스마트폰 악성코드 제거를 위한 단말 관리 시스템 설계

정기석*

요 약

최근 많은 외산제품들이 국내시장에 유입되고 국내 제품의 출시로 스마트폰 사용자는 급속히 증가하고 있다. 스마트폰 사용자가 증가함에 따라 모바일 악성코드 또한 빠르게 증가하고 있다. 이에 모바일 악성코드에 대한 적절한 대응의 필요성이 증대되고 있다. 단말 관리 방법으로는 SNMP, TR-069 프로토콜이 널리 사용되었지만 이들 프로토콜은 제한적인 관리기능, 이동성 미지원 등으로 인해 모바일 단말 관리에는 적합하지 않다. 모바일 단말 관리 표준인 OMA DM 프로토콜이 대부분의 2G, 3G 무선 단말들의 관리 프로토콜로 채택되고 있으며, 따라서 스마트폰 단말 관리를 위해서도 적합한 프로토콜이라 할 수 있다. 본 논문에서는 악성코드에 대한 현황을 설명하고 스마트폰의 악성코드를 원격제어로 제거할 수 있는 OMA DM기반의 단말 관리 시스템을 설계하였다.

Design of Device Management System for Removing Smartphone Malware

Jeong Gi Seog*

ABSTRACT

Recently, the number of smartphone users is rising rapidly due to an influx of foreign smartphones and sales of domestic products. According to the increase of smartphone users, smartphone malwares are also increasing sharply. Hence it is necessary to protect smartphone against mobile malwares. There are device management protocols as SNMP, TR-069. But these protocols are not suitable for mobile device management because of restrictive management function and unsupported mobility. OMA DM which is a standard for mobile device management has been adopted as mobile device management protocol for most of 2G,3G. Thus it amounts that OMA DM is suitable for smartphone management system. In this paper, the mobile device management system based on OMA DM is designed. This system can remove smartphone malware by remote control.

Key words : Smartphone, Malware, Device Management, OMA DM

접수일(2011년 07월 19일), 수정일(1차: 2011년 09월 10일)
게재확정일(2011년 09월 11일)

* 영동대학교 정보통신보안학과

1. 서 론

방송통신위원회가 2008년 12월 무선인터넷 표준 플랫폼인 위피 탑재 의무를 폐지한 이후 2009년 11월 아이폰의 국내 출시를 계기로 안드로이드폰, 심비안, 블랙베리 등 외국의 스마트폰이 출시되었고 갤럭시S 등 국내 스마트폰은 2010년 한햇 동안 총 45종이 출시되었으며 스마트폰의 편리함으로 인해 사용자수는 급격히 증가하였다. 2009년 말 80만 명에 불과했던 스마트폰 가입자수가 2011년 3월23일 천만 명을 돌파했고 2011년부터 신규단말기의 60%이상이 스마트폰으로 판매되고 있다. 이러한 증가세가 지속되어 올 연말에는 스마트폰 가입자가 2천만 명에 도달할 것으로 전망되는 등 본격적인 스마트폰 대중화 시대에 진입하였다.

스마트폰은 일반 PC와 같이 범용 OS와 웹브라우저가 탑재되어 이용자가 다양한 소프트웨어 및 프로그램을 직접 설치·이용할 수 있는 단말기로 정의된다. 이러한 스마트폰의 본격 확산으로 이동전화는 종래의 음성통화 중심의 기본적 통화수단에서 벗어나 정보검색·교통·게임·금융·교육·모바일 오피스 등 종합 문화서비스 플랫폼으로 진화하였다[1].

스마트폰의 가장 큰 특성은 개방성이라 할 수 있다. 즉, 스마트폰은 범용 운영체제를 사용하고 표준화된 개발 환경을 제공하여 개방화된 운영체제를 통해 개발자들이 자유롭게 애플리케이션을 개발할 수 있는 환경을 제공하고 있다. 그러나 이런 스마트폰 고유기능인 개방성으로 인하여 스마트폰은 모바일 악성코드의 제작을 용이하게 만들고 제작된 모바일 악성코드는 범용 운영체제로 인해 이식성이 높기 때문에 모바일 공격의 규모 및 피해가 증가할 것으로 예상된다. 또한 스마트폰은 3G망, 무선WiFi , 블루투스 등을 통해 24시간 인터넷에 연결할 수 있기 때문에 편리한 반면 무작위로 검색되는 보안이 취약한 무선AP를 이용할 경우 악성코드에 감염될 위험이 있다.

전 세계적으로 2010년 말까지 1000여종의 악성코드가 발생하였으며, 국내에서는 2010년 4월 윈도우 모바일 스마트폰을 대상으로 한 악성코드가 최초로 발생한 이후 2010년 말까지 안드로이드 악성코드가 16개 발생하였으나 2011년 상반기에만 74개가 발견되는 등 단시간 내에 급속히 증가하는 추세에 있다.

본 논문에서는 지금까지 발생한 국내외 모바일 악성코드의 발생현황을 살펴보고 원격으로 악성코드를 제거할 수 있는 단말 관리 시스템을 설계하고자 한다.

2. 스마트폰 현황

스마트폰은 글자 그대로 똑똑한(smart) 휴대폰(phone)이라는 의미를 담고 있다[2]. 스마트폰은 PC와 유사한 기능을 가진 모바일 단말로서 범용 운영체제가 탑재된 휴대폰으로 일반폰(feature phone)보다 진보한 능력을 가지는 휴대폰으로 정의할 수 있다[3].

스마트폰은 일반폰보다 월등히 뛰어난 성능을 가지고 있으며 멀티미디어 처리도 우수하다. 하지만 최근에는 일반폰들의 사양이 스마트폰과 거의 차이가 없을 정도로 개선되어 이를 기준으로 스마트폰과 일반폰을 구분하기는 어렵다. 스마트폰과 일반폰을 구별짓는 가장 큰 특성은 개방성이라 할 수 있다. 스마트폰은 일반폰과는 다르게 무선인터넷 및 외부인터페이스를 개방하여 제공하고 있다. 또한 애플리케이션 개발시 시스템자원의 사용을 위해 SDK를 이용하여 API를 제공하고 있다. 스마트폰의 다양한 외부 인터페이스는 사용자에게 다양한 네트워크 서비스를 지원

<표 1> 2011년 1분기 OS별 전 세계 스마트폰 판매량

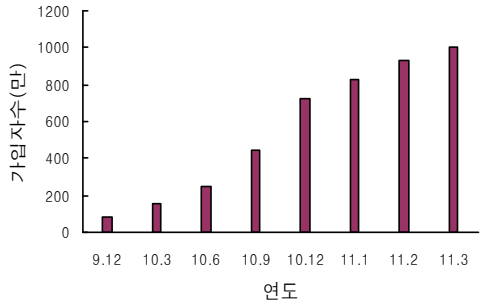
회사	2011년 1분기 (천대)	2011년 1분기 시장점유율(%)	2010년 1분기 (천대)	2010년 1분기 시장점유율(%)
안드로이드	36,267.8	36.0	5,226.6	9.6
심비안	27,598.5	27.4	24,067.7	44.2
iOS	16,883.2	16.8	8,359.7	15.3
림(RIM)	13,004.0	12.9	10,752.5	19.7
MS윈도우 모바일	3,658.7	3.6	3,696.2	6.8
기타	3,357.2	3.3	2,402.9	4.4
총계	100,769.3	100.0	54,505.5	100.0

출처:가트너

하고 내부 API 인터페이스 제공은 개발자에게 편리한 개발환경을 제공한다[4]. 하지만 이를 보안적 측면에서 해석하면 다양한 외부인터페이스 제공은 악성코드 전파 경로의 다양성을 제공하고 내부 인터페이스는 악의적인 개발자에 의해 악성코드가 은닉된 모바일 애플리케이션 제작을 용이하게 만드는 취약점을 가지고 있다.

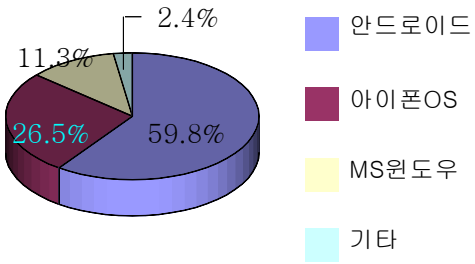
전 세계 스마트폰의 판매량을 살펴보면 2011년 1분기에 전년 동기 5450만대보다 85% 증가한 1억76만대가 판매된 것으로 조사되었다. <표 1>은 전 세계 스마트폰 판매 현황을 나타낸다.

(그림 1)은 국내 스마트폰 가입자 추이를 보여주고 있다. 국내 스마트폰 가입자는 2011년3월23일 1000만 명을 넘어섰으며 2011년 말까지 2000만 명에 도달할 것으로 예상하고 있다.



출처: 방송통신위원회
(그림 1) 국내 스마트폰 가입자 추이

국내 2011년 1월 기준 OS별 스마트폰 가입자 현황을 살펴보면 안드로이드 가입자가 60%, 아이폰 OS가 27%로 안드로이드와 아이폰 가입자가 전체의 87%를 차지한다.

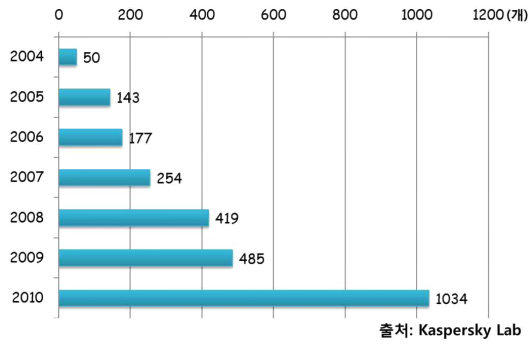


출처: 방송통신위원회
(그림 2) 국내 OS별 스마트폰 가입자 현황
(2011.1 기준)

3. 모바일 악성코드 현황

모바일 악성코드란 스마트폰 및 모바일 기기 등에서 동작하면서 PC 환경에서와 같이 개인정보 유출, 시스템 손상 등의 악의적인 행위를 유발시켜 사용자에게 피해를 끼치는 악성코드를 말한다.

최초의 모바일 악성코드로 알려진 Cabir가 2004년 8월에 필리핀에서 발견된 이후, 2009년 까지 발견된 모바일 악성코드는 총 485종이었으나, 2010년 말에는 약 1000여종으로 2010년 한햇동안 100%가 넘는 증가율을 보임에 따라 앞으로 가파른 상승세가 예상되고 있다[5].



(그림 3) 모바일 악성코드 증가 추이

그동안 발생되었던 모바일 악성코드의 유형을 살펴보면, 감염된 스마트폰 내부의 시스템 파일을 삭제하거나 변형시켜 정상동작을 방해하는 시스템 파괴 및 변경 유형, 배터리 소모를 통한 가용성 저하 유형, 과금 피해를 유발시키는 악성코드 유형, 스마트폰 기기 정보 및 개인정보 등을 유출하는 유형 등이다.

2010년 말 기준 모바일 OS 플랫폼별 악성코드 현황을 살펴보면, 약 89% 이상이 국내 보급률이 미미한 심비안 OS에서 발생하였다. 이는 그동안 전 세계적으로 모바일 OS플랫폼을 주도한 것이 노키아사의

심비안 OS 플랫폼이었기 때문에, 상대적으로 다른 플랫폼들에 비해 악성코드 피해가 많이 발생한 것이라 볼 수 있다. 현재는 아이폰 및 안드로이드폰 출시로 인해 과거 심비안, RIM, 윈도 모바일이 주도하였던 모바일 OS 플랫폼 시장이 다각화되었다.

스마트폰 악성코드는 주로 앱을 통해서 전파되며 안드로이드는 아이폰과 달리 개방형 마켓을 운영하고 있기 때문에 앱을 통한 악성코드가 빠르게 증가하고 있다. 최근 주니퍼네트웍스가 발표한 악성 모바일 위협 보고서 2010/2011에 따르면 안드로이드 악성코드는 2010년 6월 대비 2011년 1월 400%가량 증가했다[6]. 2010/2011년에 발견된 안드로이드용 악성코드를 <표 2>에 정리하였다.

국내의 모바일 악성코드 발생현황을 살펴보면, 2010년 4월 MS 윈도우모바일 플랫폼을 탑재한 스마트폰을 대상으로 국제전화 무단발신을 유발 시키는 악성코드가 (WinCE/TerDial) 최초로 발생하였다. WinCE/TerDial로 인해 2010년 3월말 기준, 국내 스마트폰 가입자 수 163만 명 중 155명의 단말기에서

<표 2> 안드로이드 악성코드 현황

시기	악성코드명	유형
2010.1	Droid09	은행계좌정보 유출(피싱)
.3	마리포사봇넷 Mariposa botnet	개인정보 유출, 모바일 기기를 PC와 연결시 좀비PC
.7	Tap snake	개인정보유출, 사용자 위치 추적 모니터링
.8	Fake player	과금, 러시아로 SMS 전송
.12	게이니미 Geinimi	개인정보유출,중국에서 수만명 감염
2011.1	ADRD	개인정보유출, 수많은 변종 등장
.3	DroidDream	개인정보유출, 마켓에 올라있는 정상적인 앱 감염시킴, 단말기 고유번호 수집
.4	Walk and text	과금, 인기앱의 존재하지 않는 버전,강제 SMS 발송

국제전화 발신이 이루어 졌으나 과금 피해는 발생하지 않았다. 국내에서는 아이폰과 안드로이드폰의 보급이 확대됨에 따라 2010년 말에 16개에 불과하던 안드로이드 악성코드가 2011년 상반기에만 74개가 발견되어 약 5배의 증가세를 보였다[7].

4. 단말 관리 기술 분석

스마트폰의 악성코드를 제거할 수 있는 관리방법은 단말을 원격에서 관리할 수 있는 방법이 적용되어야 한다. 이에 현재 데스크톱 컴퓨터와 모바일 단말기 관리에 적용되고 있는 단말 관리 기술, SNMP, TR-069, OMA DM 등을 살펴보고 스마트폰 악성코드 관리로의 적용 가능성을 분석하고자 한다.

4.1 SNMP

네트워크 상에 존재하는 데스크톱 컴퓨터들을 관리하기 위한 기기 관리 기술로 널리 사용되고 있다. 에이전트와 매니저로 구성된 SNMP (Simple Network Management Protocol)는 MIBs(Management Information Bases)라는 관리객체를 기반으로 기기의 상태 및 네트워크 상태를 읽어오며 일부 설정값을 변경한다. 매니저가 에이전트에게 특정정보를 먼저 요청하고 에이전트가 요청에 응답하는 폴링방식을 사용한다. 또한 에이전트에 특정 이벤트가 발생하면 매니저에게 이벤트정보를 전송하는 트랩(Trap)이라 불리는 방식도 제공한다. 하지만, 이름에서도 알 수 있듯이 SNMP는 Get, Set 등 단말의 설정값을 읽고 수정하는 것과 같은 간단한 기능만을 제공하고 있으며 애플리케이션관리, 오류보고 등의 기능은 제공하지 않는다. 더욱이 SNMP는 유선 LAN의 PC들을 대상으로 설계되었기 때문에 스마트폰에 적용하기 위해서는 상당한 프로토콜 업그레이드가 필요하다.

4.2 TR-069

TR-069(Technical Report-069)는 DSL 서비스 사업자 및 장비제조사 등을 주축으로 한 표준화기구인 DSL 포럼에 의해 개발된 표준으로, CPE(Customer

Premises Equipment : 댁내가입자단말)의 WAN 관리를 위한 프로토콜로서 TPS서비스와 같은 광대역 서비스를 위한 효율성, 확장성, 보안성을 갖는 프로비저닝 및 지원을 위한 프레임워크를 제공한다.

TR-069는 단말의 구성, 진단 및 제어, 업그레이드 등의 관리를 담당하는 서버인 ACS(Auto Configuration Server : 자동환경설정서버)와 CPE간에 양방향 SOAP/HTTP기반통신을 한다.

TR-069는 프로비저닝, 펌웨어.소프트웨어 관리, 상태 및 성능 모니터링, 네트워크 연결성 및 서비스 관련 진단을 제공한다. 그러나 유선WAN의 디지털홈 디바이스에 적합하게 설계되어 있기 때문에 스마트폰에의 적용은 어려운 점이 있다.

4.3 OMA DM

모바일 단말기를 관리하기 위한 기술로는 OMA (Open Mobile Alliance) DM(Device Management)[8]이 널리 사용되고 있다. OMA DM은 단말내 탑재되는 관리 에이전트(DM에이전트)와 관리서버(DM서버)로 구성된다.

단말기는 물리적인 특징을 담당하는 하드웨어와 하드웨어를 관리하는 다수의 소프트웨어 그리고 OMA DM 서버와 상호작용을 통해 소프트웨어의 유지, 보수, 관리 및 펌웨어 업데이트 등의 작업을 수행하는 단말기 관리 에이전트로 구성된다. 관리 서버는 관리 에이전트와 주기적으로 통신하며 관리 에이전트의 요구 사항에 응답 또는 처리를 담당하는 원격지에 위치한 단말기 관리 서버를 말한다. 단말기 관리 에이전트를 통한 소프트웨어의 관리는 각 소프트웨어의 관리 객체를 추가, 수정, 삭제함으로써 이루어진다.

단말 관리 에이전트와 관리 서버 간에는 OMA DM 프로토콜로 전송하며 XML을 기반으로 하는 SyncML을 사용하여 데이터동기화를 한다.

관리 서버는 OMA DM에서 제공하는 관리명령(GET, ADD, DELETE, REPLACE, EXEC)을 사용하여 원격으로 단말의 설정값을 관리하는 기능뿐만 아니라 원격 소프트웨어 다운로드, 펌웨어 업데이트, 오류진단 및 보고기능을 제공한다.

4.4 SCMDM

SCMDM(System Center Mobile Device Manager) [9]은 MS사의 모바일 단말기 관리 기술로서 단말기 관리, 보안 관리, 모바일 VPN 기능을 제공한다. 하지만 플랫폼 종속적이어서 윈도우 모바일 기반의 기기에서만 적용 가능하므로 스마트폰 관리에 일반적으로 적용될 수 없다.

스마트폰 악성코드 관리를 위해 위의 4가지 기기 관리 기술들을 분석한 결과, 다음과 같은 이유로 OMA DM이 가장 적합하다는 결론을 내릴 수 있다.

- OMA DM은 모바일 단말기 관리에 관한 세계적인 표준으로서 앞으로 더욱 확산이 예상되는 기술이며, 최근 국내외 이동통신사들과 단말기업체들도 OMA DM 표준안을 적극 반영하고 있다.
- OMA DM이 제공하는 관리 명령을 사용하여 사용자 상태보고, 설정값 관리, 소프트웨어 관리, 오류진단 및 보고 기능을 수행할 수 있다.
- OMA DM은 모바일 단말기와 같은 제한된 컴퓨팅 리소스를 가진 기기를 위해 설계된 프로토콜이다. 따라서 데스크톱 컴퓨터에 비해 상대적으로 제한된 리소스를 가진 스마트폰에 적합하다.

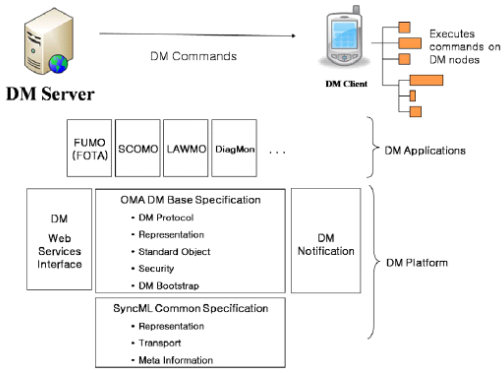
5. OMA DM 표준

5.1 OMA DM 규격

OMA는 2002년 6월 230여개의 이동통신 업체들이 참가하여 설립한 모바일 서비스 표준화단체이다. 이동통신 산업의 급속한 발전에 따라 멀티미디어, 위치기반서비스, 콘텐츠 다운로드, 메시징 서비스 등의 다양한 모바일서비스가 활성화되자 이동통신 서비스업체들은 단말이나 네트워크 및 베어러에 독립적으로 모바일서비스를 제공할 수 있는 모바일서비스에 대한 표준의 필요성을 느끼게 되었다. 이에 따라 OMA는 이동통신사업자 및 단말제조사, 솔루션업체들이 참여하여 모바일 서비스 플랫폼에 대한 표준을 제정하고 있으며, OMA규격을 기반으로 개발된 다양한 단말들 간의 호환성 및 안정성을 인증하는 Testfest도 진행하고 있다. DM은 OMA산하의 워킹 그룹 중 하나이

며 단말을 원격으로 관리하는 규격을 제정하고 있다. OMA DM 버전 1.2[10]는 2007년 2월에 표준을 완료하였으며 현재 OMA DM 버전1.3과 2.0이 표준화를 진행중이다.

OMA DM 규격은 DM서버와 단말간의 통신 프로토콜, 필수 단말 관리 객체 정의, 단말 관리 메시지의 보안 방법 등의 단말 관리에 대한 기본 규격과 그 외의 단말 관리 서비스를 위한 부가 규격으로 구성된다. 단말 관리 객체는 관리 대상이 되는 단말기의 구성요소이다. 단말 관리 객체는 트리 형태로 구성되며 트리에서 각 객체들은 노드로 표현된다[11]. 관리 객체는 가상의 트리 구조를 가짐으로써 효과적인 관리



(그림 4) OMA DM의 구조

객체의 접근을 가능하게 한다. 다시 말해, 관리 서버는 관리 에이전트를 통해 관리 트리의 각각의 노드에 해당하는 관리 객체를 개별적으로 접근할 수 있을 뿐만 아니라 상위 노드에 위치한 관리 객체의 접근을 통해 그 노드의 하위에 위치한 모든 관리 객체까지 접근할 수 있다.

5.2 OMA DM 구조

SyncML(Synchronization Markup Language) 과 OMA DM은 모바일 단말장치와 서버 간에 데이터 동기를 제공하고, OMA DM은 SyncML 에 기반하여 단말 관리(부트스트래핑, 고장 점검, 관리, 응용 및 펌웨어 신규설치 및 갱신)를 제공한다.

OMA DM의 프로토콜 구조는 (그림 4)와 같으며 전통적인 관리자-에이전트 구조를 사용하고 있다. <표 3>은 OMA DM v1.2에서 제시하고 있는 8가지 세부 스펙을 보인다.

2002년에 배포된 OMA DM v1.1.2는 <표 3>의 1~7까지의 세부 스펙을 포함한다. OMA DM v1.2에서는 이러한 요구사항에 추가적으로 XML 또는 WBXML 형태의 관리 트리를 전송하기 위한 방법에 대해 정의하고 있는 TNDS (Tree and Description Serialization)가 추가되었다.

<표 3> OMA DM v1.2에서 제시하고 있는 8가지 세부 스펙

요구사항	내 용
Bootstrap	OMA DM 서버와 단말기의 관리 세션 초기화 절차 및 이에 필요한 프로파일에 대한 정의
Notification Initiated Session	단말기의 에이전트에게 세션 시작 요청을 보내기 위한 절차와 메시지에 대한 정의
Protocol	SyncML Representation Protocol 을 사용하는 관리 프로토콜과 관리 절차에 대한 정의
Representation Protocol	OMA DM 서버와 에이전트가 서로 상호 교환하는데 필요한 모든 XML 메시지에 대한 정의
Security	일반적인 보안, 전송 계층 그리고 어플리케이션 계층에 대한 보안 요구 사항에 대한 정의
Standardized Objects	모든 OMA DM에 적합한 단말기들에게 필수적인 관리 객체에 대한 정의
Tree and Description	관리 객체를 트리 구조로 구성한 관리 트리와 관리 트리의 노드 속성을 기술하기 위해 필요한 방법에 대한 정의
Tree and Description Serialization	관리 트리의 부분 또는 전체를 XML 또는 WBXML 형태의 바이트 스트림을 전송하기 위한 방법에 대한 정의

6. 단말 관리 시스템 설계

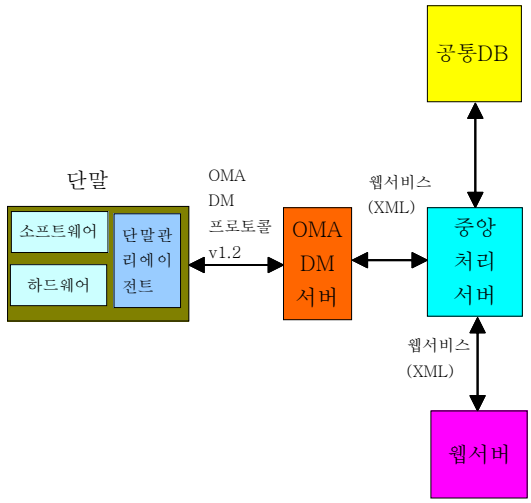
4장에서 살펴본 바와 같이 여러 단말 관리 기술 중 OMA DM이 스마트폰 관리에 가장 적합한 것으로 판정되었으므로 스마트폰의 악성코드를 원격으로 제거할 수 있는 단말 관리 시스템을 OMA DM 기술을 기반으로 하여 설계한다.

6.1 시스템의 구조

단말 관리 시스템은 (그림 5)와 같이 단말 관리 에이전트, OMA DM 서버, 중앙 처리 서버, 공통 DB, 웹 서버 등 다섯 부분으로 구성된다.

단말 관리 에이전트는 OMA DM 서버와 상호작용을 통해 단말 소프트웨어의 유지, 보수, 관리 및 펌웨어 업데이트 등의 작업을 수행한다. OMA DM 서버는 관리 에이전트와 주기적으로 통신하며 관리 에이전트의 요구 사항에 응답 또는 처리를 담당하는 원격지에 위치한 단말기 관리 서버를 말한다. 단말기 관리 에이전트를 통한 소프트웨어의 관리는 각 소프트웨어의 관리 객체를 추가, 수정, 삭제함으로써 이루어진다.

OMA DM 서버는 단말 관리 에이전트와 OM A DM의 SyncML과 OMA DM 프로토콜1.2를 이용하여 통신하며 특정관리 기능을 요청하여 응답을 받아 이를 웹 서비스로 변환하여 중앙 처리 서버로 보내주는 역할을 한다. OMA DM서버는 웹을 이용하고 있는 운영자 혹은 관리정책에 따른 중앙 처리 서버로부터 관리 명령을 받으면 관리 명령을 수행하기 위해서 단말 관리 에이전트로 통지 메시지를 전송한다. OMA DM 서버는 중앙 처리 서버와 단말 사이에서 OMA DM 프로토콜과 웹 서비스 연동 XML로 변환을 담당하는 서버이다. OMA DM 서버는 전송된 관리 명령을 처리하기 위해서 단말 관리 에이전트로 관리를 위한 세션을 초기화 한다. 중앙 서버와의 웹 인터페이스는 DM명령 요청 처리 기능, DM 명령에 대한 결과 처리 기능 , 성능 및 이벤트 정보전송에 따른 응답처리기능 등으로 분류할 수 있다.



(그림 5) 단말 관리 시스템 구성도

중앙 처리 서버는 OMA DM 서버로부터 온 정보 및 이를 가공한 내용을 DB서버에 저장하거나 웹 서버로 전송한다. 중앙 처리 서버는 모든 관리 기능에 대한 처리를 담당하는 서버이다. OMA DM 서버로부터 전송된 DM 명령의 결과 및 성능, 이벤트 정보 들을 공통DB로 저장하거나 웹 서버로 정보를 전송한다.

공통 DB는 단말로부터 전송되었거나 또는 중앙 처리 서버에서 가공된 정보들을 저장한다.

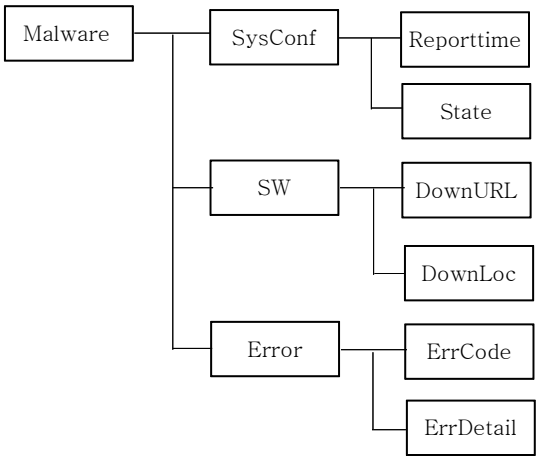
웹 서버는 운영 단말에 접속하여 스마트폰 단말 관리 명령을 수행하고 처리 결과를 확인한다. 웹 서버는 웹을 통해 접속하는 운영자에게 단말들에 대한 현황, 원격 단말 정보 조회 및 원격 관리 기능, 성능 및 이벤트에 대한 통계 정보, 관리 서버들에 대한 실시간 감시 등의 기능을 제공해 준다.

6.2 관리 객체 정의

단말 내 관리 객체는 트리 형태로 구성되며 (그림 6)과 같이 정의한다. (그림 6)의 노드 중 자식 노드가 없는 리프 노드(leaf node)만이 실제 설정값을 가지며 각 리프 노드들이 나타내는 단말 내 설정값은 다음과 같다.

・Reporttime : 단말 상태 전송 주기

- State : 단말 상태
- DownURL : 다운로드할 소프트웨어가 저장 되어 있는 외부 서버의 주소
- DownLoc : 다운로드 된 소프트웨어가 저장 되어 있는 단말 내 위치
- ErrCode : 단말 내 발생한 악성코드의 종류
- ErrDetail : 단말 내 발생한 악성코드의 세부 내용



(그림 6) 트리 형태의 악성코드 관리 객체

6.3 단말 상태 보고

단말 상태 보고는 정기적으로 이루어지며 단말 내 타이머가 (그림 6)의 노드 ./Malware /SysConf /Reporttime에 설정된 상태 보고 주기에 도달하면, DM 에이전트가 실행되게 하면 된다. DM 에이전트는 실행과 동시에 DM 서버에게 단말 관리를 요청한다. 이때 OMA DM 패키지 교환 절차[12]에 의하여 관리 요청 패키지인 패키지#1이 사용되며 패키지#1에는 단말정보와 에이전트 인증 정보가 포함되어 있다. 패키지#1에 단말 상태를 나타내는 ./Malware / SysConf/State노드의 값을 Replace 명령과 함께 전송하면 상태 보고를 할 수 있다.

6.4 단말 관리

6.4.1 악성코드 진단 및 보고

단말 내 악성코드로 인한 하드웨어적 오류 또는 소프트웨어적인 오류가 발생하면 Error노드의 자식 노드인 ErrCode와 ErrDetail 노드가 동적으로 생성된다. 이때 DM 에이전트는 관리 서버에게 관리를 요청한다. 패키지 #1에 ./Error/ErrCode와 ./ Error / ErrDetail 노드의 값을 Replace 명령과 함께 전송하면 악성코드 발생 보고를 할 수 있다.

6.4.2 소프트웨어(백신) 관리

단말 내에 악성코드가 발견되면 관리 서버는 백신을 다운로드할 수 있는 주소를 DM 에이전트에 알려준다. 이를 위해 관리 서버는 다운로드할 주소정보를 나타내는 노드 ./Malware /SW/DownURL을 DM 에이전트의 트리에 추가하기 위한 Add 명령을 전송한다.

DM 에이전트는 ./Malware/SW/DownURL 노드가 트리상에 추가되면 자동으로 해당 노드의 값이 나타내는 주소에 접속하여 백신을 다운로드한다. 다운로드가 완료되면 다운로드된 백신의 단말 내 위치를 ./Malware/SW/DownLoc에 설정하고 다운로드된 백신을 설치한다. 다운로드 및 설치가 완료되면 관리 서버에게 결과를 보고한다.

7. 결 론

스마트폰 대중화시대의 도래는 생활의 편리함과 서비스 시장형성 및 산업활성화의 기반이 되지만, 한편으로 새로운 보안 위협의 등장을 초래했다.

본 논문에서는 스마트폰 보안 위협 요소인 모바일 악성코드의 발생현황을 살펴보고 이에 대응하기 위한 단말 관리 시스템을 설계하였다. 본 논문에서 설계한 스마트폰 단말 관리 시스템은 OMA DM을 이용함으로써 SNMP 및 TR-069를 이용한 경우에 비해 더 안정적이고 관리 세션에 대한 높은 보안으로 관리 기능을 수행할 수 있다.

향후에는 성능평가를 통해 단말 관리 시스템의 처

리능력을 측정해 보고 효율적인 관리기능을 제공하기 위한 시스템의 최적화 방안을 연구해야 할 것이다.

참고문헌

[1] 방송통신위원회, 보도자료, “스마트폰 가입자, 1000만 돌파, 스마트시대 본격 개막”, 2011년 3월 24일

[2] 심재홍, “모바일 인터넷 정보보호를 위한 모바일 악성코드 분석”, 정보보호학회지, 제19권, 제6호, pp.41-48, 2009.

[3] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안기술”, 정보보호학회지, 제19권, 제5호, pp.21-28, 2009.

[4] 강동호 외 6인, “스마트폰 보안 위협 및 대응 기술”, 전자통신동향분석, 제25권, 제3호, pp. 72-80, 2010.

[5] D. Maslennikov, "Mobile Malware Evolution : An Overview, Part4", http// www. securelist. com/en/analysis?pubid=204792168, KasperskyLab , Mar.2011

[6] Juniper Networks, “Malicious mobile threats report 2010/2011", http://globalthreatcenter .com/?p=2280

[7] 안철수연구소, “안드로이드 악성코드 폭발적 증가세”, http://blog.ahnlab.com /ahnlab /1185

[8] OMA Device Management, http:// www .openmobilealliance.org

[9] Microsoft System Center, http://technet .microsoft. com/en-us/ systemcenter / mdm /default. aspx

[10] OMA Device Management v1.2, http://www .openmobilealliance.org /technical/ release_program/dm_v1_2.aspx

[11] OMA Device Management Tree and Description, http://www.openmobilealliance.org, OMA-TS-DM TND-v1 2 1-20080617-A.pdf

[12] 박주건, 박기현, “유비쿼터스 환경에서 개인건강기기를 위한 원격관리시스템 구축”,정보과학회지, 제29권, 제1호, pp72-82, 2011.

[저 자 소 개]

정 기 석 (Gi-seog Jeong)

1983년 2월 고려대학교 전자공학과 학사
1988년 8월 고려대학교 전자공학과 석사
1992년 8월 고려대학교 전자공학과 박사
현재 영동대학교 정보통신보안학과 교수

email : gsjeong@yd.ac.kr