모바일 환경에서의 보안위협 분석

정연서 · 김기영
한국전자통신연구원

Threat Analysis of Mobile Environment

Youn-Seo Jeong . Ki-Young Kim
Dept. of Network Security Research, ETRI
E-mail : jys847@etri.re.kr

요 약

1986년 컴퓨터 바이러스가 발견된 후, 매년 새로운 바이러스들이 나타나고 있다. 최근에는 모바일 기기(휴대폰, PDA)들을 대상으로 하는 악성코드(바이러스, 웜, 트로이목마)들이 발생하고 있다. 향후 모바일 기기의 보급과 업무 활용이 증가함에 따라 이에 대한 대비가 필요하다. 본 논문에서는 악성코드들의 종류와 특징들을 조사 분석하고 모바일 환경에서의 보안 고려사항들을 살펴본다.

ABSTRACT

Since the appearance of the first computer virus in 1986, a significant number of new viruses has appeared every year. Recently, there has been a marked increase in the number of mobile malicious code(virus, worm, trojan) in Mobile devices(smart phone, PDA). As a growing number of people use mobile device, we have to prepare for coming mobile attacks.

In this paper, we study trends and characteristics of mobile malicious code. And, we describe considerations of on-device and network security in mobile environment.

키워드

모바일 보안, 모바일 바이러스

Ⅰ. 서 론

최근 휴대폰, PDA 등과 같은 모바일 기기들의 해킹위협에 대한 경고들이 강조되고 있다. 가트너(2005) 자료에 따르면 휴대폰과 스마트폰을 포함해 판매된 모바일 기기는 8억 1200만대로 나타나고 있으며, 오는 2008년 연간 모바일 장치의 수요는 10억대를 넘어설 것으로 예상하였다.

IDC의 조사에서도 2004년 이동단말을 사용하는 사람들의 수가 6억5천만명에 달하고 있으며 2009년에는 8억5천만명에 이를 것으로 예측하였다. 이동단말을 사용하는 이동직원수의 증가는 모바일 장치 수요의 증가를 가져오게 된다.

2000년 1월 노르웨이에서 특정 SMS가 일부 노키아 휴대폰에 전달되어 휴대폰의 동작을 정지시키는 오동작을 일으킨 이후 현재까지 200여건의 휴대폰용 모바일 악성 코드들이 발견되었다. 이는 PC용 바이러스의 증가와 비교하여 볼 경우 빠른 속도로 전개되고 있음을 알 수 있다. 최근 DMB, Telemetics, Wibro 등의 서비스 도입들과 발맞추어 다양한 유비쿼터스 환경으로 접어듬에 따라 더욱 더 모바일 환경에서의 보안대책 마련이 필요하다.

본 논문에서는 휴대폰과 PDA 등을 대상으로 하는 모바일 악성 코드들의 종류와 특징, 피해 등을 조사 분석하고 향후 다가오는 모바일 환경에서의 보안고려사항들을 제시한다. 2장에서는 현재

모바일 악성코드에 대해서 기술하고, 종류와 피해들을 분류한다. 3장에서는 이에 대한 모바일 환경에서의 보안 고려사항들을 기술한다.

II. 모바일 환경에서의 악성코드

1. 악성코드 분류

일반적으로 컴퓨터 바이러스라 부르는 것은 크게 바이러스와 트로이 목마, 웜으로 분류한다.

바이러스는 자기 복제 능력을 가진 일종의 프로그램으로 다른 프로그램의 코드를 수정하여 바이러스 코드를 그 안에 포함하는 형태를 가지며 대부분 악의적인 목적을 가지고 제작된다. 부팅 불능, 파일 손실, CMOS 파괴, 디스크 손상과 같은 피해를 일으킬 수 있다.

트로이 목마는 자체적인 자기 복제 능력은 없는 악의적인 목적의 프로그램으로 사용자 모르게 설치되어 문제를 발생시킨다. 유용한 프로그램으로 가장하여 시스템 자원에 접근하거나 파일을 파괴한다. 대표적으로 Back Oriffice와 같은 것이 있다.

웜은 자기 복제를 하지만 바이러스와 다른 점은 특정한 감염 대상을 지니지 않는다. 바이러스의 경우 COM이나 EXE와 같은 특정 파일에 감염되지만 웜은 그러한 성격을 가지지 않으며 웜 자체가 다른 PC로 전파된다. 그러나 이러한 구분은 명확하게 적용시키기는 어렵고 근래의 악성코드들은 각각의 특성들을 다 갖추고 있는 경우도 빈번하다.

2. PC환경에서의 악성코드

PC 환경에서 처음 바이러스가 나타난 것은 1986년의 일이다. 파키스탄에서 프로그램의 무단복제 사용에 대한 불만으로 제작, 유포된 브레인 바이러스를 시작으로 20여년이 지난 현재는 형태와 종류에서 그 수를 헤아리기 어려울 정도로 생겨났다. 그 대상 운영체제도 DOS, Windows, UNIX, Linux, MAC 등으로 다양해졌으며 공격 대상도 컴퓨터에서 네트워크, 인터넷으로 확산되었다. 주요 악성코드와 특징들은 다음과 같다.

- 1986. 파키스탄에서 첫 컴퓨터 바이러스인 브레인 바이러스 발견.
- 1987. 예루살렘 대학에서 13일의 금요일에 맞춰 실행되는 예루살렘 바이러스 발견.
- 1999. 4. CIH 바이러스가 하드디스크 바이오스(BIOS)를 손상시키고 파일을 삭제하는 등 막대한 피해를 입힘. 이외에도 워드 문서에 첨부되어 메일로 자동 발송되는 멜리사 바이러스 등장.
- 2000. 아웃룩 주소로 자동 발송되어 JPG, DOC 등의 파일 손상을 일으키는 러브레터(Loveletter) 웜, 아웃룩 주소로 자동 발송, 감염되면 눈 모양의 아이콘이 생기는 나비다드(Navidad) 웜 등 등장
- 2001. 아웃룩 주소로 자동 발송되어 EXE 파일을 손상시키는 님다(Nimda) 웜, 자체 SMTP를 이용해 메일로 발송되며 C드라이브 파일과 폴더를 삭제하는 서캠(Sircam) 웜 등 출현.
- 2003. 1. 25 인터넷 대란을 일으킨 SQL_Overflow (일명 슬래머) 웜 등장, 이후 8월에는 1, 2분 간격으로 컴퓨터를 강제 재부팅 시켜서 큰 피해를 발생시켰던 블래스터 웜(Blaster worm), 웰치아 웜(Welchia worm), 엄청난 양의 스팸 메일을 발송하는 소빅.F 웜(Sobig.F worm) 등 출현
- 2004. 마이둠 웜(Mydoom)은 1월 26일 처음 등장해 역대 최고의 전파속도로 세계적으로 100만대 이상의 PC를 감염시킴. 이외에도 넷스카이(Netsky), 베이글(Bagle), 새서(Sasser) 웜 등이 지속적으로 변종을 등장시키며 악명을 떨침.

3. 모바일 환경의 악성코드

모바일 환경에서의 바이러스는 향후 큰 위협으로 꼽히고 있다. 아직은 특정 플랫폼의 PDA와 휴대폰을 그 대상으로 하고 있으나, 컴퓨터 바이러스와 함께 컴퓨터 바이러스의 파괴적 방식을 모방하는 악성 프로그램들이 빠른 속도로 증가하고 있다.

3.1 모바일 악성코드

2000년 노키아 휴대폰에 나타난 SMS 바이러스 이후 200여개의 휴대폰용 악성코드들이 발견되었다.

- 2000. 1. 특정 SMS가 일부 노키아 휴대폰에 전달되어 휴대폰 오동작
- 2000. 6. 스페인 텔레포니카사 이용자들에게 스팸 메일 발송, 회사 GSM 게이트웨이로 대량의 메일 발송, 동작방해
- 2001. 2. NTT 도코모의 i-Mode SMS 발송으로 대량의 전화시도, 불통
- 2004. 6. Cabir.A - 자기 복제와 전파 능력을 가진 최초의 웜, 블루투스를 이용하여 전파, 후에 변종 다수 출현
- 2004. 11. Skulls.A - 감염된 휴대폰의 아이콘을 해골로 변경, 동작 정지, 블루투스를 통해 전파

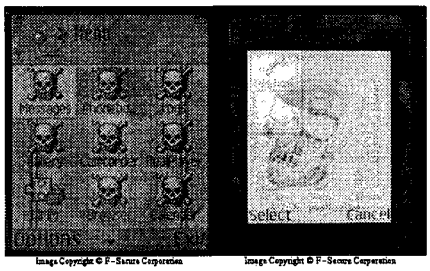

그림 2-1 Skulls 감염화면

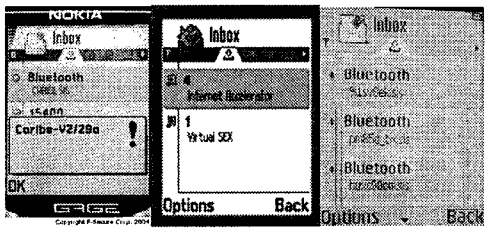

그림 2-2 Cabir 감염화면

주요 모바일 악성코드와 특징들은 다음과 같다.

- Cardtrap.A - Trojan, Symbian, 2005.9.20, PC와 이동 단말기 통합 바이러스, 단말기 메모리카드에 의해 감염, 실행시 PC에 백도어 설치, PC 패스워드 등 유출
- Cabir.A - Worm , Symbian, 2004.6.15 , 다양한 변종, 블루투스를 이용 SMS 발송, 휴대폰 배터리 소모
- Skulls.A - Trojan, Symbian, 2004. 11.19, 기존의 아이콘을 스컬스(해골) 이미지로 변경, 감염된 파일을 다운로드하여 실행시 감염
- CommWarrior.A - Worm, Symbian, 2005.3.7, 감염시 MMS(Multimedia Message Service) 발송, MMS, 블루투스 이용, 주변전파 - 확산위협 높음
- Redbrowser.A - Trojan, J2ME, 2006.2.27, 유용한 프로그램으로 위장 유포, 감염시 SMS 다수 발송
- Liberty - Virus, Palm, 2000.1.8, 파일 실행시 메모리 적재 프로그램 삭제, 모든 프로그램 삭제됨
- Phage - Virus, Palm, 2000.1.9, 메모리 적재된 모든 프로그램 실행중단
- Vapor - Trojan, Palm, 2000.1.9, 모든 아이콘 삭제됨
- Brador - Backdoor, WinCE, 2004. 6, 감염시 제어권을 상실하며, 바이러스 배포자가 기기를 제어가능, 전화 및 기타 기능들을 마음대로 이용

3.2 모바일 악성코드 분석

모바일 악성코드들은 대부분이 Nokia의 Symbian 플랫폼(96.5%)을 대상으로 하고 있으며, Trojan 형태의 코드(77%)들이 주를 이루고 있다. 모바일 악성코드들은 아직까지는 크게 피해를 발생시키거나 확산된 경우는 없으며, 실제 많은 수의 개념 증명 바이러스(연구실 제작 실험바이러스)들이 목록에 등록되어 있다. Symbian을 대상으로 하는 것들 이외에는 Palm과 WinCE 대상의 코드들이 소수 보고되어 있었으며 최근에는 자바플랫폼(RedBrowser.A)을 대상으로 하는 코드도 보고되어 있다. 이외에도 최근 단말기(Symbian)의 사용내역(주소록, 통화내역 등)을 원격서버로 전달해 주는 프로그램(FlexiSpy)도 소개되어 있다.

표 2-1 모바일 바이러스 통계(F-SECURE, 2006.4 현재)

플랫폼	갯수	악성코드	갯수
Symbian	193	Virus	11
Palm	3	Worm	33
PocketPC	3	Trojan	154
J2ME	1	etc	1
계	200	계	200

악성코드들의 수는 많으나 대부분 특정 코드들의 변종들이 보고되고 있으며 현황은 다음 표 2-2와 같다.

표 2-2 주요 모바일코드의 변종(F-SECURE, 2006.4 현재)

코드명	특성	종류	수	비고
Cardtrap.	Trojan	A ~ AF	32(16%)	
Cabir	Worm	A ~ AD	30(15%)	Worm, Virus, Trojan으로 변형
Skulls	Trojan	A ~ V	22(11%)	
Cdropper	Trojan	A ~ N	14(7%)	
Doomboot	Trojan	A ~ M	13(6.5%)	
Commwarrior	Worm	A ~ H	8(4%)	
계			119(59.5%)	전체 200개

현재 나타난 모바일 바이러스들의 감염경로와 피해 유형들을 정리하면 아래와 같다.

- 감염경로
  - PC와의 동기화시 감염
  - 통신에 의한 감염
    - Bluetooth, IrDA

- 네트워크 연결에 의한 감염
  · Internet 접속을 통한 감염
  · Contents download에 의한 감염
- Memory card에 의한 감염
- SMS, MMS에 의한 감염
  · 첨부파일, 첨부 프로그램 설치

• 피해 유형
- 개인 정보 변경, 삭제, 유출
  .주소록, 개인 데이터, 전화번호, 사진 등 유출
  .통화 내역 유출
- 프로그램의 임의 변경
  .프로그램 변경, 삭제
- 이상동작
  .특정 사이트 접속, 사용료 부가
  .통화방해, 성능저하, 리소스 소모
- SMS, MMS 발송
  .다량의 SMS, MMS 발송, 요금 부가
- 원격제어
  .원격에서 기능을 자유자재로 이용, 요금 부가

3.3 모바일용 보안제품

모바일용 악성코드들에 대한 보호를 위해 현재 국외 F-secure, Symantec, MacAfee, TrendMicro 등에서 모바일 휴대폰, PDA 등을 위한 백신을 제공하고 있으며, 국내에서는 안철수연구소에서 WIPI용 모바일 바이러스 백신을 제공하고 있다.

III. 모바일 환경의 확대와 보안 고려사항

1. 모바일 환경의 확대

현재 휴대폰의 경우 시장현황은 표 2-3과 같다. 현재 모바일 악성코드들은 앞에서 조사한 바와 같이 Nokia의 플랫폼인 Symbian을 주 대상으로 발견되고 있다.

표 3-1휴대폰 시장점유율

회사	시장점유율
SAMSUNG	13%
LG	6%
NOKIA	32%
MOTOROLA	15%
SONYERICSON	6%
SIMENS	7%
ETC	21%

향후 유비쿼터스 환경으로 전개되고 국내에서는 신규서비스(Wibro, DMB, 텔레매틱스)들이 실시 확대될 전망이며, 이러한 서비스들의 진행과 맞추어 단말기의 요구와 개발이 있을 것이다. 이외에도 Wireless AP, Router, PDA, Handheld Computer, VOIP phone, Robot, Audio/video entertainment devices, Tablet, Webpad, ThinClient, WebCAM 등의 다양한 분야에서 임베디드용 기기들이 필요하다. 서론에서 조사기관들의 자료에서 본 바와 같이 점차 모바일 환경에서의 작업이 늘어나고 좀 더 다양하고 강력한 기능들을 갖춘 이동단말기들이 요구/개발될 것이다. 현재 휴대폰 단말기 제조사들의 경우 새로 출시되는 단말기들의 플랫폼(Smart Phone)으로 Open Source인 Linux(Embeded Linux)를 탑재하고 있으며, 셋톱박스나 로봇, 가정용 백색가전 제품들에도 적용되고 있다. PC환경에서와 같이 공통 플랫폼 환경이 조성되고 휴대용 임베디드 기기들의 네트워크 사용이 확대된다면 지금까지의 미비한 공격들과는 달리 1.25 인터넷 사태와 같은 큰 문제가 발생될 수 있다.

2. 모바일 환경에서의 보안

현재 PC환경의 보안 상태와 향후 모바일 환경을 예측하여 비교하여 보았다. PC환경에서는 네트워크의 연결과 인터넷의 사용 확대로 인해 급속도로 악성코드들의 종류와 수가 늘어났으며, 향후 개인 사용자들이 네트워크 연결확대로 인해 그 피해도 심각해지게 될 것이다.

표 3-2 PC 보안환경 vs. 모바일 플랫폼 보안환경

	PC	모바일 플랫폼
디바이스 보안	Personal Firewall, Anti-spyware, Virus vaccine IPS(Host based), SecureOS	Secure Embeded OS, Embeded Firewall Mobile Virus vaccine Anti-Spyware
네트워크 보안	Firewall, IDS, IPS(Network based)	Firewall, IPS(Network based)
운영시간	개인용 - 필요시 서버용 - 상시	상시
피해 유형	정보유출, 서비스 마비, 시스템 손상, 전체 망 마비	정보유출, 단말기 손상, 통신요금부과, 전체망 마비
사용용도	개인용, 서버용	개인용
접속환경	유, 무선	무선
운영체제	Windows, Linux, UNIX	Linux, WinCE, Palm, Symbian, VxWorks, VRTX, pSOS 등

모바일 환경은 점차 유선환경을 대체해 갈 것으로 전망되며, 각 용도와 기기의 특성에 따라 자원(Resource)이 제한적이지만 현재 사용하는 개인용 컴퓨터들과 유사한 수준의 고성능의 기기들도 요구되

고 있으며, 휴대의 간편성과 이동성으로 인한 모바일 기기들의 네트워크 이용 트래픽의 양은 기존의 유선망 트래픽을 초과할 날도 오게 될 것이다.

다음에서 모바일 환경에서의 고려사항들을 보안측면에서는 크게 두 가지 경우로 나누어 정리하였다. 자체 플랫폼에 대한 보안(On-device)과 망 차원(Network)의 보안이다. PC 환경에서와 마찬가지로 단말과 자원에 대한 접근통제와 유해코드의 탐지 및 차단, 바이러스 백신과 스파이웨어 탐지 및 제거 APPLICATION 들의 개발이 필요하다. 그리고, PC와는 달리 단말의 이동성/개인성으로 인한 단말 자체의 분실에 대비해 저장된 주요 데이터들의 암호화 기능이 필수로 요구되며 안전한 통신을 위한 통신채널의 확보도 필요하다. 차후, 사용 환경의 확대와 더불어 필요에 따라서는 단말의 사용기록들을 저장하고 분석하는 기능(Forensic)도 추가되어야 할 것이다. 여러 가지 고려사항들을 정리하면 다음과 같다.

On-device 보안 :

- 암호화 기능 필요
- 접근통제 기능 필요(Access Control, Authentication, 외부로부터의 장비 사용 및 자원에 대한 접근제어)
- 유해패킷 탐지 및 차단 기능 필요(IPS, IDS)
- 유해코드 탐지 및 제거(Anti-Virus, Anti-Spyware)
- Embeded Forensic 필요(로그기록, 해석 기술)
- 보안성이 강화된 플랫폼 필요(Embeded Platform)
- 기능들의 모듈화 설계(기기별 리소스에 따른 기능 선택 가능)

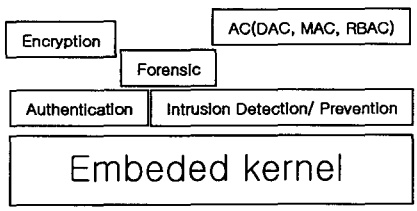

그림 3-1 모바일 플랫폼 보안(On-device)

Mobile Network 보안 :

- 모바일 망의 인입점에서 망 차원의 보안관리 및 관리 프레임워크 필요(Update, Monitoring 등)
- 모바일 망용 보안장비 필요(Firewall, IPS, IDS, Viruswall 등)

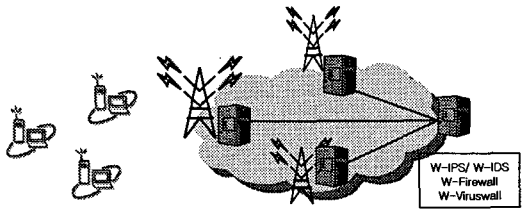

그림 3-2 모바일 네트워크 보안(Network)

Ⅳ. 결 론

모바일 환경은 이제 새로운 작업환경으로 다가오고 있다. 새로운 서비스의 도입에 따라 단말들의 요구/출시가 기대되고 공통플랫폼으로의 전이가 진행되고 있다. 모바일 환경에서는 개인들의 주요한 데이터들과 업무와 관련된 직무 데이터들이 유출/손실되고, 원치 않는 사용으로 인한 통신요금 부과 등 금전적 피해도 뒤따르며, 모바일망의 트래픽으로 인해 전체 네트워크가 마비되는 경우도 발생할 수 있다.

본 논문에서는 현재 휴대폰(Smart Phone) 환경에서의 모바일 악성코드들을 조사하고 이를 분석하였다. 이를 바탕으로 차후에 다가올 모바일 환경에서 고려해야 할 점들을 단말기 측면과 망 측면에서 정리하고 제시하였다.

참고문헌

[1] F-Secure Mobile Threats, http://www.f-secure.com/wireless/threats/
[2] Linux Device, http://www.linuxdevices.com
[3] 강정민 외 3인, "리눅스 커널 보안동향," 한국정보보호학회지, 15권 2호, 2005. 4
[4] 윤민홍외 4인, "스마트폰용 임베디드 리눅스 솔루션," 전자통신동향분석, 21권 1호, 2006. 2
[5] 김재영외 4인, "차세대임베디드 시스템을 위한 소프트웨어 플랫폼 현황 및 동향," 전자통신동향분석, 21권 1호, 2006. 2