스마트폰 악성코드 분석을 통한 확산 방지 모델에 관한 연구

임수진* · 이정현** · 강 형* · 박원형* · 국광호*

요 약

최근 전 세계적으로 스마트폰을 이용한 인터넷 이용인구의 증가에 따라 스마트폰 악성코드에 대한 관심이 높아지고 있다. 특히, 해외에서는 심비안, 윈도우 모바일이 탑재된 스마트폰을 대상으로 모바일 악성코드가 발생하고 있어 이에 대한 대응이 필요하다. 따라서 본 논문은 2004년 이후 발생한 모바일 악성코드에 대한 현황 및 구체적 사례 분석을 통해 보안 위협을 설명한다. 또한, 국내 스마트폰 악성코드의 발생에 대응하기 위해 향후 발생할 수 있는 악성코드 확산 방지 시스템에 대한 모델을 제시한다.

A Study on Protection Model of Propagation through Smartphone Malware Analysis

Su Jin Lim* · Jung Hyun Lee** · Hyung Kang*
Won Hyung Park* · Kwang Ho Kook*

ABSTRACT

Recently, the number of internet users using smartphone is increasing worldwide, and the interest in the smartphone malware is increasing. Especially, since mobile malware are occurring to the smartphones using Symbian or Windows Mobiles in the abroad, it is necessary to have an action plan against these malwares. This paper describes the possible security threat through the analysis of the malwares occurred after 2004. Also we present a model for the future propagation prevention system which can cope with domestic smartphone malwares.

Key words : Smartphone, Malware, Threat

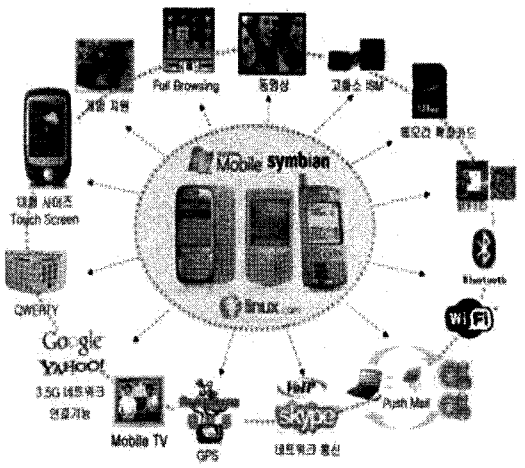
접수일 : 2010년 1월 4일; 채택일 : 2010년 2월 12일

* 서울산업대학교 산업정보시스템공학과
** 고려대학교 정보경영공학전문대학원

1. 서 론

스마트폰은 똑똑한(Smart)과 휴대폰(Phone)이라는 단어의 합성어이다[1]. 스마트폰은 최근 통신 인프라의 발전에 따른 휴대폰의 변화 및 사용자들의 다양한 요구에 의하여 출현하게 되었으며, 이렇게 대두된 스마트폰의 다양한 인터페이스 및 기능이 하나의 스마트폰 기기에서 제공됨으로 인하여 스마트폰 컨버전스가 우리의 실생활에서 실현되었다. 일반 휴대폰보다 진보된 능력을 가진 스마트폰은 PC와 유사한 기능의 단말기로써 범용 운영체제가 탑재한 휴대폰으로 정의 할 수 있다. 주요 특징으로 PDA 기능 및 Wi-Fi를 통한 무선 인터넷 서비스, QWERTY 자판 등을 탑재하고 있다.

(그림 1)은 스마트 폰의 여러 가지 기능을 보여주고 있다.



(그림 1) 스마트폰의 기능[2, 3]

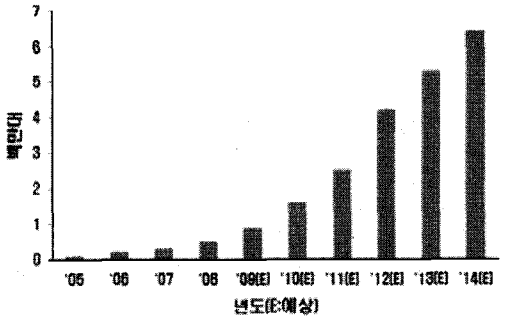
전 세계 스마트폰의 판매량을 살펴보면 세계적으로 개방형 플랫폼 기반 스마트폰 시장의 규모는 2008년 12.9%에서 2010년까지 26.5%로 성장할 것으로 예상하고 있다. <표 1>은 전 세계 스마트폰 판매 현황을 나타낸다.

국내 스마트폰 이용자 수는 2009년 약 50만 명으로 추산되고 있으며 이는 전체 이동통신서비스 이용자의 1% 정도에 불과하다. 이 수치는 미국의 스마트폰 보급현황이 약 20% 수준임을 감안할 때 국내 스마트폰 시장의 성장 가능성이 매우 높을 것으로 보여주고 있다. (그림 2)는 국내 스마트폰 판매량 추이를 보여주고 있다.

〈표 1〉 전 세계 스마트 폰 판매 현황[3]

(단위 : 천대)

Company	2009 Sales	2009 Market Share(%)	2008 Sales	2008 Market Share(%)
Nokia	18,441	45.0	15,297.9	47.4
Research in Motion	7,678.9	18.7	5,594.2	17.3
Apple	5,434.7	13.3	892.5	2.8
HTC	2,471.0	6.0	1,330.8	4.1
Fujitsu	1,249.0	3.0	1,071.5	3.3
Others	5,688.2	13.9	8,085.8	25.1
Total	40,962.8	100.0	32,272.7	100.0



(그림 2) 국내 스마트폰 판매량 추이[1]

지난 2004년 F-Secure(안티 바이러스 업체)가 29A라는 바이러스 제작 그룹으로부터 스마트폰 단말기에도 컴퓨터 바이러스의 제작이 가능하다는 개념증명(Proof of the Concept)코드인 Cabir를 확보했을 때만 해도 현재처럼 수많은 스마트폰 악성코드와 변종이 창궐할지를 예상하지 못했다[5].

본 논문은 스마트폰 악성코드인 Cabir가 출현한

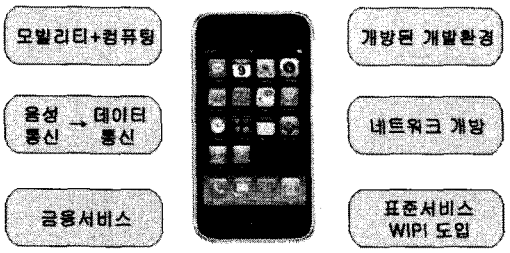
2004년을 기준으로 꾸준히 증가하고 있는 스마트폰 악성코드를 분석하고 국내 출현에 대비해 사용자 기반의 스마트폰 악성코드 확산 방지 시스템을 모델링하여 대응 방안에 대해 연구하고자 한다.

2. 관련 연구

2.1 스마트폰 위협

2000년 이후 지속적으로 발전한 스마트폰 서비스는 그 가입자의 증가 속도만큼이나 연관된 많은 산업들이 함께 발전했다.

음성통화만 가능했던 휴대폰에서 게임, 인터넷 등 다양한 서비스를 자유로이 즐길 수 있는 시대가 되면서 스마트폰 컨텐츠의 보급 및 발전이라는 긍정적인 면과 함께 스마트폰 악성코드를 제작하여 유포하는 부정적인 사례가 발생하기 시작하였다. 다음은 스마트폰 단말기의 잠재적인 위협에 대한 설명이다.



(그림 3) 스마트폰의 잠재적 보안 위협[6]

① 모빌리티(Mobility) + 컴퓨팅 파워(Computing Power)결합 : 휴대폰의 전화기능에 MP3, 동영상과 같은 멀티미디어서비스 등 각종 부가서비스의 추가로 컴퓨팅 기능이 향상했다.

② 음성통신에서 데이터통신으로 : 휴대폰의 기능이 음성통신에서 데이터 통신으로 영역이 넓어지면서 사용자들은 단말기를 통하여 무선인터넷을 이용해 더 많은 정보에 접근할 수 있게 되었다.

③ 개인화된 장비 : 스마트폰 단말기는 사용자의 주소록, 인터넷 뱅킹 정보 등 중요한 데이터를 유지·보관하는 개인화 장비로 자리 잡았다.

④ 스마트폰 단말기의 금융 결제 : 단말기와 스마트폰 결제 기능의 결합은 악의적인 사용자들이 쉽게 돈을 벌 수 있는 새로운 대상으로 자리 잡고 있다.

⑤ 개방된 개발환경 : 개방된 개발환경은 악의적인 개발그룹이 쉽게 악성코드를 개발할 수 있는 환경을 조성할 수 있다.

⑥ 개방된 네트워크 : 개방된 네트워크를 통해 악성코드의 유포가 용이해 진다.

⑦ 표준화된 플랫폼(운영체제) : 스마트폰 단말기의 표준화된 플랫폼은 개방된 개발환경에서 제작된 악성코드가 개방된 네트워크를 통해 쉽게 전파될 수 있는 환경이 조성된다.

위의 환경요소의 거의 모든 부분을 충족하는 스마트폰 운영체제가 바로 심비안 운영체제와 윈도우 스마트폰 운영체제이다. 특히, 심비안 운영체제는 시장 점유율이 73.3%로 가장 많은 시장을 차지하고 있어 현재 많은 악성코드의 공격대상이 되고 있다[6].

2.2 스마트폰 악성코드 현황

2004년 Cabir가 출현한 이후 다양한 스마트폰 악성코드가 발견되고 있으며, 초기의 실험실 수준의 코드에서 점차 다양한 악성코드 변종을 출현시켜 스마트폰 환경의 위험수준이 증가되고 있다.

<표 2>는 스마트폰 악성코드를 2004년부터 현재까지 출현한 순서대로 나열한 도표이다.

Cabir발견 이후 F-Secure에 따르면 2007년 12월 말까지 180종[7]의 바이러스 백신이 개발되었으며, 376종[8]의 악성코드들이 발견되었다. 그리고 2008년 이후의 정확한 통계는 확인하기 어려운 실정이다.

〈표 2〉 스마트폰 악성코드 현황[7]

발견연도	악성코드 명	변종수	점유율(%)
2004. 6	Cabir	14	7.7
2004. 11	Cdropper	17	9.4
2005. 3	Commwarrior	16	8.8
2005. 9	Cardtrap	20	11.1
2005. 11	AppDisabler	10	5.5
2006. 3	Singlejump	11	6.1
2006. 3	FlexiSpy	4	2.2
2006. 3	CommDropper	11	6.1
2006. 6	Romride	11	6.1
2007. 12	HatiHati	1	0.5
	기타	65	36.1
합계	180종		100%

주) 2007년 12월 기준.

다음은 주요 악성코드들의 출현 기록이다.

① Cabir : 노키아 단말기의 블루투스를 이용해 전파되는 최초의 웜이다. 이 웜의 소스가 공개되면서 여러 변종이 출현하는 계기가 되었다.

② Cdropper : 스마트폰 장치에 Cabir 변종을 설치할 심비안 SIS 파일 trojan의 일종으로 Cabir 변종이 드롭 되는 곳에 위치한다.

③ Commwarrior : 기존의 스마트폰 악성코드의 유형과는 다른 새로운 형태로 블루투스가 아닌 MMS를 통한 확산을 시도한다. 사용자에게 부당 요금이 청구되는 금전적인 피해를 줄 수 있는 최초의 스마트폰 웜이다.

④ Cardtrap : Cardtrap.SIS 파일을 설치하면 메모리 카드에 윈도우 악성코드인 Padobot.Z와 Rays를 복사하며 Padobot.Z는 Autorun이 가능하므로 윈도우 PC에서 자동실행 될 수 있다.

⑤ AppDisabler : 악의적인 SIS 파일의 Trojan으로 third party application의 대부분의 기능을 무력화시킨다.

⑥ Singlejump : 시스템 파일과 3rd party 어플리케이션을 손상된 바이너리로 교체하는 심비안 SIS 파일 trojan이다.

⑦ FlexiSpy : 최초의 상업용 Spy 프로그램으로 음성, SMS, 그리고 컨텐츠의 정보를 수집하여 기록하고 원격서버로 전송한다.

⑧ CommDropper : Commwarrior 악성코드로부터 파일을 드롭시켜 설치한다.

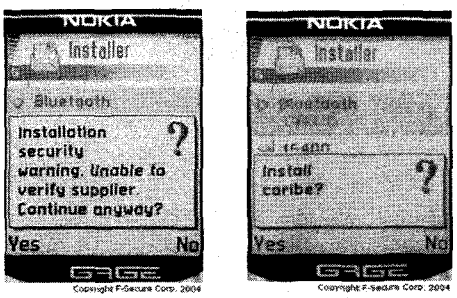
⑨ Romride : malfunctioning system 환경 구성요소를 설치하는 악의적인 SIS trojan이며, 휴대폰이 스타트업 장애를 발생시킨다.

⑩ HatiHati : MMC 카드로 전파되는 웜으로 휴대폰에 복사되어 고음의 SMS 메시지를 보내게 된다.

3. 스마트폰 악성코드 분석과 특징

3.1 스마트폰 악성코드 분석

본 장에서는 Cabir와 Commwarrior 악성코드를 분석한 두 악성코드의 특징은 모두 블루투스를 통해서 여러 나라로 확산되었다는 점이다. Cabir 웜은 유럽에서 많이 쓰이는 심비안 운영체제 기반의 노키아 단말기에서 사용되는 블루투스를 이용해 전파되는 최초의 웜이다.



(그림 4) Cabir 악성코드

블루투스 기능을 이용하여 주변기기로 전파되므로 블루투스 기능을 Off시 피해 방지가 가능하다.

아래 국가별 Cabir 확산 현황을 보면 Cabir가 전파된 나라의 공통점은 전통적으로 컴퓨터의 보급률이 높은 나라가 아닌 저개발 국가가 다수임을 보여준다.

〈표 3〉 국가별 Cabir 확산 순위

순 위	국 가
1	필리핀
2	싱가포르
3	아랍에미레이트
4	중국
5	인도
6	핀란드
7	베트남

이는 Cabir가 블루투스를 이용해 전파된다는 점을 생각하면 악성코드 전파의 필요조건이 많은 수의 사람들과 제한된 공간 등 인구 밀도가 높은 나라에서 빠르게 확산될 수 있음을 보여준다.

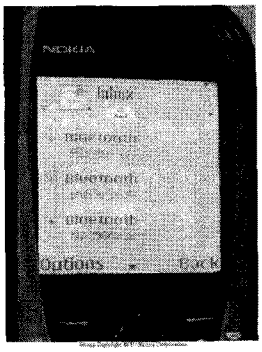
아래는 국가별 Commwarrior 악성코드 확산 순위이다.

〈표 4〉 국가별 Commwarrior 확산 순위

순 위	국 가
1	아일랜드
2	인도
3	오만
4	이탈리아
5	필리핀
6	핀란드
7	그리스

Commwarrior는 Cabir가 출현된 후 약 8개월 후에 출현하였고, 이 악성코드는 블루투스와 멀티미디어메시지(MMS)를 이용해 동시에 전파되는데 Cabir 악성코드 확산보다 빠르게 스마트폰 단말기에 전파된다.

기존의 모바일 악성코드의 유형과는 다른 새로운 형태로 블루투스와 멀티미디어메시지(MMS)를 통해 확산되며, 사용자에게 부당 요금이 청구되는 금전적인 피해를 줄 수 있는 최초의 모바일 악성코드이다.



(그림 5) Commwarrior 악성코드

F-Secure의 조사 기록[9]을 보면 Commwarrior의 감염 수가 2006년 6월 11~17일 사이에 약 5,000개였고, 그 다음 주인 2006년 6월 18~24일에는 6,200개로 약 1,200개가 증가했다. 약 1주일 동안에 20%이상 감염수가 늘어난 것을 확인 할 수 있다.

3.2 스마트폰 악성코드의 특징

현재까지 출현한 스마트폰 악성코드의 행위들을 종합하면 다음과 같은 악의적인 행동들이 가능하다.

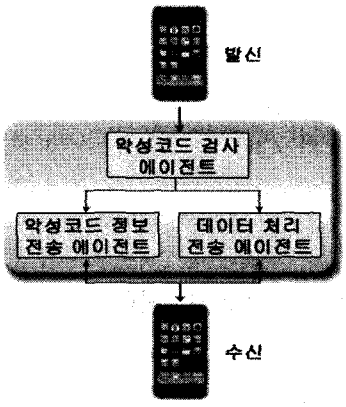
① 파일 감염 및 실행 차단
② 메모리 카드 차단
③ 스마트폰 단말기의 원격 제어
④ 어플리케이션 혹은 아이콘 변경
⑤ 블루투스 혹은 멀티미디어메시지(MMS)를 통한 확산
⑥ SMS 메시지 전송을 통한 과도한 요금 발생
⑦ 다른 사용자의 SMS파일 훔쳐보기
⑧ 사용자 데이터 은닉 및 도난
⑨ 다른 악성코드 다운로드 설치

4. 스마트폰 악성코드 확산 방지 모델

Commwarrior 악성코드는 블루투스와 멀티미디어메시지(MMS)를 이용한 무차별 확산이 문제가 되었다. 국내에 악성코드 출현 시에도 동일한 현상이 발생할 것으로 판단되어 본 장에서는 악성코드에 대응하기 위해 블루투스와 멀티미디어메시지(MMS) 서비스 기능을 자동 차단하는 사용자 기반의 스마트폰 악성코드 방지 시스템을 모델링한다.

4.1 스마트폰 확산 방지 모델 개념

스마트폰 악성코드 방지 시스템은 아래와 같이 악성코드 검사, 악성코드 정보 전송, 데이터 처리 전송 에이전트를 둔다.



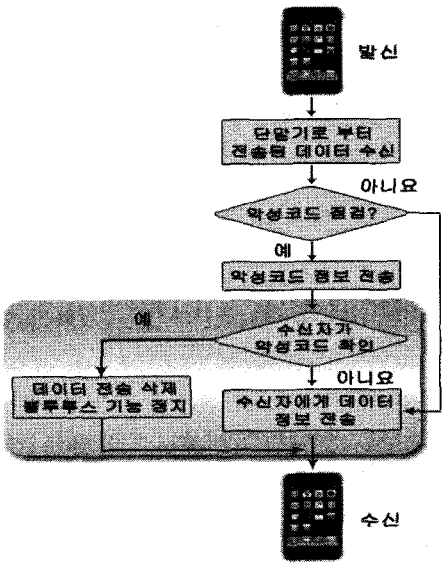
(그림 6) 스마트폰 악성코드 감염 방지 시스템 개념

악성코드 검사 에이전트는 스마트폰 단말기로부터 전송된 데이터를 분석하여, 전송된 데이터에 악성코드가 포함되어 있는지 여부를 검사한다. 악성코드를 검출하는 기술은 기존에 알려진 문자열에 대해 패턴 매칭(Pattern Matching)기술을 사용한다. 패턴 매칭은 스마트폰 단말기로부터 전송된 데이터를 데이터베이스에 저장된 악성코드 패턴과 비교하여 전송된 데이터에 악성코드가 포함되어 있는지 여부를 판단하도록 설계 한다.

악성코드 정보전송 에이전트는 상기 악성코드 검사 에이전트에 의해 전송된 데이터에 악성코드가 포함되어 있다고 판단되면, 메시지(Message)를 통해 수신자 스마트폰 단말기로 악성코드 정보를 전송한다. 데이터를 전송하기 전에 트래픽 채널(Traffic Channel)을 통해 수신자 스마트폰 단말기에 메시지(Message)를 전송하여 전송할 데이터가 어떤 성격의 데이터인지 통보하는 과정을 수행한다.

데이터 처리전송 에이전트는 수신자 스마트폰 단말기로부터의 데이터 수신 여부 선택정보에 따라 해당 수신된 데이터를 수신자 스마트폰 단말기로 전송하거나 또는 삭제 및 블루투스 차단 기능을 한다.

4.2 스마트폰 악성코드 확산 방지 모델

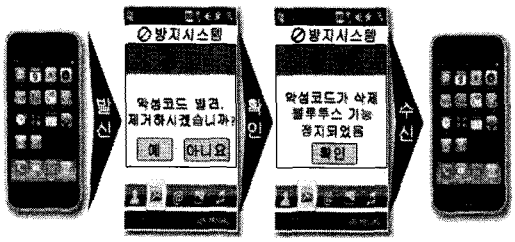


(그림 7) 악성코드 확산 방지 흐름도

① 스마트폰 단말기가 악성코드에 감염된 멀티미디어서비스 송신
② 악성코드 에이전트가 검사
③ 악성코드에 감염 되었다는 정보를 수신자에

계 통보
④ 수신자는 메시지를 통해 악성코드를 확인
⑤ 선택한 데이터정보에 따라 악성코드 삭제 및 블루투스 기능을 정지

다음은 사용자 기반의 악성코드 방지 시스템 수행 과정을 설명한다.



(그림 8) 악성코드 방지 시스템 수행 과정

이동통신 시스템과 스마트폰 단말기 상호간에 프로토콜 메시지를 이용해 스마트폰 시스템이 악성코드가 포함된 데이터를 수신할 수신자 스마트폰 단말기로 데이터를 전송하기 전에 악성코드 정보를 통보함으로써 수신자가 해당 데이터를 수신할지 여부를 선택할 수 있고 수신자의 동의하에 스마트폰 악성코드를 사전에 차단할 수 있어 오탐 여부 등을 사용자가 판단하여 스마트폰 단말기를 보호할 수 있다.

5. 결 론

2005년 이후 국내 이동 3사는 WIPI 플랫폼으로 표준화 되었고, 현재 WIPI 2.0으로 업그레이드되면서 강력한 플랫폼을 구성하게 되었다.

패쇄적인 네트워크 구조에서 개방적인 네트워크로 변화되면서 국내에도 자연스럽게 스마트폰 악성코드의 출현이 임박한 상태이다.

앞서 스마트폰 악성코드가 출현할 수 있는 환경에서 언급했듯이 이미 국내는 스마트폰 악성코드가 출현할 수 있는 환경이 조성되었다.

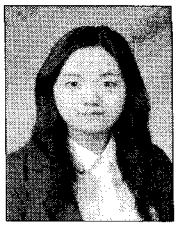
다만, 이동통신사의 폐쇄적인 서비스 구조와 제한된 개발자 그룹으로 인해 현재 악성코드의 출현이 저지되고 있다고 판단되며, 악성코드에 많은 피해를 당한 심비안社는 9버전 이상부터 Trusting Computing을 도입하여 악의적인 행동을 방지 할 수 있는 보안 프레임워크를 도입했다. 국내의 WIPI 플랫폼도 폴더와 API접근 제한을 통해서 만일의 경우 악성코드 출현 시 실행을 제한할 수 있다.

하지만, 이보다 더 확실한 대응방법은 앞서 제안한 악성코드 방지 시스템을 이용하여 사용자 동의하에 악성코드를 제거하는 방법이 최적이라 판단된다.

또한 스마트폰 취약점에 대한 철저한 모니터링과 정보공유를 통해 이동통신 사이버 대란이 발생하지 않도록 국내 스마트폰 악성코드 출현 및 확산에 대비하여야 하겠다.

참 고 문 헌

[1] 심재홍, "모바일 인터넷 정보보호를 위한 모바일 악성코드 분석", 정보보호학회지, 2009.
[2] KIEI, "휴대폰(스마트폰) 및 부품/소재 기술시장분석 세미나", 2009.
[3] 김기영, "개방형 모바일 환경에서 스마트폰 보안기술", 정보보호학회지, 2009.
[4] Gartner, "Worldwide Smartphone Sales to End Users in 2Q2009", 2009.
[5] http://www.expoapt.com/education/html/pc/pc04-02.htm.
[6] "스마트폰 장치로 인해 기업의 보안 위협 증가", 트랜드마이크로 보안칼럼, http://www.trendmicro.co.kr/security/column/cl/archive/2006/column_2_5.asp, 2006.
[7] http://www.f-secure.com/v-descs/mobile-description-index.shtml.
[8] http://mobile.f-secure.com/news/september_07.html.
[9] "F-Secure mobile virus", http://www.f-secure.com.



임 수 진

2006년 서울산업대학교 산업정보시스템공학과 입학
현재 서울산업대학교 산업정보시스템공학과 네트워크 보안 Lab 연구원

이 정 현

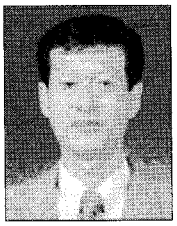
2002년 중앙대학교 정보산업대학원 석사(정보보호 및 인터넷)
현재 고려대학교 정보경영공학전문대학원(박사과정)

강 형

2006년 서울산업대학교 산업정보시스템공학과 입학
현재 서울산업대학교 산업정보시스템공학과 통합정보시스템 Lab 연구원

박 원 형

2002년 서울산업대학교 산업정보시스템공학과 (공학사)
2005년 서울산업대학교 정보산업공학과(공학석사)
2009년 경기대학교 정보보호학과 이학박사 (정보보호전공)
현재 서울산업대학교 산업정보시스템공학과 겸임교수



국 광 호

1979년 서울대학교 공과대학 (공학사)
1981년 서울대학교 대학원 (공학석사)
1984년 청주대학교 산업공학과 전임강사
1989년 Georgia Institute of Technology, U.S.A (공학박사)
1993년 한국전자통신연구원 선임연구원
현재 서울산업대학교 산업정보시스템공학과 교수