스마트폰 DDoS 공격과 악성코드에 관한 대응책 연구

최우석*, 한승조*
*조선대학교 정보통신공학과
e-mail:charismaws@naver.com

A Study of DDoS Attack and Malicious Code Countermeasures for Smartphone

Woo-Seok Choi*, Seung-jo Han*
*Dept of Information & Communication Engineering, Cho-Sun University

요 약

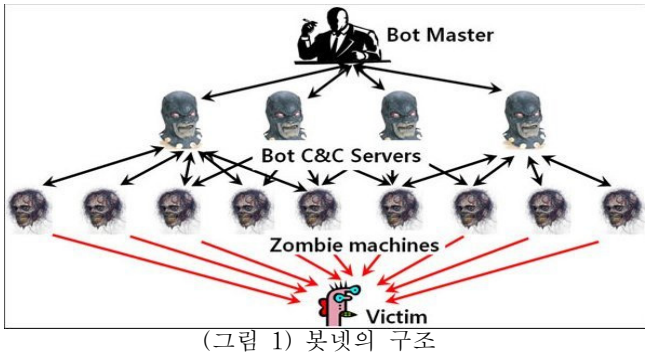
현재 스마트폰 사용자가 급증하면서 통계적으로 국민 1인당 1대의 스마트폰 혹은 태블릿PC를 사용하고 있는 것으로 집계되고 있다. 스마트폰 이용자가 증가함에 따라 보안에 대한 위협도 증가하고 있다. 실제 좀비 스마트폰에 대한 좀비 악성코드에 감염된 사례도 있으며 본 논문에서는 PC를 이용한 기존의 DDoS(Distributed Denial of Service)공격과 스마트폰을 이용한 DDoS공격 기법의 공격을 살펴보고, 스마트폰의 패킷을 캡쳐하여 Wi-fi 데이터망에서 앱 실행이나 웹에 접속 할 때 어떤 패킷이 나가고 들어오는지 확인하는 방법을 소개하며, 스마트폰 DDoS 공격 등의 악성코드에 대한 대응책을 제시한다.

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 개발되어지고 있으며 서비스하고 있는 솔루션도 등장하였다. 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. 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 DDoS공격의 공격 기법과 스마트폰 DDoS 악성코드에 대한 대비책을 살펴본다.

Ⅱ. 관련연구

2.1. Botnet



(그림 1) 봇넷의 구조

Botnet은 Bot Master에 의해 원격으로 조정되어지는 각종 악성행위를 수행할 수 있는 수많은 악성 소프트웨어인 Bot에 감염된 컴퓨터들이 네트워크로 연결되어 있는 형태를 칭한다.[1] 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.

2.2. 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 공

격의 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

2.3.1. 스마트폰을 이용한 DDoS공격

공식마켓을 통해 유포되는 어플리케이션도 있지만 대부분 안드로이드의 루팅이나 아이폰의 탈옥 등을 통하여 이용이 가능한 3rd-party 마켓을 통해 악성코드가 유포되는 경우가 많다.[2]

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 부팅 시 자동으로 악성 어플리케이션이 실행 될 수 있다.

2.3.2. 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]

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 하고 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.

2.3.3. 스마트폰 악성코드

PBStealer : 최초의 스마트폰 이용자 데이터를 훔치는 트로이목마형 악성코드이며, 감염된 스마트폰의 주소록을 txt파일로 저장하여 해당파일을 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 무자를 정송, 수신되는 문자를 조작 또는 차단한다.

III. 제안하는 패킷 캡쳐 및 분석

3.1 패킷 캡쳐 및 분석

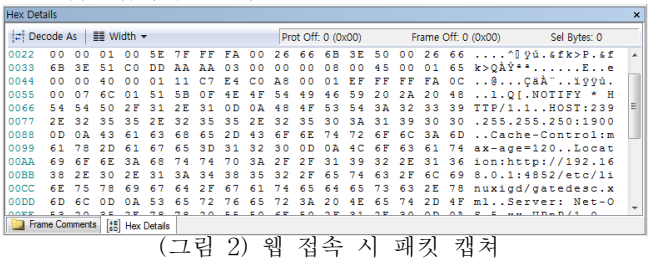
본 논문에서는 이용자가 직접 자신이 스마트폰을 사용할 때 오가는 패킷을 확인하고 이상패킷을 감지하는 방법을 제안한다. 일반적으로 스마트폰을 이용하여 Wi-fi망에 접속을 하려고하면 DHCP 프로토콜을 통해 자동으로 IP주소를 할당하게 된다. 스마트폰 자체에서 패킷을 캡쳐 하는 것이 아니기 때문에 스마트폰의 라우터 주소를 공유기가 아닌 노트북의 아이피로 수동으로 설정하여, 스마트폰으로 사용하는 모든 데이터망을 이용하는 패킷의 최초 경유지를 공유기가 아닌 노트북으로 변경하였다. Wi-fi 데이터서비스를 이용하면서 이용자의 스마트폰을 자가 점검 할 수 있다. PC를 라우터로 동작하도록 하면 스마트폰에서 나가는 패킷에 최초 경유지가 PC가 되므로PC에서 패킷 필터링 방식을 이용하여 이용자의 스마트폰에서 빠져나가고 들어오는 패킷을 차단하고 패킷를 확인 할 수 있으므로 패킷 분석 툴을 이용하여 패킷 분석도 가능하다.

IV. 스마트폰 패킷 캡쳐

4.1. 테스트 환경

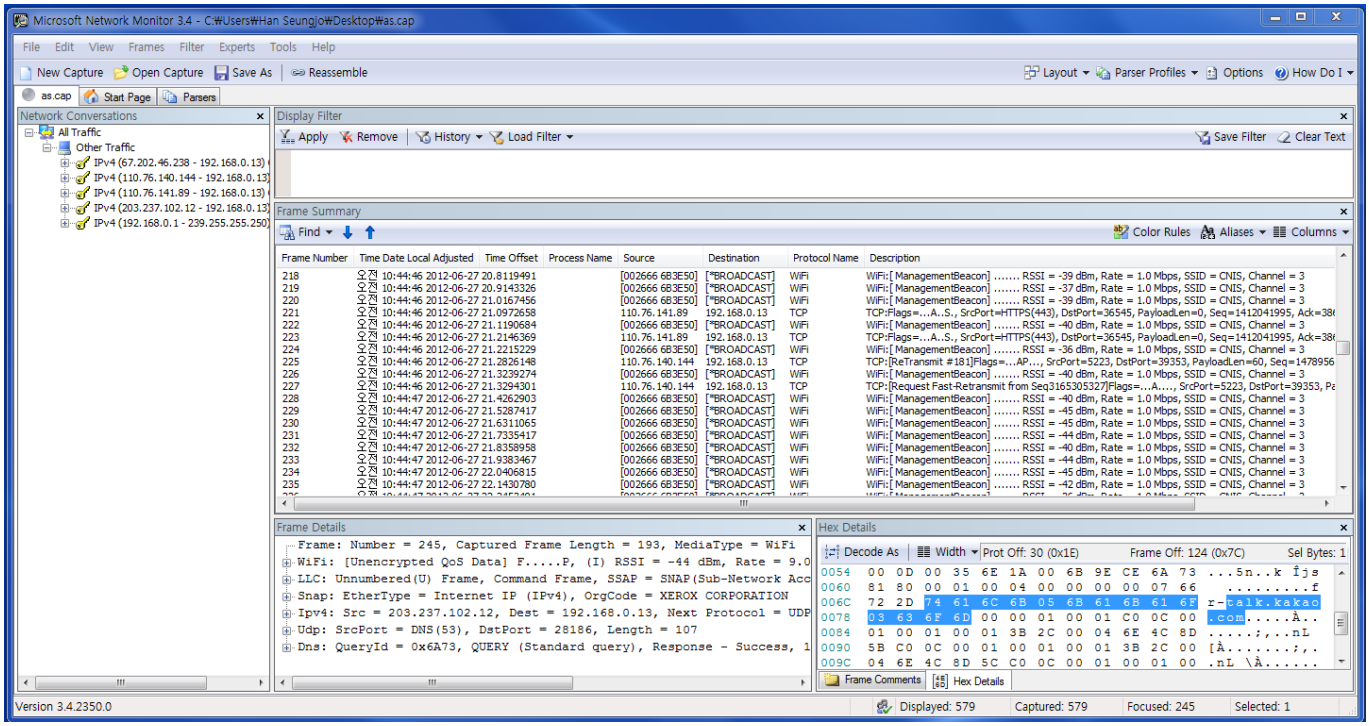
스마트폰은 모토로라 아트릭스를 사용하였고 이 스마트폰은 안드로이드 2.3.4 버전(ginger bread) 기반으로 사용되었으며 노트북은 windows 7 64bits를 사용하고 공유기는 Iptime N704m 유, 무선 공유기를 사용하여 패킷 캡쳐를 시도 하였다.

4.2. 패킷 캡쳐 및 분석



(그림 2) 웹 접속 시 패킷 캡쳐

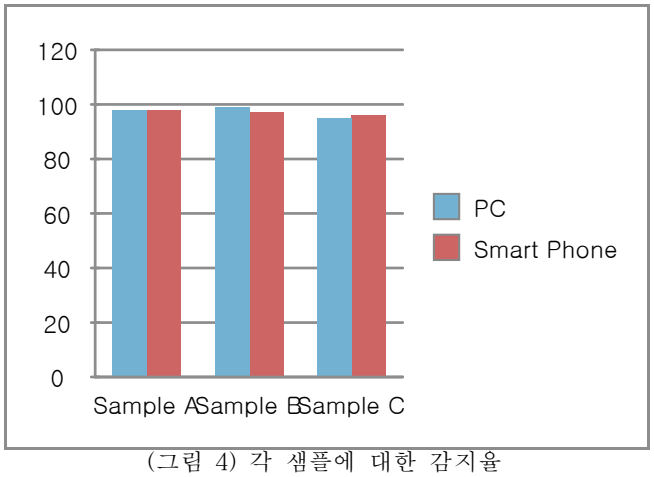
위와 같이 설정 후 카카오톡이나 기타 메신져, 웹 페이지 접속 등을 시행하면서 패킷을 관찰하였다. 평문이 패킷에 그대로 노출되는 모습 등 스마트폰에서 나가는 모든 패킷이 확인되었다. 네트워크에 접속하여 이용하는 어플리케이션을 실행하게 되면 (그림 3)과 실행되는 어플리케이션이 보내는 패킷을 확인할 수 있다. 테스트 시에 네이버 앱을 이용하여 네이버에 접속을 시도 하였고 스마트폰에 있는 웹 브라우져를 이용하여 웹에 접속을 시도하였다. 이때 (그림 2)에서 확인되는 바와 같이 해당 웹에 대한 접속 정보도 확인 할 수 있었다. 위 테스트에 사용된 스마트폰은



(그림 3) 앱 실행 시 패킷

루팅을 시행하지 않았으며 정상 마켓에서 다운로드한 스마트폰 메신저인 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.

4.3 이상패킷 감지 및 감지율 비교



(그림 4) 각 샘플에 대한 감지율

악성코드 샘플을 구하여 PC에서 악성코드 침입 시 탐지율과 제안한 방식의 패킷 캡쳐를 이용한 이상패킷 감지율을 테스트하였으며, 사용된 악성코드 샘플은 3가지이며 각 샘플 당 약 200회를 시행하여 통계하였다. 테스트 시 패킷의 최초 경유지가 PC가 되고 PC에서 패킷을 내보내는 방식으로 통신이 진행되므로 기존 PC에서 사용하던 snort툴을 이용하여 테스트하였다. 현재 스마트폰 이용자들이 사용하고 있는 스마트폰 백신의 경우 절반 이상의 백신들이 40%도 안되는 탐지율을 가지고 있으며 사용할만한 성능을 가진 앱은 실험대상 앱 중 7개에 불과하다는 통계가 있다.[10] 본 논문에서 제안한 방식은 <표 1>에서 나타난 바와 같이 악성코드를 탐지하는 성능은 기존 PC에서 사용하던 성능과 거의 유사하게 나타나고 있다. 제안한 탐지 방법은 PC를 이용하여야 하고 Wi-fi서비스가 가능하고 PC 혹은 노트북이 무선네트워킹이 가능하여야 실행 할 수 있다는 단점이 있다. 반면에 이용자가 직접 자신의 스마트폰에서 오가는 패킷을 확인 할 수 있고 높은 탐지율을 나타낸다는 점이 강점이다.

Ⅴ. 결론

안드로이드 운영체제에서 루팅을 통해 이용이 가능한 블랙마켓이나 3rd-party 마켓을 통해 이미 DDoS 공격 등의 악성코드들이 유포 되고 있는 실정이며 중국에서는 실제로 좀비 악성코드에 의해 100만대 정도의 스마트폰이 감염된 일이 있었다. 유포되는 악성코드 그리고 하우리 선행기술팀에서 시연한 스마트폰 DDoS공격과 중국의 좀비 스마트폰 감염사례를 보면 스마트폰을 이용한 DDoS 공격이 충분히 가능하며 현재 스마트폰 이용자가 국내에만 2000만명이 넘는 실정이기에 일부 스마트폰만을 가지고도 충분히 공격 대상이 된 서버를 마비시키는 것이 가능하다. 3G 서비스를 넘어 4G 서비스를 이용하는 스마트폰이 대중화됨에 따라 3G 데이터망보다 높은 대역폭을 가지고 빠른 속도를 제공하게 되어 공격 대상이 되는 서버나 웹의 경우에

는 트래픽이 보다 대량으로 들어오기 때문에 피해가 더욱 심각해질 수 있다. 또한 스마트폰의 경우에는 스마트폰 이용자들이 전원이 꺼지거나 부족할 시에 배터리를 교체한다거나 충전을 시키면서 24시간 거의 전원이 켜져 있도록 유지를 하기 때문에 PC에서의 DDoS 공격보다 많은 피해를 입힐 수 있다.

스마트폰을 이용한 DDoS 공격은 공격대상이 된 서버만이 문제가 아니라 좀비 스마트폰 이외에 3G/4G 데이터 통신 서비스 자체를 방해하게 되며 심각한 경우 데이터 통신 자체를 사용하지 못하는 경우도 발생할 수 있다.[5]

추후 연구에서는 본 논문에서 제안한 패킷 캡처와 패킷 필터링을 동시 할 수 있는 툴을 구현하여 보다 편리하고 안전한 보안체계를 수립하도록 할 것이다.

참고문헌

[1] 류창주, 한경헌 "Botnet 공격 탐지 차단 기술에 대한 보안 연구", 한국통신학회 춘계 학술대회, 2010.

[2] 장기헌, 최상명, 염흥열 "스마트폰 DDoS 공격 동향", 정보보호학회, Aug, 2011.

[3] 이성욱, "DDoS 공격 기법의 변화 및 전망", 금융보안연구원 이슈리포트, Mar, 2011.

[4] 최상명, "좀비 스마트폰과 DDoS 공격", 하우리 선행기술팀 하우리, Apr, 2011.

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

[6] 곽창규, “DDoS 공격 기법의 변화 및 전망”, 금융보안연구원 이슈리포트, Mar, 2011.

[7] 김기연, 조성제, “스마트폰 보안 취약점 동향”, 한국정보과학회 가을 학술발표눈문집, 제37권 제2호 pp.90-91, 2010.

[8] Bud Smith. How to do Everthing Nexus One. July. 2010.

[9] Ken Dunham, “Mobile Malware attacks andDefense”, SYNGRESS 2009.

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

[11]. 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, 3, 2000.