활동 과정에서 사용자가 아닌 공격자 임의로 정보를 변경함으로써, 스마트폰의 식별 및 인증과 접근제어를 훼손함을 의미한다.

대응관계는 포괄적 측면에서 보면 모든 항목이 모든 위협과 연관되어 있다고 생각할 수 있으나, 본 절에서는 직접적인 연관성을 기준으로 정리하였다.

표 6. 스마트폰 보안위협과 보안목적의 대응관계
Table 6. Relations of Threats and Security Objectives

보안위협 \ 보안목적	O1. 기밀성	O2. 무결성	O3. 가용성	O4. 식별 및 인증	O5. 접근제어
T1	O	O		O	O
T2			O	O	O
T3			O	O	O
T4	O			O	O
T5	O	O			
T6			O		
T7			O		
T8			O		
T9	O	O			
T10			O		
T11			O		
T12	O	O	O		
T13	O	O	O	O	O
T14	O				
T15			O		

T16	O	O			
T17	O	O			
T18			O		
T19			O		
T20	O	O			
T21	O	O			
T22	O				
T23	O				
T24	O	O	O		
T25			O		
T26	O				
T27	O				

4.2 스마트폰 보안위협 대응기술

본 절에서는 정의한 보안목적을 충족시키기 위한 위협대응 기술을 설명한다. 대응기술은 현재 다양한 연구가 진행 중인 기술도 있고, 개발이 완료되어 제공되는 것도 있다.

대응기술은 위협과 대응하며, 모든 위협에 대해 대응기술이 존재함으로써, 앞서 언급한 스마트폰의 보안목적을 충족할 수 있다. 아래 [표 7]은 스마트폰의 위협과 이에 대응하기 위한 대응방법을 나타낸다.

표 7. 스마트폰 위협대응기술
Table 7. Countermeasures

위협	대응방법
T1	- 스마트폰 전용 보안프로그램의 사용으로 악성코드의 활동을 방지할 수 있음 - 응용 프로그램 개발자 및 응용 프로그램 검수를 통해 악성코드의 배포를 사전에 차단할 수 있음 - 스마트폰에 저장되는 데이터를 암호화하여 위변조를 방지할 수 있음 - 응용 프로그램에 대한 주기적인 보안 패치를 통해 악성코드로 인한 피해를 경감할 수 있음 - 접근제어 및 사용자 인증기술을 적용함으로써 악성코드로 인한 피해를 경감할 수 있음
T2	
T3	
T4	
T5	- 응용 프로그램에 대한 보안 패치의 주기적인 업데이트를 통해 자체적인 취약성으로 인한 피해를 경감할 수 있음
T6	- 응용 프로그램을 사전에 시험하고 배포 후에도 주기적으로 업데이트를 함으로써 알려지지 않은 오류에 대해 대응할 수 있음
T7	- 응용 프로그램 사전 시험을 통해 주요 프로그램들 간의 호환성을 확인할 수 있음
T8	- 응용 프로그램 사전 시험을 통해 플랫폼과의 호환성을 확인할 수 있음
T9	- 플랫폼의 주기적인 업데이트를 통해 플랫폼 취약성을 악용한 피해사례를 예방할 수 있음 - 보안 API를 적용하여 데이터를 암호화함으로써 스마트폰 내부 정보의 유출을 방지할 수 있음 - 전자서명 등의 보안 기술을 적용하여 스마트폰 내부 정보의 무결성을 유지할 수 있음
T10	
T11	- 응용 프로그램 사전 시험을 통해 플랫폼과의 호환성을 확인할 수 있음
T12	- 보안 프로그램의 사용을 통해 악성코드에 의한 위협을 방지할 수 있음
T13	- 스마트폰에 사용자 인증 기술을 적용함으로써, 주요 정보에 대해 인증된 사용자만 접근을 허가할 수 있음 - 원격으로 스마트폰을 잠금으로써 불법적인 사용을 차단할 수 있음 - 분실이나 도난당한 스마트폰의 정보를 원격으로 삭제함으로써 정보의 유출을 방지할 수 있음
T14	- 위치정보를 암호화하여 처리하거나, 위치정보를 기반으로 서비스를 제공하는 웹서버의 보안을 통해 위치정보의 불법적인 유출을 방지할 수 있음
T15	- 전자기파 간섭제거 기술을 적용하여 방지할 수 있음
T16	- 스마트폰에 탑재된 웹브라우저가 제공하는 암호화 통신을 적용하여 데이터의 무결성 및 기밀성을 보장할 수 있음 - 응용 프로그램을 사용하여 전송데이터를 암호화함으로써 기밀성을 보장할 수 있음 - 전자서명 등의 보안 기술을 적용하여 데이터의 무결성을 보장할 수 있음
T17	- 암호화, 전자서명 등의 보안기술을 적용하여 인증과정을 강화함으로써 공격에 대응할 수 있음 - 생체인식이나 음성인식 등의 기술을 적용하여 인증과정을 강화함으로써 공격에 대응할 수 있음
T18	- 서버를 운영할 때 적절한 보안운영지침과 방화벽, 침입탐지 시스템, 안티 DDOS 솔루션을 사용함으로써, 서버에 대한 공격에 대응할 수 있음
T19	- 기지국에 대한 DOS 공격 시 사용자 행동분석, 블랙리스트 관리 등을 통해 적절히 통신량을 조절하고 차단함으로써 DOS 공격에 대응할 수 있음
T20	- 항상 최신의 보안패치를 유지하고 적절한 보안지침을 운영함으로써 알려지지 않은 취약성에 대응할 수 있음 - 주기적인 보안 패치를 통해 자체적인 취약성으로 인한 피해를 경감할 수 있음
T21	
T22	- 브라우저 및 포털 사이트에서 제공하는 웹서버 인증기능을 사용하여 부적절한 피싱사이트로 인한 피해를 방지할 수 있음

T23	- 보안정책을 통해 인가되지 않은 네트워크에 대한 접근을 차단하거나, 인가되지 않은 AP에 대한 접근을 불허함으로써 악의적인 AP에 따른 피해를 방지할 수 있음
T24	- 보안 프로그램을 사용하여 콘텐츠를 사전에 검사함으로써, 악성코드로 인한 피해를 방지할 수 있음
T25	- SPAM 필터링 기술을 사용하여 무분별한 SPAM 메시지에 의한 피해를 방지할 수 있음
T26	- 서버를 운영할 때 적절한 보안운영지침과 방화벽, 침입탐지 시스템, 안티 DDOS 솔루션을 사용함으로써, 서버에 대한 공격에 대응할 수 있음
T27	- PC의 운영체제에서 제공하는 방화벽, 외부 네트워크에서 제공하는 침입탐지시스템 등의 보안장비를 사용하여 악성코드의 침입을 방지할 수 있음 - PC에서 백신 등의 보안 프로그램을 사용하여 악성코드를 방지하고 발견하는 경우 제거할 수 있음

소프트웨어 및 플랫폼의 검증은 현재 응용 프로그램을 제공하는 앱스토어를 중심으로 활발하게 전개되고 있다. 애플에서 제공하는 앱스토어의 경우 개발자에 대한 인증뿐만 아니라 개발자가 개발한 응용 프로그램에 대해서도 사전에 인증과정을 거침으로써 악성코드의 유포를 사전에 차단하기 위해 노력을 경주하고 있다. 스마트폰 시장에서 후발주자로 등장한 안드로이드의 경우 현재까지는 이러한 응용 프로그램 검수과정이 정착되지 않아 앱스토어가 애플에 비해 활성화가 더딘 편이다. 응용 프로그램의 검증은 개발자의 서명을 추가하거나 DRM 기술을 적용하여 가능하다. 그러나 현실적으로 모든 프로그램을 검수하는 것은 무리가 있으며, 프로그램들 간의 호환성까지 확인하는 것은 어렵기 때문에 좀 더 효율적인 방법이 고찰되어야 한다.

보안프로그램의 경우 현재 스마트폰 보안프로그램이 서서히 출시되고 있는 상황이다. 국내에서도 최근 아이폰 및 안드로이드폰 전용 보안 프로그램을 출시하였다. 또 스마트폰 운영체제 역시 자체적으로 방화벽을 제공하고 있다. 그러나 급증하는 응용 프로그램과 앞으로 등장할 다양한 악성코드의 유형에 발 빠르게 대처하기 위한 기술적 진보가 필요하다.

암호화통신은 스마트폰에 탑재된 웹브라우저 및 응용 프로그램을 통해 제공되고 있다. 스마트폰에 탑재된 웹브라우저는 기존 PC와 동일한 형태의 SSL 프로토콜을 지원한다. 웹브라우저 외에도 스마트폰은 응용 프로그램을 통해 데이터의 암호화 및 복호화를 제공하고 있다.

스마트폰의 접근제어 기술은 현재 연구가 집중적으로 진행되고 있는 분야로 스마트폰의 접근제어 기술을 통해 개인정보 보호를 도모하고 있다. 현재의 스마트폰은 사용자 인증과정이 없고, 사용자의 권한에 따른 접근제어 기능 역시 미약한 수준이다. 스마트폰 접근제어 기술을 적용하면, 스마트폰의 분실이나 도난에 의한 개인정보 유출 및 과금유발 등을 방지할 수 있다. 또 주요 개인정보의 암호화 등을 통해 데이터의 무결성을 유지할 수 있다[9].

스마트폰 플랫폼 보안은 스마트폰 운영체제의 개발자들을 중심으로 연구가 진행되고 있다. 운영체제의 취약성 분석 및 주기적인 패치와 보안 커널의 개발을 통해 플랫폼의 취약성으로 인한 스마트폰의 문제에 대응하고 있는 상태이다[10]. 그러나 소위 탈옥(Jail Breaking)으로 인한 보안위협을 간과하기는 어렵다. 많은 아이폰 사용자들이 탈옥을 한 버전으로 스마트폰을 사용하고 있고, 안드로이드의 경우에도 최근 루팅(rooting)이라 불리는 관리자 권한 획득방법이 공개되었다. 이는 개발자가 예상하지 못한 환경에서 스마트폰을 사용하는 것으로 보안위협에 적절히 대응하기 어렵다는 단점이 있다. 그러나 탈옥 사용자 커뮤니티를 주요 보안 이슈와 대응방법이 알려져 있고, 스마트폰 전용 보안프로그램이 속속 등장하고 있기 때문에 보안위협 역시 자체적으로 충분히 완화할 수 있으리라 기대된다.

외부 서버 보안은 네트워크 서버 및 기지국을 중심으로 보안기술이 개발되어 적용되고 있다. 외부 네트워크에 대한 공격은 이미 공격방법과 대응기술이 널리 알려져 있고, 현재 널리 적용되어 있다. 외부 서버에 대한 DOS 공격이나, 서버 취약성으로 인한 취약성은 주기적인 보안패치와 방화벽, 침입탐지시스템, DOS 대응장비, 보안감사 등을 통해 대응하고 있으며, 보안지침을 유지하고 관리함으로써 대응이 가능하다.

기업보안의 경우 일반 사용자와 보안위협 및 대응기술은 크게 다르지 않다. 단, 사안의 기밀성이나 피해범위는 개인보다 더 크다고 할 수 있다. 기업 환경에서 스마트폰 보안은 독립적인 보안체계를 갖추고 있는 경우 기존의 보안대응기술에서 기업에서 제공하는 솔루션 사용 및 기업의 스마트폰 사용 관련 보안지침을 준수함으로써 충족할 수 있다.

V. 결론

스마트폰은 PC와 유사한 수준의 강력한 성능을 바탕으로 사용자에게 다양한 서비스를 제공함으로써, 현재 시장규모가 급속히 성장하고 있다.

사용자는 스마트폰을 사용하여 일반 휴대폰과 마찬가지로 음성통화, 문자메시지, 멀티미디어 메시지 등의 기능을 사용할 수 있으며, 다양한 응용 프로그램을 바탕으로 여러 가지 서비스를 부가적으로 사용할 수 있다. 최근에는 응용 프로그램을 공유하는 앱스토어가 등장하면서 전세계 개발자들이 사

용자의 요구를 반영한 다양한 응용 프로그램을 출시하고 있으며, 그 개수는 아이폰의 경우 16만여개에 달하며, 안드로이드 역시 5만개여개에 달한다. 이처럼 다양한 응용 프로그램은 스마트폰의 활용용도를 PMP, MP3 Player, 전자사전, 지도 등으로 확장시키고 있다. 즉, 스마트폰은 다양한 모바일 기기의 융합 형태로 발전하고 있다. 바꾸어 말하면 이는 스마트폰에 다양한 정보가 집적되어 있음을 의미한다.

또 스마트폰은 휴대용 기기로서 분실의 우려가 높고, 통화, 문자메시지, 무선네트워크 접속 등의 서비스는 과금과 직접적으로 연결되어 있기 때문에 스마트폰의 취약성은 정보의 손실뿐만 아니라 즉각적인 금전적 피해도 야기할 수 있다.

따라서 스마트폰의 보안이 최근 중요한 이슈로 부각되고 있다. 그러나 연구동향을 살펴보면 스마트폰의 악성코드에 의한 취약성 분석, 스마트폰 플랫폼의 취약성 분석 등 단편적인 주제에 대한 연구는 활발하게 진행되고 있으나, 스마트폰의 총체적인 보안위협과 그에 대한 대응기술에 대한 정의가 명확하지 않은 실정이다.

이에 본 논문은 스마트폰의 사용환경을 중심으로 위협을 도출하고 이에 대응하는 기술을 설명하였다. 본 논문의 연구결과는 스마트폰의 향후 보안기술 연구 및 스마트폰의 보안기준 개발에 활용될 수 있을 것이다.

참고문헌

[1] Collin Richard Mulliner, "Security of Smart Phone," Master's Thesis of University of California, 2006. 06.

[2] Chuanxiong Guo, Helen J. Wang, Wenwu Zhu, "Smart-Phone Attacks and Defenses," HotNets III, 2004. 11.

[3] Jengchung V. Chen, David C. Yen, Kuanchin Chen, "The acceptance and diffusion of the innovative smart phone use: A case study of a delivery service company in logistics," Information & Management Volume 46, Issue 4, 2009. 03.

[4] Asaf Shabtai, Yuval Fledel, Uri Kanonov, Yuval Elovici, Shlomi Dolev, "Google Android : A State of the Art Review of Security Mechanisms", arXiv 2009, 2009. 11.

[5] *http://seriot.ch/resources/talks_papers/iPhone Privacy.pdf*

[6] *http://www.mt.co.kr/view/mtview.php*

[7] Andrew Monk, Evi Fellas, Eleanor Ley, "Hearing only one side of normal and mobile phone conversations," Behaviour & Informaion Technology, Volume 23, Issue 5, 2004. 09.

[8] *http://threatcenter.smobilesystems.com*

[9] Xudong Ni, Zhimin Yang, Xiaole Bai, Adam C. Champion, and Dong Xuan, "DiffUser : Differentiated User Access Control on Smartphones," Proc. 5th IEEE Int'l. Workshop on Wireless and Sensor Networks Security (WSNS '09), 2009. 09.

[10] Aubrey-Derrick Schmidt, Hans-Gunther Schmidt, Jan Clausen, Ahmet Camtepe, and Sahin Albayrak, "Enhancing Security of Linux-Based Android Devices," 15th International Linux Kongress, 2008. 10.

저 자 소 개

전 웅 렬

2006 : 성균관대학교 컴퓨터공학과 (공학사)

2008 : 성균관대학교 전기전자컴퓨터공학과(공학석사)

2008~현재 : 성균관대학교 전기전자컴퓨터공학과 박사과정

관심분야 : 보안성평가, 스마트폰 보안

E-mail : wrjeon@security.re.kr

김 지 연

1995 : 성균관대학교 정보공학과 (공학사)

1997 : 성균관대학교 컴퓨터공학과 (공학석사)

2008 : 성균관대학교 컴퓨터공학과 (공학박사)

1996-2007 : 한국정보보호진흥원 선임연구원

관심분야 : 암호프로토콜, 암호이론, 정보보호관리체계 인증

E-mail : jeeyeonkim@paran.com

이 영 숙

1987 : 성균관대학교 정보공학과 (공학사)

2005 : 성균관대학교 정보보호학과 (공학석사)

2008 : 성균관대학교 컴퓨터공학과

(공학박사)
2009-현재 : 호원대학교 사이버수사경찰학부 전임강사
관심분야 : 암호프로토콜, 암호이론, 네트워크 보안
E-mail : ysooklee@howon.ac.kr

원 동 호
1976년-1988년 :
성균관대학교 전자공학과(학사, 석사, 박사)
1978년-1980년 :
한국전자통신연구원 전임연구원
1985년-1986년 :
일본 동경공업대 객원연구원
1988년-2003년 :
성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년-1998년 :
국무총리실 정보화추진위원회 자문위원
2002년-2003년 : 한국정보보호학회장
2002년-2008년 :
대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT감사 자문위원
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장
관심분야 : 암호이론, 정보이론, 정보보호
E-mail : dhwon@security.re.kr