Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.3, Jun. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.3.499

안드로이드 플랫폼 기반 악성사이트 차단 방법*

김 대 청,† 류 재 철‡
충남대학교

The blocking method for accessing toward malicious sites based on Android platform*

Dae-cheong Kim,† Jae-cheol Ryou‡
Chungnam National University

요 약

스마트폰, 태블릿과 같은 스마트 기기의 사용이 늘어남에 따라 스마트 기기를 대상으로 하는 모바일 오피스, 금융 서비스, 모바일 전자정부 등 생산성이나 사용자 편의를 위한 서비스들이 대거 등장하였다. 이에 따라 중요한 정보들이 스마트 기기를 통해 다루어져 스마트 기기를 대상으로 하는 악성행위가 꾸준히 증가하고 있다. 특히 스마트 기기를 대상으로 하는 유해사이트, 악성코드 배포 사이트, 피싱(phishing) 사이트 등으로 인한 피해사례가 꾸준히 발생하고 있어 사회적인 이슈로 부각되고 있다. 스마트 기기의 경우 2013년 국내에서 사용하는 플랫폼의 90%가 안드로이드를 사용하고 있어 단말 수준의 차단방법이 필요하였다. 본 논문에서는 안드로이드 플랫폼에서 웹브라우저를 사용하여 악성사이트를 방문할 때 효과적으로 차단할 수 있는 방법을 기술하고 실제 애플리케이션으로 구현하여 악성사이트 차단성능을 분석하였다.

ABSTRACT

According to the increasing use of smart devices such as smart phones and tablets, the service that targets mobile office, finance and e-government for convenience of usage and productivity has emerged significantly. As a result, important information is treated with the smart devices and also, the malicious activity that targets smart devices is increasing steadily. In particular, the damage case by harmful sites, malware distribution sites and phishing sites that targets smart devices has occurred steadily and it has emerged as a social issue. In the case of smart devices, the Android platform is occupied the 90% in Korea, 2013 therefore the method of device block level is required to resolve the social issues of smart devices. In this paper, we propose a method that can be effectively blocked when you try to access an illegal site to Web browser on the Android platform and develop the application and also analyze the wrong site block function.

Keywords: Android, Malicious websites, Phishing, Smishing

I. 서 론

스마트폰, 태블릿과 같은 스마트 기기의 사용자수는 2013년 1월말 기준 방송통신위원회의 유무선 통신서비스 가입자 통계를 살펴보면 각각 약 3,300만 명

접수일(2013년 10월 24일), 수정일(2014년 3월 7일), 게재확정일(2014년 5월 14일)
* 본 연구는 미래부가 지원한 2014년 정보통신·방송(ICT) 연구개발사업의 연구결과로 수행되었음. 또한, 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 ICT연구센터육성지원사업의 연구결과로 수행되었음 (NIPA-2014-H0301-14-1010)

† 주저자, dcmru@cnu.ac.kr
‡ 교신저자, jcryou@home.cnu.ac.kr(Corresponding author)

과 약 73만 명이 사용 중인 것으로 조사되었다[1]. 스마트 기기의 사용자가 늘어남에 따라 스마트 기기를 이용하여 모바일 오피스, BYOD(Bring Your Own Device)와 같이 업무에 활용되고, 스마트폰 뱅킹이나 주식거래와 같은 금융거래에 이용되고, 모바일 전자정부와 같은 민원처리, 병원 및 영화 예약 등 각종 생활 편의 서비스에 사용되고 있다. 이에 따라 스마트 기기를 통해 사용자의 개인정보나 업무에 활용함으로 인해 기업비밀과 같은 중요한 정보가 다루어져 악성행위의 주요대상이 되고 있다.

이러한 서비스들에 사용되는 스마트 기기의 OS(Operating System)로 해외의 경우 2013년 1분기 가트너(Gartner)에 따르면 74.4%가 안드로이드(android)를 사용하고[2], 국내의 경우 아이크로싱(iCrossing)에 따르면 90.1%가 안드로이드를 사용하고 있다고 발표하였다[3]. 이와 같이 안드로이드 플랫폼(platform)은 모바일 시장에서 과반수이상을 차지하고 있고, 안드로이드의 마켓 이외의 앱(apps)을 설치할 수 있는 특성상 안드로이드를 대상으로 하는 악성코드가 많이 발생하고 있다. 2013년 2분기 트렌드마이크로(Trend Micro)에 따르면 안드로이드 기반 누적 악성코드 수는 2013년 2분기 718,000건으로 안드로이드 기반의 악성코드가 350,000건에 도달하기까지는 3년이 소요되었지만 최근에는 단 6개월만에 350,000건 이상 증가하였다고 발표하였다[4].

최근 안드로이드의 악성코드 유형으로는 트로이목마 유형과 유해가능 프로그램 형태가 대부분이다. 트로이목마 유형은 정상적인 앱으로 가장하여 설치된 후 사용자 몰래 악의적인 기능을 수행하며 스미싱(smishing)에 많이 이용되고 있다. 스미싱은 문자메시지를 통해 악성코드 설치를 유도하기 위한 URL(Uniform Resource Locator)을 전달하여 사용자에 의해 악성코드가 설치된 후 스마트폰의 개인정보와 문자메시지를 탈취하여 통신사 소액결제를 통한 금전탈취에 이용된다.

이와 같이 안드로이드에 악성코드를 배포하기 위해 웹서버를 통한 APK(android application package file) 배포방법이 사용되며 주로 해외에 소재를 둔 웹서버를 통해 배포되고 있다. 그리고 안드로이드에서 악성코드를 직접적으로 설치하기 위한 악성사이트의 접근은 안드로이드의 웹브라우저를 통해 이루어진다. 그러므로 악성코드 배포 또는 피싱(phishing) 사이트와 같은 악성사이트나 음란사이트 또는 도박사이트 같은 유해사이트에 접근을 안드로이드의 웹브라우저에서 직접 차단한다면 악성코드 설치를 효과적으로 막을 수 있는 대응방법이라고 할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서 관련연구를 살펴보고, 3장에서는 악성사이트 방지 시스템의 구성에 대해서 살펴보고, 4장에서 실제 웹브라우저의 차단 방법을 제안하고 차단성능을 평가한다. 마지막으로 5장에서 결론을 맺는다.

II. 관련연구

본 장에서는 악성사이트 차단을 단말 상에 관련된 연구와 단말 외적으로 관련된 연구로 나누어 살펴본다.

2.1 단말 상의 관련연구

단말 상에서 악성사이트 차단을 위한 연구로는 스미싱 차단, 자녀관리 등의 애플리케이션 형태이다.

정보보안 기업들은 안드로이드에서 스미싱 차단을 위한 서비스를 제공하고 있다. 스미싱 차단은 안드로이드 단말의 문자메시지 내용을 분석하여 URL을 포함할 경우 네트워크를 통해 URL을 원격의 서버에 질의를 하여 해당 URL의 피싱사이트 여부를 반환을 받아 피싱사이트일 경우 문자메시지를 차단한다. 안드로이드에서는 문자메시지의 내용을 API(Application Programming Interface)를 사용하여 가져올 수 있다. 그러나 안드로이드 시스템의 특성으로 애플리케이션 설치 순서에 따라 문자메시지 내용을 가져오지 못하는 문제가 있고, 문자메시지에 포함된 URL을 사용자가 눌렀을 경우 웹브라우저를 통해 접근을 할 수 있으므로 악성 URL을 포함하는 문자메시지의 확실한 관리가 필요하다.

자녀관리 애플리케이션은 부모가 자녀들의 스마트폰을 관리하기 위한 기능을 제공한다. 주요 기능으로는 음란물의 차단과 유해사이트로의 접근을 방지하거나 스마트폰 사용 기록을 저장하고, 사용시간을 차단하는 기능과 같이 자녀의 스마트폰 사용 통제에 초점을 맞추고 있다.

2.2 단말 외적 관련연구

악성사이트 접근을 방지하기 위하여 네트워크 기반 및 다른 플랫폼을 대상으로 하는 연구를 들 수 있다.

PC의 대표적인 플랫폼인 MS Windows를 대상으

Fig.1. Network configuration of the pattern update system

로 하는 악성사이트 방지시스템을 들 수 있다[5]. 악성 URL 블랙리스트를 생성하기 위해 가상 머신(virtual machine) 환경에서 악성 URL을 수집하는 크롤러(crawler) 시스템을 구성한다. 사용자가 악성사이트로 이동하는 것을 방지하기 위해 MS 익스플로러에서 키보드로 입력하는 URL과 마우스로 클릭하는 URL을 OS 커널(kernel) 드라이브에서 가로채어 URL 블랙리스트와 비교하여 이동을 차단하는 시스템이다. 제안하고 있는 악성 URL을 수집하는 방법은 패턴의 수집목적으로 사용할 수 있지만 MS Windows라는 다른 플랫폼을 대상으로 하고 있어 안드로이드 환경에서 사용할 수 있는 방법이 필요하다.

네트워크 기반의 연구로는 HTTP의 특성을 사용하여 피싱사이트를 탐지하는 연구를 들 수 있다[6]. 피싱사이트는 원시사이트와 유사하게 보이기 위해 원시사이트의 이미지와 게시글 등의 컨텐츠를 링크로 화면에 표시하는 특성을 가진다. 그러므로 피싱사이트 URL의 HTTP 헤더필드를 통해 원시사이트로 유입되는 특성을 이용하여 피싱사이트를 실시간 탐지한다. 네트워크 레벨에서 피싱사이트를 탐지하는 시스템이므로 안드로이드 모바일 환경에서 직접적으로 적용하는 방법은 아니지만 사용자가 접근할 수 있는 피싱사이트를 사전에 탐지하여 차단할 수 있는 방법이다.

III. 시스템 구성

안드로이드 플랫폼에서 사용자가 웹브라우저를 사용하여 악성사이트로 접근할 때 이를 차단하기 위해 클라이언트는 안드로이드에서 제공하는 API를 사용하여 방문하고자하는 URL을 가져온다. 가져온 URL을 악성사이트 패턴과 비교하여 악성사이트일 경우 클라이언트는 웹브라우저에 차단화면을 표시한다. 이와 같은 시스템의 요구사항을 분석하여 설계한 시스템의 구성은 다음과 같다.

3.1 업데이트 서버

업데이트 서버는 패턴 파일을 안드로이드 플랫폼의 웹브라우저를 감시하는 클라이언트에 제공하는 역할을 한다. Fig.1.은 업데이트 시스템의 네트워크 구성을 나타낸다. 업데이트 서버는 웹서비스를 기반으로 하는 시스템으로 단말의 인증절차를 거친 후 업데이트 파일을 제공한다. 업데이트 파일은 네트워크 전송 시 데이터 통신량을 줄이기 위해 ZIP 압축알고리즘을 사용하여 압축을 하고, 공개키 암호화 알고리즘을 사용하여 전자서명을 거친 후 SHA-256 해쉬 알고리즘(hash algorithm)을 사용하여 무결성을 검사하였다. 통신은 HTTPS를 사용한 암호화 통신으로 네트워크상의 기밀을 유지하였다.

3.2 패턴

```
;<?브랜드명?> <?타입?> <?ACTION?> <?도메인명?> <?서브URL?> <?User-Agent?>↵
<?APWG EBAY?> <?0?> <?9?> <?duedaa.org?> <?/paypal/index.html?> <?[*]?>↵
<?APWG EBAY?> <?0?> <?9?> <?111.90.133.28?> <?[*]?> <?[*]?>↵
<?APWG EBAY?> <?0?> <?9?> <?61w52c3xie.ssl.paypal-verifikation.org?> <?/?> <?[*]?>↵
<?APWG EBAY?> <?0?> <?9?> <?adf.ly?> <?/3106546/new?> <?[*]?>↵
```

Fig.2. Pattern file format

안드로이드 플랫폼에서 웹브라우저를 차단하기 위해서는 피싱사이트나 악성코드 배포사이트와 같은 악성사이트 URL 패턴이 필요하다. 패턴의 구성은 이름, 타입, ACTION, 도메인, 서브URL, User-Agent를 하나의 규칙으로 하는 리스트이다. Fig.2.는 패턴파일의 예를 보여준다. 이름은 규칙의 분류를 나타내고, 타입은 룰의 타입을 표현한다. ACTION은 허용 또는 차단과 같은 동작을 정의한다. 하나의 URL을 도메인과 서브URL로 나누어 도메인 레벨에서 차단할 수 있도록 하였고, User-Agent는 클라이언트 웹브라우저의 종류별로 대응을 할 수 있도록 패턴을 구성하였다.

패턴파일의 수집은 피싱사이트의 경우 APWG(Anti Phishing Working Group)에서 제공하는 URL을 시스템의 패턴에 맞게 재분류하였고[7], 악성코드 배포사이트의 경우 신고를 통하여 수집하거나 악성코드의 분석을 통하여 수집을 하였다.

3.3 클라이언트

본 장에서는 클라이언트의 구성요소와 웹브라우저의 차단방법을 살펴본다.

3.3.1 클라이언트 구성

Fig.3. User interface of client

안드로이드 플랫폼에서 범용적인 사용을 위해 클라이언트는 애플리케이션 형태이다. 클라이언트는 UI(User Interface)를 구성하는 액티비티(activity)와 상시 구동을 위한 서비스(service)로 구성되어 있다. 업데이트 서버로부터 패턴을 다운로드 받아 암호화하여 저장하고, URL의 빠른 비교를 위해 서비스 구동 시 패턴을 읽어 메모리상에 로드해둔다. Fig.3.은 클라이언트의 UI를 나타낸다.

3.3.2 차단 방법

안드로이드에서 기본적으로 제공하는 보안모델은 리눅스 시스템을 기반으로 하기 때문에 리눅스의 기본 보안모델인 DAC(Discretionary Access Control)을 그대로 차용하였으며, 자바 가상 머신(java virtual machine)을 기반으로 안드로이드에 최적화된 달빅 가상 머신(dalvik virtual machine)에서 제공하는 샌드박스(sandbox) 모델로 시스템에서 구동되는 프로세스들은 각각의 멀티 유저시스템과 비슷하다[8]. 그러므로 프로세스들은 권한이 없이 다른 프로세스의 영역을 접근할 수가 없다. 이러한 특징으로 인해 정상적인 안드로이드 시스템에서 클라이언트와 독립적으로 실행이 되는 웹브라우저의 정보들을 가져온다는 것은 불가능한 일이다.

그러므로 안드로이드에서 제공하는 API인 ContentProvider, ContentObserver, ContentResolver를 이용하여 허용하는 범위 내에서 웹브라우저의 정보들을 가져와서 사용하였으며 애플리케이션 레벨에서 차단을 위한 기술을 적용하였다.

ContentProvider는 웹브라우저에서 URL과 같은 정보를 제공하는 API로 웹브라우저 내의 로컬 데이터베이스의 정보를 제공하기 위해 구현이 되며, ContentResolver는 클라이언트에서 웹브라우저의 정보들을 가져오기 위해 사용한다[9]. ContentObserver는 ContentProvider에서 브라우저의 정보가 변경되었다는 것을 알려주는 역할을 한다[10]. Fig.4.는 API의 개념도를 나타낸다.

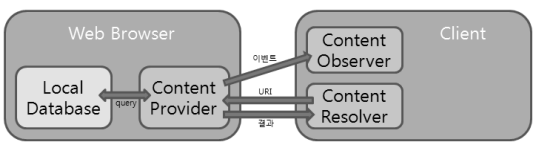

Fig.4. The concept image of blocking API on the web browser

클라이언트에서 차단의 순서는 사용자가 웹브라우저를 사용하여 방문하고자하는 URL로 이동하고자 할 때 웹브라우저상의 URL을 가져와서 패턴과 비교하여 패턴과 매칭이 되는 URL인 경우 패턴의 ACTION에 맞게 웹브라우저의 화면을 제어한다. 만약 ACTION이 차단일 경우 웹브라우저의 화면을 차단화면으로 표시한다. 웹브라우저에 차단화면을 표시하는 방법은 안드로이드에서 정보를 주고받을 때 사용하는 단위인 Intent에 URL 형식의 차단화면에 대한 정보를 설정하고 웹브라우저에 startActivity API를 사용하여 요청을 한다.

마지막으로 허용 및 차단에 대한 로그를 기록한다. 웹브라우저가 차단되는지 확인을 위해 안드로이드에

서 웹브라우저는 기본적으로 설치되어 있는 인터넷(Internet)이라는 이름을 가진 웹브라우저와 구글(Google)에서 서비스 중인 크롬(Chrome) 웹브라우저를 사용하여 차단이 되는 것을 확인하였다.

IV. 검증

본 장에서는 각각의 단말에 기본으로 설치되어 있는 인터넷 웹브라우저와 크롬 웹브라우저의 차단 확인과 차단 성능을 분석한다.

4.1 차단 확인

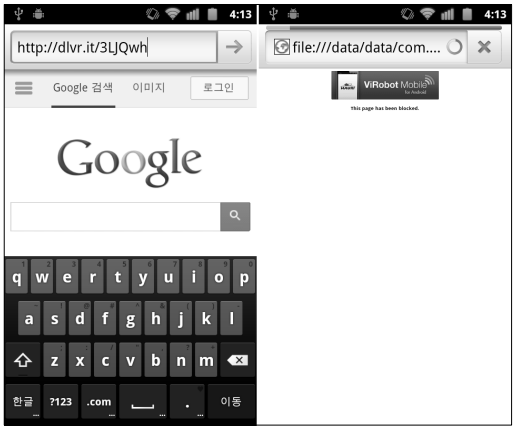

Fig.5. Confirm blocking on the web browser

Fig.5.는 스미싱의 악성코드 배포에 사용되는 단축형태의 URL을 차단한 화면이다. 실제 동작형태는 파일 공유 서비스인 드랍박스(Dropbox) 사이트로 이동하여 APK를 다운로드하게 된다. 악성 URL을 패턴에 포함시킨 후 웹브라우저를 사용하여 URL을 입력하고 이동 버튼을 누르면, 클라이언트가 이를 탐지하여 브라우저에 차단화면이 실행되어 악성사이트로 이동할 수 없다. Fig.6.은 허용 또는 차단된 URL을 시간과 같이 기록하여 감사로그를 제공하는 화면이다.

Fig.6. Audit log

4.2 성능 평가

Table 1.은 테스트를 위한 기기의 환경을 나타낸다. 두 대의 기기를 사용하여 악성사이트 차단 평균속도를 측정하였다. Fig.7.과 같이 패턴의 수는 7272개를 사용하였고, 웹브라우저에서 URL을 입력한 후 이동을 할 때 시간을 시작시간으로 하고, 차단이 완료되었을 때 시간을 종료시간으로 하여 테스트 기기 두 대에서 각각 1000회씩 실행하여 평균속도를 측정하였다.

Table 2.는 두 대의 단말에서 각각 차단 평균 속도를 나타내는 것으로 SM-N900S 모델의 Internet 웹브라우저의 차단 평균 속도는 172.379 ms로 측정이 되었고, Nexus 5 모델의 Chrome 웹브라우저의 차단 평균 속도는 105.055 ms로 측정이 되어 빠른 속도로 차단이 되는 것을 볼 수 있다. 각 단말에서 속도의 차이가 나는 이유는 안드로이드 버전에 따라 웹브라우저 엔진의 버전이 다르고, 네트워크의 연결 상태와 SM-N900S의 경우 제조사에서 웹브라우저의 기능을 대폭 수정하여 이에 따른 오버헤드가 발생한

```
D  05-12 21:41:10.738  21060  29926  com.hauri.vrma.web...  com.hauri.vrma.webfilter  initVrPsList[7272][00:00.718]
D  05-13 18:05:06.720    774    981  com.hauri.vrma.web...  com.hauri.vrma.webfilter  initVrPsList[7272][00:01.235]

D  05-12 21:10:35.880  19819  19819  com.hauri.vrma.web...  com.hauri.vrma.webfilter  handleMessage[00:00.293][true][false]
D  05-12 21:10:36.140  19819  19819  com.hauri.vrma.web...  com.hauri.vrma.webfilter  Block url: http://www.volkeren875.nl/

D  05-13 18:07:58.390    774    774  com.hauri.vrma.web...  com.hauri.vrma.webfilter  handleMessage[00:00.015][true][false]
D  05-13 18:07:58.560    774    774  com.hauri.vrma.web...  com.hauri.vrma.webfilter  Block url: http://www.volkeren875.nl/
```

Fig.7. An example of blocking speed measurement

Table 1. Test environment

Model number	SM-N900S	Nexus 5
Android version	4.3	4.4.2
Web browser version	Internet 1.5	Chrome 33.0.1750.136
CPU	2265 MHz QualcTomm Snapdragon 800 MSM8974AB	2265 MHz Qualcomm Snapdragon 800 MSM8974
GPU	Qualcomm Adreno 330	Qualcomm Adreno 330
RAM	3 GiB	2 GiB
ROM	32 GiB	32 GiB
Manufacturer	Samsung Electronics	LG Electronics

Table 2. Average blocking speed (1/1000 sec)

Model / Average	SM-N900S	Nexus 5
Average of 100 times	139.57	108.16
Average of 100 times	166.4	106.27
Average of 100 times	162.14	100.05
Average of 100 times	175.4	103.5
Average of 100 times	172.72	100.23
Average of 100 times	175.88	97.48
Average of 100 times	168.14	108.66
Average of 100 times	183.23	117.52
Average of 100 times	178.28	106.67
Average of 100 times	202.03	102.01
Average of 1000 times	172.379	105.055

것이다. 각 기기마다 1000회의 반복수행을 하는 동안 SM-N900S 모델의 경우 차단이 되지 않는 경우가 1회 발생을 하였다. 원인을 파악해본 결과 Content Observer API로부터 이벤트를 받지 못하는 상황이 발생을 한 것으로 ContentObserver를 재등록하기 위해 클라이언트를 재실행한 결과 다시 정상적으로 동작이 되는 것을 확인하였다. 이와 같은 API상의 오류는 예외처리를 통해 보완이 가능하다.

본 논문에서 제안하는 안드로이드에서 웹브라우저의 화면을 차단하는 방법은 SDK(Software Development Kit)를 사용하여 애플리케이션 레벨에서 사용할 수 있는 방법으로 안드로이드의 NDK (Native Development Kit), PDK(Platform Development Kit) 및 커널과 같은 하위레벨의 기술적, 안정성에 있어서 보다 접근하기 쉬운 범용적인 방법이고, 안드로이드 플랫폼의 보안 특성상 웹브라우저를 직접 제어를 하지 못하지만 제안하는 방법을 통해 웹브라우저의 URL 이동을 차단할 수 있다. 마지막으로 성능의 큰 저하 없이 차단이 효과적으로 되는 것을 반복적인 수행을 통해 확인하였다.

V. 결 론

스마트 기기의 사용이 늘어남에 따라 스마트 기기에서 다루어지는 중요한 정보가 많아지고 이를 대상으로 하는 악성행위가 늘어나고 있다. 특히 스마트 기기의 과반수를 차지하는 안드로이드는 악성행위의 주요 대상이 되고 있다. 본 논문에서는 안드로이드 플랫폼 기반의 악성사이트 차단 시스템을 구성하여 안드로이드에서 웹브라우저를 사용하여 악성사이트를 방문하고자 할 때 효과적으로 차단되는 것을 확인하였다. 본 논문에서 제안하는 시스템을 통해 안드로이드 플랫폼에 노출되어 있는 유해사이트와 피싱사이트, 악성코드 배포사이트 등과 같은 악성사이트로의 접근을 효과적으로 줄일 수 있을 것이다.

References

[1] Korea Communications Commission, Wired and wireless communication services subscriber statistics (At the end of January, 2013), Mar. 2013.

[2] Gartner, http://www.gartner.com/newsroom/id/2482816, May. 2013.

[3] iCrossing, http://connect.icrossing.co.uk/2013-mobile-market-share-infographic_10062, Jan. 2013.

〔4〕 Trend Micro, TrendLabs 2Q 2013 Security Roundup, Apr. 2013.
〔5〕 Hye-Young Chang, Min-Jae Kim, Dong-Jin Kim, Jin-Young Lee, Hong-Kun Kim and Seong-Je Cho, "An implementation of system for detecting and filtering malicious URLs," Journal of KIISE : Computing Practices and Letters, 16(4), pp. 405-414, Apr. 2010.
〔6〕 Joon-Ho Sa and Sang-Jin Lee, "Real-time Phishing Site Detection Method," Journal of The Korea Institute of Information Security and Cryptology, 22(4), pp. 819-825, Aug. 2012.
〔7〕 APWG, http://www.antiphishing.org, May. 2013.
〔8〕 Android Security Overview, http://source.android.com/devices/tech/security, Feb. 2014.
〔9〕 Content Providers, http://developer.android.com/guide/topics/providers/content-providers.html, Feb, 2014.
〔10〕 ContentObserver, http://developer.android.com/reference/android/database/ContentObserver.html, Feb, 2014.

〈저자소개〉

김 대 청 (Dae-cheong Kim) 정회원
2006년 2월: 대전대학교 컴퓨터공학과 졸업
2010년 8월: 충남대학교 컴퓨터통신및보안 석사
2014년 2월: 충남대학교 컴퓨터통신및보안 박사수료
2006년 2월~현재: 티에스온넷(주) 정보보호연구소 선임연구원
〈관심분야〉 모바일보안, 시스템보안, 디지털 포렌식, 악성코드 분석

류 재 철 (Jae-cheol Ryou) 종신회원
1985년 2월: 한양대학교 산업공학과 졸업
1988년 5월: Iowa State University 전산학 석사
1990년 12월: Northwestern University 전산학 박사
1991년 2월~현재: 충남대학교 컴퓨터공학과 교수
〈관심분야〉 정보보호, 네트워크보안, 암호학, 보안프로토콜