JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 17, No. 8 : 1835~1841, August. 2013

PC를 이용한 스마트폰 악성코드 대응

윤풍식[1] · 한승조[2*]

Response Guide of Smart-Phone Malware Using PC

Poong-sik Yoon[1] · Seung-jo Han[2*]

[1] Department of Information and Communication Engineering, Chosun University, Gwangju 501-759, Korea
[2] Department of Information and Communication Engineering, Chosun University, Gwangju 501-759, Korea

요 약

스마트폰 사용자가 증가함에 따라 스마트폰 악성코드, 좀비 스마트폰등의 스마트폰을 겨냥한 공격이 증가하고 있다. 스마트폰에 대한 보안은 PC보안 보다 더 취약하며, 스마트폰에 대한 공격은 날이 갈수록 다양해지고 있으며 좀비 스마트폰의 경우 좀비 PC보다 심각한 문제를 야기시킨다. 본 논문에서는 PC에서 DDoS 공격과 스마트폰 DDoS공격 및 악성코드를 비교 분석하고 데이터망에 접속하여 서비스를 이용할 때 이용자가 직접 스마트폰의 패킷을 확인하는 방법과 스마트PC폰에 대한 악성코드들을 PC를 이용하여 탐지 하는 방법에 대해 제안하며 스마트폰 DDoS 공격과 악성코드에 관한 대응책을 제시한다.

ABSTRACT

With the increase in smartphone users, attacks targeting smartphone malware, zombie smartphone, such as smart phones is increasing. Security of smart phones is more vulnerable than PC security, for a zombie smartphone and generates a serious problem than the zombie PC attack on the smartphone every day is diversification. In this paper, the comparative analysis of malicious code and smartphone DDoS attacks and DDoS attacks from the PC, When using a service by connecting to the data network, proposes a method for users to confirm the packet smartphone direct a method for detecting by using the PC malware Smart PC Phone. Propose the measures of malicious code and smartphone DDoS attacks.

키워드 : 스마트폰 보안, 스마트폰 DDoS, 좀비 스마트폰, 스마트폰 악성코드

Key word : SmartPhone Security, SmartPhone DDoS, Zombie SmartPhone, SmartPhone MalignantCode

접수일자 : 2013. 05. 07 심사완료일자 : 2013. 05. 21 게재확정일자 : 2013. 06. 07

*** Corresponding Author** Seung-Jo Han(E-mail:sjbhan@Chosun.ac.kr, Tel:+82-62-230-7069)
Department of Information and Communication Engineering, Chosun University, Gwangju 501-759, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2013.17.8.1835 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

현재 스마트폰 이용자수는 전체 모바일 이용자에 대부분을 차지하고 있으며 3G망 혹은 Wi-fi망을 이용하여 무선인터넷을 이용하고 웹에 접속이 가능하게 되었다. 스마트폰이나 태블릿PC등 언제 어디서나 웹에 접속할 수 있는 모바일 디바이스들은 보안 측면에서 볼 때 위협적인 존재이다. 2011년 기준 스마트폰 이용자는 꾸준히 증가하고 있는 추세이며 스마트폰 이용자가 2000만명이 넘어섰다. 이러한 스마트폰의 대중화로 모바일이나 클라우드 컴퓨팅이 화두 되고 있고 이로 인해 보안이 이슈가 되고 있지만, 정작 이를 해결할 수 있는 보안 솔루션은 많지 않다. 현재 이러한 스마트폰이나 태블릿PC에 대한 보안 대책으로 모바일 통합 보안 관리 및 정보 유출방지 솔루션이 개발되어 지고 있으며 서비스하고 있는 솔루션도 등장하였다 [1].

하지만 스마트폰 사용자 모두가 이러한 보안 솔루션을 사용하는 것은 아니며 아이폰의 경우 탈옥, 안드로이드 기반 스마트폰의 경우는 루팅을 시도하여 허가되지 않은 어플리케이션을 다운받고 이를 설치함에 따라 많은 피해가 발생 되어지고 있다.

DDoS공격으로 인한 웹사이트의 마비 이외에도 악성코드를 사용자의 스마트폰이나 태블릿PC에 삽입하여 음성녹음 기능을 이용한 도청이나 사용자의 개인정보 유출 등 여러 가지 피해사례가 발생 되었으며 사용자는 위험에 노출되어 있다. 또한, 일반적으로 사용하는 PC의 경우는 사용자가 일정시간 사용을 하고 전원을 차단하는데 비해 스마트폰이나 태블릿PC의 경우에는 거의 24시간 전원이 켜져 있고 배터리가 떨어진 경우에는 충전기를 연결하여 사용하거나 새로운 배터리로 교체하여 지속적으로 전원을 유지하기 때문에 기존 좀비 PC를 이용한 DDoS공격에 비해 보다 더 큰 피해가 발생되고 3G혹은 Wi-fi를 이용하기 때문에 통신망 자체에 장애가 올 수도 있다.

본 논문에서는 기존의 DDoS공격 및 스마트폰 DDoS 공격의 공격 기법과 스마트폰 DDoS 악성코드에 대한 대비책을 분석하고, 2장에서는 PC에서와 스마트폰에서 DDoS공격과 악성코드 공격에 대해 고찰하고, 3장에서는 이에 대한 대응방법을 기술하고, 4장에서는 패킷 캡쳐와 PC를 이용하여 스마트폰 악성코드를 탐지하는 방법을 제안하고 5장에서는 결론을 제시한다.

Ⅱ. 본 론

2.1. Botnet

Botnet은 Bot Master에 의해 원격으로 조정되어지는 각종 악성행위를 수행할 수 있는 수많은 악성 소프트웨어인 Bot에 감염된 컴퓨터들이 네트워크로 연결되어 있는 형태를 칭한다. Botnet은 여러 가지 기능이 있지만 그 중 가장 두드러지는 공격은 DoS(Deny of Service)이며, 웹서버의 서비스 중단, 거부뿐만 아니라 특정 프로그램의 오류, 악성 스크립트를 이용한 오버플로우 등 여러 가지가 DoS로 분류 될 수 있다.

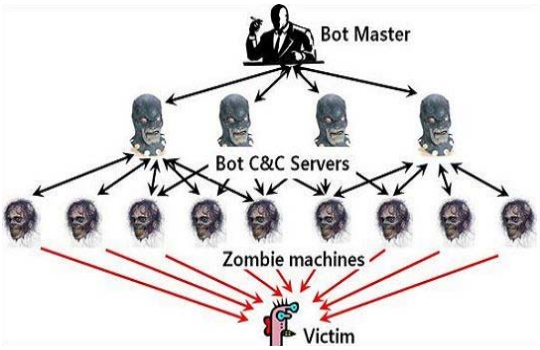

그림 1. 봇넷의 구조
Fig. 1 Architecture of Botnet

[그림 1]에서 보는 바와 같이 Botnet이 구성된다. Bot Master는 공격자이고 그 밑으로 C&C 서버들, 그리고 C&C 서버가 통제하는 Bot들이 좀비가 되며, 악성 Bot에 감염된 좀비는 Bot Master의 원격제어를 받아 특정 공격을 수행하는 형태이다. 최근 시연되기도 하였고 예상되는 스마트폰 좀비 악성코드에 의한 공격은 Botnet과 유사한 구조를 가지고 있다 [2,3].

2.2. PC에서 DDoS 공격

2.2.1. 플래그먼트 플루딩 공격(Fragment Flooding)

가장 단순하면서 강력한 공격 수단중에 하나로써, ICMP(Internet Control MessAge Protocol)를 이용하여 대량의 트래픽을 발생시키는 공격이다. 플래그먼트 플루딩 공격의 경우에는 탐지가 쉬운 반면에 이미 허용 대역폭을 넘은 공격이 시행되고 있기 때문에 이에 대한 대응이 제한적이다 [4].

2.2.2. URL 리다이렉트 우회 공격

2009년 7월 DDoS 공격시 사용되었던 대응 기법중의 하나가 URL 리다이렉트 기법이다. 최근 중국에서 사용되는 중국블루해커연맹 DDoS 공격기의 경우 302 URL 리다이렉트 신호를 인식하여 전송된 새로운 URL로 접속을 수행하여 URL 리다이렉트를 통한 대응 기법을 우회하는 특징을 지닌 공격기법이다 [5].

2.2.3. Pyloris 공격

아파치 계열 웹 서버에 적용되는 Slowloris공격 기법을 응용한 형태로 Slowloris와 같이 HTTP헤더에서 헤더의 끝을 알리는 '\r\n\r\n'을 제거한 패킷을 발송하고, HTTP GET 헤더 전체를 1 바이트씩 쪼개어 느린 속도 전송하는 공격기법이다 [6].

2.2.4. Slow HTTP POST 공격

2010년 11월 미국 워싱턴에서 개최된 2010 OWASP AppSec Conference에서 소개된 공격으로써, 웹 서버와의 커넥션을 최대한 장기간 유지하여 웹 서버가 정상적인 이용자를 받아들이지 못하게 하는 공격 방식으로 Slowloris와 유사하나, 아파치 계열과 IIS 계열 웹 서버 모두에 영향이 가능하다는 차이점이 있다. 이 공격은 HTTP 프로토콜 자체적인 문제점을 악용한 공격이다.

이 공격은 HTTP POST 메서드를 사용하여 헤더의 Content-Length 필드에 임의의 큰 값을 설정하여 전송함으로써, 웹 서버가 클라이언트에서 해당 크기의 메시지를 전송할 때 까지 커넥션을 유지하게 되고 공격자는 소량의 데이터를 느리게 전송함으로써 HTTP POST 메서드를 수용하는 모든 웹서버는 이러한 공격의 위협에 취약하다 [7,8].

2.2.5. 7.7 DDoS와 3.4 DDoS 비교

2009년 7.7 DDoS대란에 이어 2011년 3.4 DDoS공격은 파일 공유 사이트를 통하여 유포 되었으며 유포방법 역시도 자동 업데이트 되는 파일을 악성코드로 바꾸는 것과 Cache Control 공격이라는 공통점을 가진다. 두 DDoS 공격의 차이점은 7.7 DDoS는 같은 파일 구성에 의한 공격을 시행한데 반해 3.4 DDoS는 공격할 때마다 변하는 파일을 구성하여 공격하였다.

2.3. 스마트폰 DDoS 및 악성코드 공격

공식마켓을 통해 유포되는 어플리케이션도 있지만 대부분 안드로이드의 루팅이나 아이폰의 탈옥 등을 통하여 이용이 가능한 3rd-party 마켓을 통해 악성코드가 유포되는 경우가 많다. 정상 앱(App)에 악성코드를 리패키징하여 유포되어지고 DDLight 악성코드의 경우, 선정적인 이미지나 정보들에 2중 패키징된 상태로 발견되기도 하였다. 2중 패키징된 APK파일의 경우 내부에 포함되어 있는 두 번째 APK파일은 설치가 완료 되어도 특별한 실행화면이 존재하지 않지만 SMS, MMS등의 메시지 송/수신, 스마트폰의 위치정보 및 통화기록등의 단말기 정보유출의 가능성이 있으며, 이러한 악성코드의 경우 스마트폰 부팅시 자동으로 악성 어플리케이션이 실행 될 수 있다.

2.3.1. 스마트폰 DDoS 공격 시연

2011년 4월 하우리 선행기술팀에서 발표한 자료를 보면 3.4 DDoS 악성코드와 동일한 기능을 수행하는 스마트폰 악성코드를 제작 3rd-party 마켓에서 기존의 정상 앱에 악성코드를 리패키징하여 정상 앱으로 위장 유포를 하여 스마트폰 DDoS 공격 시연을 하였다. 3.4 DDoS 악성코드와 차이점은 PC백신 업데이트를 방해하는 것을 모바일 백신의 업데이트를 방해하고 인터넷망에서 사용되던 것을 3G와 Wi-fi를 이용하도록 하고 하드를 파괴하던 것을 내장 메모리를 파괴 하도록하고 3.4 DDoS 악성코드 와 가장 큰 차이점은 연락처 목록의 연락처로 SMS 문자 메시지를 이용하여 전파한다는 점이다. 시연한 악성코드는 스마트폰을 강제로 루팅시키고 개인정보(사용자의 이름, 전화번호, IMEI정보)와 위치정보(GPS)를 전송한다. 시연 시 가상의 웹 사이트를 공격 하였고 그 결과 해당 사이트는 접속이 차단되었다. 시연 결과 스마트폰 300~500대 정도면 일반 사이트 하나는 쉽게 접속을 차단 할 수 있다고 발표하였다 [9,10].

2.3.2. 스마트폰 악성코드

최근 악성코드가 진화하고 새로운 악성코드들이 등장하면서 스마트폰 혹은 PC에 제한된 악성코드가 아니라 스마트폰과 PC에 공통으로 동작한다.

PBStealer : 최초의 스마트폰 이용자 데이터를 훔치는 트로이목마형 악성코드이며, 감염된 스마트폰의 주

소록을 txt파일로 저장하여 해당 파일을 블루투스를 이용하여 전송한다.

Commwarrior : 스마트폰의 주소록을 MMS로 전송하는 악성코드이며, 사회공학적 기법을 응용한 트로이목마형 악성코드이다.

Arifat : MSN 프로그램으로 위장하여 이용자의 아이디와 패스워드를 특정 번호의 단말기에 SMS로 전송한다.

Allcano : 이용자의 스마트폰이 수신, 발신하는 SMS를 특정 번호로 전송하는 스파이웨어이며, 이 악성코드는 실행되면 프로세스를 은닉하므로 이용자는 악성코드의 실행 여부를 알 수 없다.

Android-Trojan/SmsSend : 사용자를 속이거나 사용자 몰래 문자를 전송하는 프로그램. 수신되는 문자를 확인하며 특정 형식의 문자를 전송, 수신되는 문자를 조작 또는 차단한다.

Ⅲ. 패킷 캡쳐

3.1. 패킷 캡쳐

편리한 생활을 보장 해주는 스마트폰 이지만 악성코드와 DDoS 공격에 취약하며 스마트폰 자체에서 이에 대한 확인을 하기도 쉽지 않은 실정이다. 본 논문에서는 이용자가 직접 자신이 스마트폰을 사용할 때 오가는 패킷을 확인하고 이상패킷이 발생되면 패킷 필터링에 의해 차단 시키는 방법을 제안한다. 일반적으로 스마트폰을 이용하여 Wi-fi망에 접속을 하려고하면 DHCP 프로토콜을 통해 자동으로 IP주소를 할당하게 된다. 스마트폰 자체에서 패킷을 캡쳐 하는 것이 아니기 때문에 스마트폰의 라우터 주소를 공유기가 아닌 노트북의 아이피로 수동으로 설정하여, 스마트폰으로 사용하는 모든 데이터망을 이용하는 패킷의 최초 경유지를 공유기가 아닌 노트북으로 변경하였다. Wi-fi 데이터서비스를 이용하면서 이용자의 스마트폰을 자가 점검 할 수있다. PC를 라우터로 동작하도록 하면 스마트폰에서 나가는 패킷에 최초 경유지가 PC가 되므로 PC에서 패킷 필터링 방식을 이용하여 이용자의 스마트폰에서 빠져나가고 들어오는 패킷을 차단하고 패킷를 확인 할 수 있으므로 패킷 분석 툴을 이용하여 패킷 분석도 가능하다.

3.2. 스마트폰 패킷 캡쳐 및 이상패킷 감지

3.2.1. 테스트 환경

스마트폰은 모토로라 아트릭스를 사용하였고 이 스마트폰은 안드로이드 2.3.4 버전(ginger bread) 기반으로 사용되었으며 노트북은 windows 7 64bits를 사용하고 공유기는 iptime N704m 유, 무선 공유기를 사용하여 패킷 캡쳐를 시도 하였다.

노트북이 라우터로 동작하도록 하기 위하여 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters 폴더의 정보중 IPEnableRouter 값을 1로 변경하였다. 노트북이 패킷을 받게 되면 ICMP Redirect를 보내어 노트북을 통하지 않고 패킷을 바로 공유기로 보내도록 메시지를 보내게 되는데 이를 막기 위해 Windows7 자체 방화벽에서 리디렉션을 차단 한 뒤 패킷을 캡쳐 하였다.

3.2.2. 패킷 캡쳐 및 분석

위와 같이 설정 후 카카오톡이나 기타 메신져, 웹 페이지 접속 등을 시행하면서 패킷을 관찰하였다. 평문이 패킷에 그대로 노출되는 모습 등 스마트폰에서 나가는 모든 패킷이 확인되었다.

네트워크에 접속하여 이용하는 어플리케이션을 실행하게 되면 [그림 2]와 실행되는 어플리케이션이 보내는 패킷을 확인할 수 있으며 어떤 어플리케이션이 실행되었는지 확인이 가능하다. 또한 테스트 시에 네이버 앱을 이용하여 네이버에 접속을 시도 하였고 스마트폰에 있는 웹 브라우져를 이용하여 웹에 접속을 시도하였다.

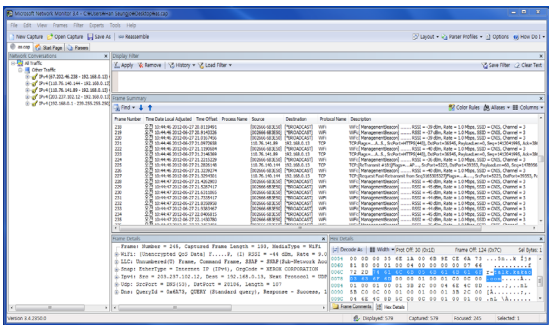

그림 2. 제안하는 패킷 캡쳐 방식
Fig. 2 The Proposed Packet Capture Method

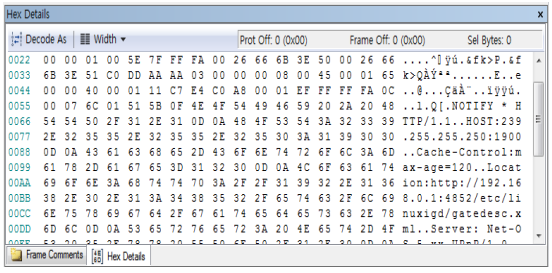

그림 3. 웹 접속 시 패킷
Fig. 3 Packet of Connect Web

이때 [그림 3]에서 확인되는 바와 같이 해당 웹에 대한 접속 정보도 확인 할 수 있었다. 위 테스트에 사용된 스마트폰은 루팅을 시행하지 않았으며 정상 마켓에서 다운로드한 무료 스마트폰 메신져인 카카오톡을 이용하여 메시지를 전송하였다. 메시지가 전송될 때 빠져나가는 패킷을 확인한 결과 패킷 상에 평문이 노출되지 않았다. 악성코드나 DDoS 공격에 감염되지 않은 스마트폰을 이용하여 테스트를 한 결과에는 실제로 앱 실행 혹은 웹 접속 이외의 스마트폰의 IMEI 정보 등의 단말기정보나 스마트폰 이용자의 정보 혹은 이용자가 실행하지 않은 앱이나 명령이 수행되는 현상은 관찰되지 않았다.

3.3. 이상패킷 감지 및 감지율 비교

루팅을 시행하지 않고 스마트폰에서 악성코드나 DDoS공격을 수행하기 힘들기 때문에 Eclipse를 이용하여 PC에서 가상으로 스마트폰과 동일한 환경을 만들고 시행하였다.

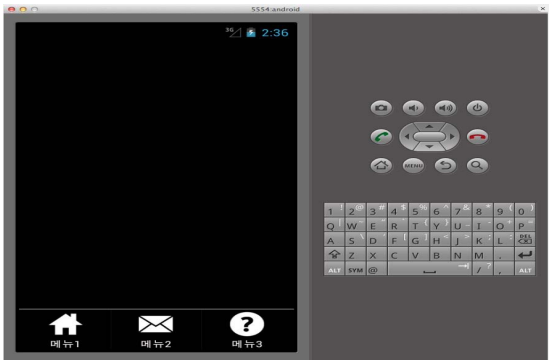

그림 4. 가상 스마트폰
Fig. 4 Virtual Smartphone

이전 테스트에서는 패킷의 최초경유지를 PC로 설정하였으나 이번 실험에서는 실제 스마트폰은 사용되지 않고 PC에서 스마트폰과 동일한 환경을 만들고 테스트하였기에 환경은 거의 동일하다. [그림 4]는 실험에 사용된 가상 스마트폰을 나타낸다.

악성코드 샘플을 구하여 PC에서 악성코드 침입시 탐지율과 제안한 방식의 패킷 캡쳐를 이용한 이상패킷 감지율을 나타낸 그래프이다. 사용된 악성코드 샘플은 3가지이며 각 샘플당 약 200회를 시행하여 통계하였고, 백분율 단위로 그래프에 표기하였다.

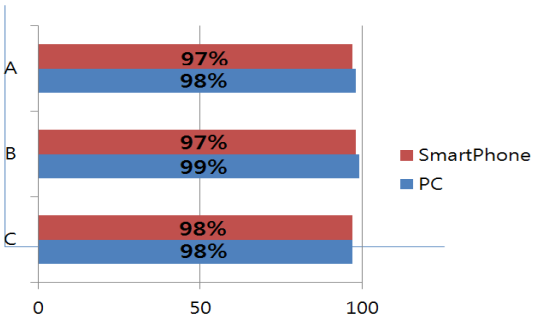

그림 5. PC와 스마트폰 이상패킷 감지율
Fig. 5 Detection rate of PC and Smartphone

샘플 A는 geinimi라는 진단명을 가진 악성코드이며, 정상 앱을 리패키징하여 백도어 기능(사용자의 정보 수집, SMS송신 등)을 수행한다. 안드로이드용 악성코드로 설계되어 국내 PC버젼의 백신들은 전혀 탐지 하지 못하는 경우도 있는데, 이는 OS와 사용하는 언어의 차이라고 판단되어 진다. 샘플 B는 FakePlayer라는 진단명을 가진 악성코드 이며 Fake에 접두어 혹은 접미어가 붙은 형태로 진단명이 공개되어 있으며 트로이목마형 악성코드이다. 이 악성코드 역시도 샘플 A와 마찬가지로 JAVA기반이 아닌 백신에서는 감지률이 떨어진다. 샘플 C는 Rootor라는 진단명을 가지며, 이는 스마트폰의 강제 루팅을 수행하여 보안을 해제시키는 악성코드이다.

3.4. 테스트 결과

현재 스마트폰 이용자들이 사용하고 있는 스마트폰 백신의 경우 절반 이상의 백신들이 약 40% 정도의 탐지율을 가지고 있으며 사용할만한 성능을 가진 앱은 실험

대상 앱 중 7개에 불과하다는 통계가 있다.[10] 본 논문에서 제안한 방식은 [그림 5]에서 나타난 바와 같이 악성코드를 탐지하는 성능은 기존 PC에서 사용하던 성능과 거의 유사하게 나타나고 있다.

PC에서 사용하는 툴 역시 신종의 악성코드는 발견하지 못함으로 DB 업데이트와 새로운 DB의 추가는 주기적으로 이루어져야 할 것이다. 패킷을 모니터링하는 탐지 방법은 PC를 이용하여야 하고 Wi-fi서비스가 가능하고 PC 혹은 노트북이 무선네트워킹이 가능하여야 실행할 수 있다는 단점이 있다. 반면에 이용자가 직접 자신의 스마트폰에서 오가는 패킷을 확인 할 수 있고 패킷이 PC를 경유하여 나감에 따라 스마트폰에서도 PC에서와 유사한 높은 탐지율을 나타낸다는 점이 강점이다.

Ⅳ. 결 론

안드로이드 운영체제에서 루팅을 통하여 이용이 가능한 블랙마켓이나 3rd-party마켓에서는 현재도 리패키징된 악성코드들이 다량 유포되고 있다. 스마트폰 이용자수는 하루가 다르게 증가하고 있으며, 이용자들의 편의나 재미를 위한 애플리케이션 또한 나날이 증가하고 있지만 그에 비해 보안체계는 아직도 많은 연구가 필요하다.

스마트폰을 이용하면서 중요한 점은 개인정보유출이나 이용자도 모르는 사이에 요금이 부가되는 악성코드들을 주의하여야 한다는 것이다.

하루에도 여러 가지의 애플리케이션을 다운 받고 설치하는 이용자들도 있는데 정상마켓에서도 애플리케이션을 설치하기 전에 나오는 주의문구를 꼭 확인하고 조금이라도 의심이 된다면 되도록 설치하지 않는 것이 좋고 루팅을 통해 슈퍼바이져의 권한을 얻은 이용자들은 스마트폰을 본인에게 맞는 설정을 바꾸는 데만 이용하고 블랙마켓이나 3rd-party마켓의 이용은 삼가야 할 것이다.

본 논문에서 제안한 스마트폰의 패킷을 캡쳐하여 이용자가 패킷을 확인하는 방법은 패킷분석이 가능하며 일반적으로도 평문이 노출되는지 알 수 없는 암호문이 오고 가는지에 대한 여부를 관찰하는 것만으로도 일부 악성코드의 흔적을 찾아낼수 있다. 또한, PC를 경유하여야 한다는 단점이 있지만 높은 탐지율을 보이고 있는 PC를 이용한 악성코드 탐지 방법은 보다 안정적이고 편리하게 스마트폰을 사용하는데 도움이 될 것이다. 추후에는 이를 스마트폰에 적용시켜 실시간 모니터링과 PC에서처럼 높은 탐지율을 지니게 되도록 연구를 거듭하여야 할 것이다.

감사의 글

본 연구는 2013학년도 조선대학교 학술연구비의 지원을 받아 연구 되었음.

REFERENCES

[1] C-J Ryu, K-H Han, “A Study on the Security Research about Botnet Attack Detection Interception” KICS, 2010.

[2] K-H Jang, S-M Choi, H-Y Yeom “Smartphone DDoS Attack Trends”, KIISC, 2011

[3] S-W Lee, “DDoS Attack Change and Forward”, Financial Security Agency Issue Report Vol.2011-004, 2011.

[4] Arun Raj Kumar, P. and S. Selvakumar, “Distributed Denial-of-Service Threat in Collaborative Environment A Survey on DDoS Attack Tools and Traceback Mechanisms”, IEEE International Advance Computing Conference 2009

[5] G-Y Kim, S-J Cho, “Security Vulnerability Trends in Smartphones”, KIISE Fall Conference, Vol.37, No.2 pp.90-91, 2010.

[6] W-S Choi, S-J Han “A Study of DDOS Attack and Malicious code Countermeasures for Smart Phone”, KIPS C2012J 0153, Fall Conference 2012.

[7] Bud Smith, “How to do Everthing Nexus One”, 2010.

[8] Ken Dunham, “Mobile Malware attacks and Defense”, SYNGRESS, 2009.

[9] G Carl, G Kesidis, RR Brooks, S Rai, “Denial of serviceattack detection techniques”, IEEE Internet Computing, pp.82-89, 2006.

[10] Felix Lau, stuart H. Rubin, Michael H. Smith, Ljiljana Trajkovic, “Distributed Denial of Service Attacks”, 2000 IEEE International Conference on Systems, Man and Cybernetics, Volume, pp.2275-2280, 2000.

윤풍식(Poong-Sic Yoon)

2008년 조선대학교 전자공학과 (학사)
2010년 조선대학교 정보통신공학과 (석사)
2011년 ~ 현재 조선대학교 정보통신공학과 (박사수료)
※관심분야 : 통신보안시스템설계, 네트워크 보안, 임베디드 시스템

한승조(Seung-Jo Han)

1980년 조선대학교 전자공학과 (학사)
1982년 조선대학교 전자공학과 (공학 석사)
1994년 충북대학교 전자계산학과 (공학 박사)
1986년 6월 ~ 1987년 3월 : 뉴올리언즈대학 객원교수
1995년 2월 ~ 1996년 1월 : 택사스대학 객원교수
2000년 12월 ~ 2002년 3월 : 버클리대학 객원교수
1998년 3월 ~ 현재 : 조선대학교 전자정보통신공학과 교수
※관심분야 : 통신보안시스템설계, S/W 불법복제 방지시스템, ASIC 설계