韓國IT서비스學會誌
第15卷 第2號
2016年 6月, pp.157-167

Journal of Information Technology Services
http://dx.doi.org/10.9716/KITS.2016.15.2.157

DDoS 공격에 대한 선제적 침입 탐지·차단 방안

김대환* · 이수진**

A Method for Preemptive Intrusion Detection and Protection Against DDoS Attacks

Dae Hwan Kim* · Soo Jin Lee**

■ Abstract ■

Task environment for enterprises and public institutions are moving into cyberspace-based environment and structing the LTE wireless network. The applications "App" operated in the LTE wireless network are mostly being developed with Android-based. But Android-based malwares are surging and they are the potential DDoS attacks. DDoS attack is a major information security threat and a means of cyber attacks. DDoS attacks are difficult to detect in advance and to defense effectively. To this end, a DMZ is set up in front of a network infrastructure and a particular server for defensive information security. Because There is the proliferation of mobile devices and apps, and the activation of android diversify DDoS attack methods. a DMZ is a limit to detect and to protect against DDoS attacks.

This paper proposes an information security method to detect and Protect DDoS attacks from the terminal phase using a Preemptive military strategy concept. and then DDoS attack detection and protection app is implemented and proved its effectiveness by reducing web service request and memory usage. DDoS attack detection and protecting will ensure the efficiency of the mobile network resources. This method is necessary for a continuous usage of a wireless network environment for the national security and disaster control.

Keyword : Android, DDoS, Preemptive, Detection, Protection

Submitted : January 29, 2016 1st Revision : May 10, 2016 Accepted : May 12, 2016

* 국군수송사령부 정보체계실 소령, 교신저자
** 국방대학교 컴퓨터공학전공, 교수

1. 서 론

기업과 공공기관의 업무환경은 사이버 공간으로 이동되고 국방 업무도 필연적으로 사이버 공간으로 이동되고 있다. 특히, 공군은 독자적인 LTE 기반 무선네트워크 체계를 구축하여 지휘관의 지시사항을 신속히 전파하고 참모간 업무협조를 위해 지휘통제용으로 LTE를 운용하고 있다. 향후 항공작전 통제용, 기지방어 통제용, 대공 방어전력 통제용, 화생방 작전 통제용, 재해·재난 인원과 시설 통제용, 항공기 정비작업 통제용 등으로 모바일 애플리케이션인 앱(APP)을 운용할 계획이다.

다양한 업무지원용 앱을 편리하게 개발하기 위해 안드로이드가 등장하였고, 그러므로 현재 안드로이드 단말기의 보급률이 다른 운영체제와 비교하여 상대적으로 높은 상황이다. 애플 iOS는 앱을 공유하고 배포하는 과정에서 검수하기 때문에 악성코드가 숨겨진 앱이 배포되기 어렵지만 안드로이드의 경우에는 상대적으로 검수가 미흡하여 악성코드가 숨겨진 앱이 등록되어 배포될 수 있다. 더욱이 오픈 소스를 기반으로 하는 안드로이드에서 DDoS 공격을 유발하는 Bot이 포함된 앱이 안드로이드 마켓에 등록되어 배포될 것이 예상된다.

모바일 사용자의 증가와 모바일 서비스의 확산으로 모바일 네트워크는 잠재적인 DDoS 공격의 경로가 되고 있다. 공격자인 敵은 사이버 공격으로 컴퓨터 시스템과 데이터 통신망 등을 교란, 마비, 무력화시켜 전쟁의 승·패에 결정적인 영향을 미치려 하고 있다(Eom et al., 2012). 이와 같이 DDoS 공격의 위협이 증가됨에 따라 많은 기관들은 DDoS 공격 보안 솔루션을 도입하고 있지만 DDoS 공격은 사전에 탐지가 어렵고 효율적인 방어가 어려운 실정이다. 군사전략 개념 중에 적의 공격이 임박한 명백한 증거와 기습 공격이 개시된 상황에서 적을 선제적으로 타격하는 공격 전략이 있다. 선제적인 공격은 적의 기습적인 군사행동에 대해 치명적인 이익을 획득하기 위한 예방전쟁 형태의 군사력 운용하는 공격이다. 본 논문은 선제적인 공격전략 개념을 적용하여 모바일 단말기 단계에서부터 선제적으로 DDoS 공격을 탐지하여 차단하는 효과적인 방안을 제시하는 연구이다.

본 논문의 구성은 다음과 같다. 제 2장 관련연구에서 안드로이드 보안, DDoS 공격의 특징, DDoS 공격에 대한 대응, 선제적인 방위전략을 살펴보고, 제 3장에서는 안드로이드 기반에서 선제적인 DDoS 공격을 탐지하고 차단하는 방안을 제시하였다. 제 4장에서는 선제적 방위개념을 적용하여 DDoS 공격을 탐지하고 차단하는 프로토타입을 구현함으로써 그 효과를 증명하였다. 끝으로 제 5장에서는 본 논문의 연구 한계와 향후 과제를 제시하였다.

2. 관련 연구

2.1 안드로이드 보안

안드로이드 운영체제에서 정보보안은 커널이 각각 분리된 앱으로 실행하도록 권한이 분리된 앱 모델로 구현한다. 권한 분리를 통해 공격자는 공격 과정이 더욱 복잡해지고 단말기 구성요소에 대한 권한 획득과 변경 과정이 까다롭게 되었다. 앱 개발자는 앱이 단말기 구성요소를 사용하기 위해 앱의 AndroidManifest.xml 파일 내에 권한 요청정보를 등록하고 단말기 사용자의 최종 승인을 획득해야만 단말기 구성요소를 사용할 수 있다. 사용자가 명시적으로 권한을 부여하지 않은 앱은 다른 앱을, 다른 앱의 데이터에 접근이 불가능하고 또한 단말기의 카메라, GPS, 네트워크 등의 API도 호출할 수 없다(Jeong, 2016).

하지만 최근 무료로 다운로드 가능한 손전등 앱에서 사용자의 개인정보, 위치정보, 유심칩정보, 개인일정 등이 유출되는 문제가 발생되었다. 해당 앱은 사용자의 승인을 받은 앱으로 교묘하게 개인정보를 빼내는 명령어 10개가 숨긴 것으로 확인되었다(Kim, 2014). 애플 iOS는 앱을 등록하는 과정에서 검수를 완벽하게 하여 악성코드가 숨겨진 앱의 배포가 어렵지만 안드로이드의 경우에는 상대적으로

검수가 미흡하여 악성 앱이 배포되기가 용이하다. 이와 같이 열악한 상황에서 DDoS 공격을 유발하는 Bot 기능을 포함한 앱이 안드로이드 마켓에서 배포될 가능성이 잠재하고 있다.

2.2 DDoS 공격

DDoS(Distributed Denial of Service : 분산 서비스 거부) 공격은 인터넷 또는 네트워크상에서 다수의 좀비 PC들이 공격 표적 대상으로 다량의 트래픽을 발생시켜 네트워크 대역폭을 점유함으로써 서비스를 마비시키는 공격이다. 최근 스마트폰은 SNS, 위치검색, 인터넷 등 다양한 서비스와 연동되어 스마트폰을 통한 새로운 정보보안 공격이 강조되고 있다. 더욱이 최근에는 DDoS 공격의 Bot 기능이 포함된 악성코드 패키지들이 증가되어 DDoS 공격의 발생 빈도, 공격에 의한 대역폭의 지속적인 점유 증가로 서비스 중단과 업무 마비 같은 공격 피해가 가능하다. DDoS 공격의 증가로 대부분의 조직들은 연 평균 4.5회의 DDoS 공격을 경험하고 공격에 사용되는 대역폭은 공격 건당 1.7GB에 이른다. DDoS 공격의 61%가 업무에 큰 지장을 주고 있지만 거의 40%에 이르는 조직들은 DDoS 공격에 대한 대비가 전혀 없고 DDoS 공격을 탐지 또는 차단하고 피해를 최소화하기 위해 정보보안 시스템들의 업그레이드를 수행하지 않고 있다(John, 2014).

모바일 네트워크의 취약성에 대해 공격 및 대응에 관련된 기술 연구가 2000년 초부터 꾸준히 되었다(Enck et at., 2005; Traynor et al., 2006; Zhao et al., 2009). 모바일 네트워크에서 DDoS 공격의 특징은 다음과 같다. 첫 번째는 모바일 서비스 및 운영에 필요한 리소스를 대상으로 한다. 인터넷을 대상으로 하는 DDoS 공격은 특정 서비스 또는 웹 서비스의 거부를 목표로 하지만 모바일 네트워크에 DDoS 공격은 Paging/Dedicated Traffic 채널, 시그널링 메시지 등을 전송하여 리소스를 소모시키는 서비스 거부가 가능하다. 두 번째는 대량의 트래픽을 생성하여 공격하는 인터넷 DDoS와 달리 소량의 트래픽만으로도 효과적인 공격이 가능하다. 사례로 SMS 문자 메시지를 이용하여 모바일 네트워크 구간의 리소스를 소모시킴으로써 전체 모바일 서비스의 장애를 일으킬 수 있다. 세 번째는 Botnet을 활용한 DDoS 공격으로 진화되고 있다. 보안이 취약한 단말기들을 Bot으로 만들어 대용량의 트래픽을 발생시키는 DDoS 공격 수단으로 악용한다. 이러한 Bot의 확산은 편리하게 앱을 판매하거나 무료로 배포하는 안드로이드 마켓의 운용에서 더욱 증폭되고 있다.

2.3 DDoS 공격 대응방법

DDoS 공격에 대응하기 위해 정부는 다음 세 가지 조치를 취하고 있다(NIA, 2010). 첫 번째는 DDoS 공격을 수행하는 좀비 단말기가 명령제어 서버에 접속하여 공격명령을 받지 못하도록 보안 DNS 서비스를 제공함으로써 인터넷 상에서 공격자용 명령제어 서버로의 접속을 차단한다. 두 번째는 웹 사이트가 악성코드를 유포하는 웹 사이트가 되지 않도록 웹 사이트의 보안성을 강화하고 있다. 세 번째는 고 위험성 악성코드의 피해 확산을 방지하기 위해 백신보급과 사이버 검역체계 구축을 통해 사용자 스스로 악성코드에 감염되었는지 확인하고 자동보안 업데이트 과정으로 면역성을 강화한다. 이 중에서 세 번째 조치인 사용자가 악성코드 감염을 인지하여 신속하게 선제적으로 치료하는 것이 가장 효과적이다.

이와 더불어 많은 기업과 조직에서는 DDoS 공격을 대응하기 위해 중요 서비스에 대한 피해 방지 대책을 마련하고 충분한 대역폭을 확보함으로써 대용량의 트래픽 공격을 처리하는 능력을 구비하고 있다. 하지만 이와 같이 DDoS 공격을 탐지하는 시스템 운영은 그 효과를 예측하기 어렵고 기업과 조직에 적합한 적정 성능의 DDoS 탐지 시스템 구축을 결정하기 또한 어렵다. 그러므로 최근 DDoS 공격 탐지 및 차단 시스템은 트래픽 분산처리 기술을 기반으로 Layer 3계층에서부터 7계층까지 다양한 DDoS 공격을 탐지하여 차단할 수 있는 체계를 도입하여 운영을 추진하고 있다. 최근

〈Table 1〉 Method of DDoS Attack Detection and Protection

Division	Method Description
Abnormal Protocol Defense	To block and detect attacks using a vulnerability in the TCP/IP protocol combinating abnormal packets and using abnormal packet size and abnormal packet source address
Blacklist Defense	To block the traffic by registering the IP address to the blacklist to cause the DDoS attack
Automatic learning Defense	To extract automatically real-time patterns of attacks and To block abnormal traffic patterns by learning automatically normal traffic situations
Community-based Defense	To block lump traffic on the DDoS countries
Denial of Service Defense	To detect and block SCAN · Flooding attacks to detect vulnerabilities on the protected internal systems and networks
Application Layer Defense	To register and block attacks attempting to exploit the vulnerability of a variety of application layer protocols such as Web, DNS, FTP
Signature Defense	To block DDoS attacks Match Matching the latest DDoS attack signatures and patterns provided by the National Intelligence and Security Agency

DDoS 공격을 탐지하여 차단하는 시스템에 적용된 다양한 방어 방법을 정리하면 <Table 1>과 같이 설명된다(Cecui, 2014).

이와 같은 DDoS 공격 탐지 및 차단 방법은 방어 중심으로 DMZ 단계에서 DDoS 공격을 대응하는 방법이다. 하지만 최근 DDoS 공격은 수십 Gbps에서 수백 Gbps 트래픽의 대용량 DDoS 공격과 전통적인 Layer인 3 · 4계층 공격에서 Layer 7까지 다양한 계층에 대한 공격이 가능한 상황이다. 또한 모바일 단말기와 앱의 급증으로 다양한 네트워크 인프라와 특정 서버들을 공격 목표 대상으로 DDoS 공격이 수행되는 상황으로 발전하였다. 이와 같은 상황에 대해 기존 DMZ 단계에서 DDoS 공격을 탐지 · 차단하는 것은 한계가 있을 것이다.

2.4 안드로이드 악성코드 분석

안드로이드 악성코드가 급증하는 상황에서 안드로이드 악성코드를 차단하기 위한 악성코드 분석은 반드시 필요하다. 안드로이드 악성코드를 분석하는 방법에는 안드로이드 애플리케이션을 디스어셈블리하여 API를 분석하는 방법, 안드로이드 애플리케이션의 권한 부여를 분석하는 방법, 악성코드가 통신하는 패킷을 검사하는 방법 등이 있다.

대부분 악성코드를 탐지하기 위해 패킷을 검사하는 방법이 사용되고 패킷의 수집은 필수적이다. 안드로이드 네트워크 패킷을 수집하는 방법으로 TCPdump를 이용하고, 다른 방법으로는 tpacketcapture 안드로이드 애플리케이션이 이용된다. 그리고 안드로이드 운영체제가 제공하는 VPN 서비스를 이용하여 VPN 터널링으로 패킷을 수집하는 방법이 있다(Seong and Im, 2014). 이 외에도 와이어샤트와 같은 안드로이드 애뮬레이터를 이용하여 패킷을 가상으로 수집하는 방법도 있다. 이 방법들은 애플리케이션 레벨에서 모바일 트래픽을 모니터링하고 분석하는 방법이다(Choi et al., 2011). 하지만 안드로이드 네트워크 패킷을 수집하는 방법들은 대부분 모바일 단말기의 성능 제약으로 네트워크상의 특정 서버로 트래픽을 수집하여 분석하는 방법이 사용된다. 하지만 수집된 트래픽을 전송하는 과정에서 손실이 있을 수 있고 트래픽 수집으로 또 다른 모바일 네트워크에 부하를 유발한다.

3. 선제적 DDoS 공격 침입 탐지 · 차단 제안

3.1 선제적 방위전략

전장상황의 속도 변화는 매우 빠르고 복잡해서 미래의 상황예측이 더욱 불확실하다. 이러한 상황

에 대한 문제 해결 방법은 기존 제도와 절차에서 해답을 찾을 수가 없다. 다시 말해서 기존의 수직적, 계층적, 분화적, 기계적 조치 방법은 한계가 있다. 이와 같은 한계를 극복하기 위해 국가방위 전략수립은 현 위험을 인지하고 선제적으로 대처함으로써 위험을 감당할 만한 수준으로 낮추는 방위전략이 사용된다(INSS, 2013). DDoS 공격 대응도 기존의 정형화된 대응방법으로 탐지 및 차단하기 어려워 선제적 방위전략 개념을 적용한 DDoS 공격 침입 탐지·차단 방안 연구가 필요하다.

이미 선제적인 방위전략은 국방 정보보안 분야에 적용되고 있다. USB를 포함한 다양한 보조저장장치가 대용량, 빠른 속도, 휴대 용이성으로 사용이 급증되고 UBS가 제한 없이 사용됨으로써 새로운 보안위협으로 등장하게 되었다. 국방 정보보안 분야에서는 비인가 USB가 조직 내 단말기에 접속하는 경우 자동으로 접속을 차단되도록 USB 사용통제 제도를 운영하고 있다. 이와 같은 제도를 통해 비인가 USB로 바이러스 등 악성코드가 유입되는 경로를 차단하고 있다.

3.2 선제적 DDoS 공격 침입 탐지·차단 고려사항

모바일 네트워크 인프라에 대한 잠재적인 DDoS 공격 위협이 증가됨에 따라 IP 기반의 DDoS 공격을 대응하기 위해 보안 장비가 설치되어 네트워크를 보호하고 있다. DDoS 공격을 탐지하기 위해 일정 시간 주기로 제어 및 데이터 트래픽 패킷을 수집한다. 수집된 패킷에서 사용자 수, 사용자별 수신 트래픽 등 사용 패턴을 산출하고 과거 유사 시점의 트래픽 패턴과 비교 과정을 통해 DDoS 공격을 탐지한다(Kim et al., 2014). 패턴 분석은 외부에 전문 패킷 분석 도구가 설치된 서버를 사용하여 수백 메가바이트 단위의 데이터를 세부적으로 분석한다. 하지만 대용량 패킷의 분석에 많은 시간이 소요되어 신속하게 DDoS 공격을 탐지하고 차단하는 것이 제한된다. 최근 손전등 앱과 같이 악성 코드가 포함된 악성 앱이 사용자도 모르게 단말기에 설치되고 있다. 악성코드 중 DDoS 공격에 관련된 앱이 설치될 수 있으므로 선제적으로 단말기 단계에서부터 DDoS 공격 앱을 탐지하여 차단하는 것이 요구된다.

〈Table 2〉 Analysis Type of Packet

① The average number of packets transferred per second
② The average packet sizes transferred per second
③ Total number of bytes
④ The average number of bytes transferred per second
⑤ The average megabit transferred per second

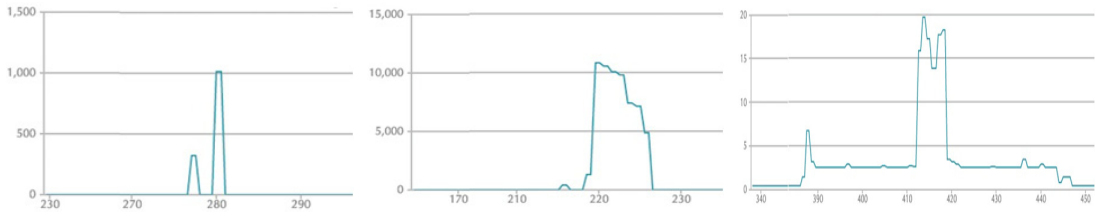
앞에서 언급한 것과 같이 DDoS 공격을 탐지하기 위해 특정 사이트를 대상으로 임의의 패킷이 어떻게 유통되었는지 <Table 2>와 같은 정보를 파악하여 분석한다. 이 경우에 호스트별, 포트별, 프로토콜별 네트워크 점유율 등이 핵심적으로 사용되지만 안드로이드는 보안을 위해 단말기 Root 권한을 공개하지 않기 때문에 단말기 단계에서 패킷 정보를 분석하는 것은 제한된다.

한편 PC와 같은 성능이 좋은 단말기는 대용량의 트래픽을 수집하여 분석하는 것이 성능 상에 문제가 없지만 스마트폰과 같은 모바일 단말기는 PC와 비교할 때 처리 속도가 느리고 메모리 용량이 부족하기 때문에 단말기 성능에 영향을 덜 받는 DDoS 공격 탐지 방법이 요구된다.

더불어 안드로이드 앱은 각각의 권한으로 분리되어 실행되고 단말기 구성요소에 대한 사용 권한이 승인된 안드로이드의 제공 API만 사용 가능하여 안드로이드 제공 API를 철저히 분석하여 DDoS 공격의 탐지와 차단에 사용한다.

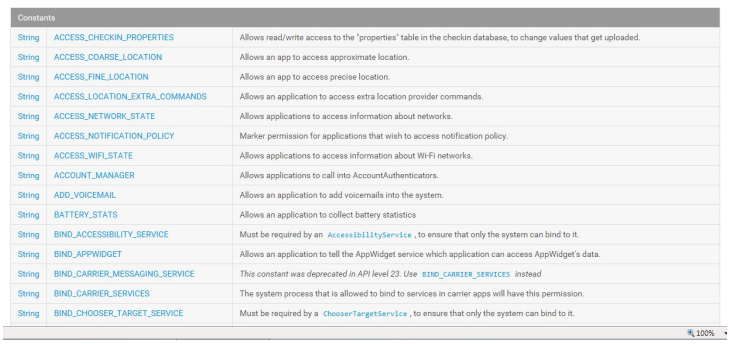
3.3 선제적 DDoS 공격 침입 탐지·차단 개념

모바일 네트워크는 한정된 무선자원을 효율적으로 사용하기 위해 일정 시간 동안 사용이 없는 단말기의 무선자원을 해제하고, 무선자원이 해제된



Document File Movie File Streaming File

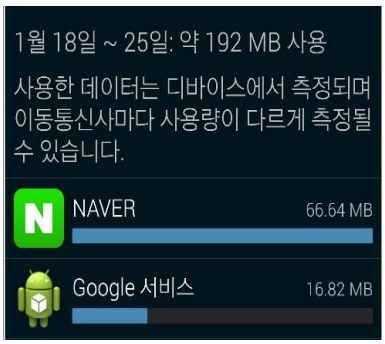
〈Figure 1〉 Data Traffic of Transfer File



Constants		
String	ACCESS_CHECKIN_PROPERTIES	Allows read/write access to the "properties" table in the checkin database, to change values that get uploaded.
String	ACCESS_COARSE_LOCATION	Allows an app to access approximate location.
String	ACCESS_FINE_LOCATION	Allows an app to access precise location.
String	ACCESS_LOCATION_EXTRA_COMMANDS	Allows an application to access extra location provider commands.
String	ACCESS_NETWORK_STATE	Allows applications to access information about networks.
String	ACCESS_NOTIFICATION_POLICY	Marker permission for applications that wish to access notification policy.
String	ACCESS_WIFI_STATE	Allows applications to access information about Wi-Fi networks.
String	ACCOUNT_MANAGER	Allows applications to call into AccountAuthenticators.
String	ADD_VOICEMAIL	Allows an application to add voicemails into the system.
String	BATTERY_STATS	Allows an application to collect battery statistics
String	BIND_ACCESSIBILITY_SERVICE	Must be required by an AccessibilityService, to ensure that only the system can bind to it.
String	BIND_APPWIDGET	Allows an application to tell the AppWidget service which application can access AppWidget's data.
String	BIND_CARRIER_MESSAGING_SERVICE	*This constant was deprecated in API level 23. Use* BIND_CARRIER_SERVICES *instead*
String	BIND_CARRIER_SERVICES	The system process that is allowed to bind to services in carrier apps will have this permission.
String	BIND_CHOOSER_TARGET_SERVICE	Must be required by a ChooserTargetService, to ensure that only the system can bind to it.

100%

〈Figure 2〉 Sample of Android Manifest API

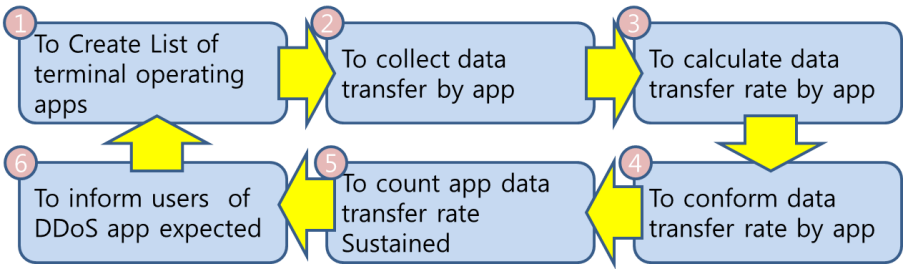


〈Figure 3〉 Data Traffic Service APP

단말기는 Idle 상태로 전환된다. <Figure 1>은 일반 문서 파일, 동영상 파일, 스트리밍 파일을 전송하는 경우로 시간에 따른 단말기의 데이터 사용 현황이 파일 전송 시작되면 데이터 사용량이 증가되었다가 다시 안정 상태로 복귀하는 것을 확인할 수 있다. 하지만 모바일 단말기에 DDoS 공격에 사용되는 악성 앱이 설치된 경우에는 단말기가 지속적으로 데이터를 전송하고 데이터 사용이 한정된 사용자의 단말기일 경우에는 데이터를 비정상적으로 사용할 수 있다.

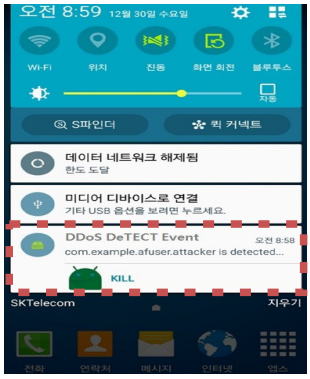
안드로이드 앱이 구동되기 위해 <Figure 2>에서 기술하는 GPS 접근권한, 외부 스토리지 저장권한, 웹브라우저 북마크 데이터 읽기권한 등 121개의 권한 중에서 필요한 권한을 AndroidManifest에 기술하여 사용한다(Android Developers, 2015). 안드로이드 권한 중에 네트워크 호출과 상태 확인에 관련된 권한에는 ACCESS_WIFI_STATE, CALL_PHONE 등 13종이 있음을 확인하였다. 이중에서 ACCESS_NETWORK_STATE 권한을 사용하여 <Figure 3>과 같이 특정 기간 동안 앱별로 사용되는 총 데이터 사용량 정보를 제공하는 앱이 구현되어 있다.

본 논문은 DDoS 공격을 근본적으로 탐지하고 차단하기 위해 단말기에 설치된 DDoS 공격 앱을 선제적으로 탐지하여 차단하는 방안을 제안한다. 선제적 DDoS 공격 침입 탐지·차단 앱 또한 ACCESS_NETWORK_STATE 권한을 사용한다. <Figure 1>에서 살펴본 것과 같이 각각 파일 전송은 전송량의 변화가 균일하지 않으므로 단말기에 설치되어 작동되는 앱을 대상으로 일정 시간 간격으로 데이터 전송량을 수집을 통해 전송량 변화율을 확인하고 임의로 설정된 DDoS 데이터 전송 가능율 범위 내에서 장시간 유지되는 경우에 DDoS 공격에 사용되는 앱으로 의심하고 사용자에게 통보한다. DDoS 데이터 전송 가능율 범위 내에 장시간 유지되는지 확인하기 위해 DDoS 가능 카운트를 설정하고 DDoS 가능 카운트가 일정 수치를 초과하는 경우에 해당 앱을 DDoS 공격 의심 앱로 식별하여 단말기 사용



〈Figure 4〉 Process for DDoS Attack Detection and Protection

〈Figure 5〉 DDoS Attack Detection and Protection APP



〈Figure 6〉 DDoS Attack Detection Result and Protection

자에게 통보함으로써 사용자로 하여금 직접 DDoS 공격 앱임을 확인하고 차단하도록 한다. <Figure 5>는 안드로이드 단말기에서 DDoS 공격을 탐지하고 차단하는 기능의 처리 과정으로 DDoS 공격 탐지·차단 앱이 중단될 때까지 무한적으로 운용된다.

4. 구현 및 검증

4.1 선제적 DDoS 공격 침입 탐지·차단 앱 구현

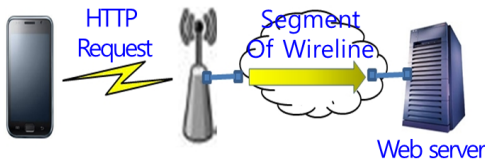
선제적 DDoS 공격 침입 탐지·차단 앱은 DDoS 공격이 단말기에서 지속적으로 균일한 데이터를 전송한다는 가정에서 단말기의 구동중인 모든 앱을 대상으로 데이터 전송량 변화율을 추출하여 DDoS 공격을 탐지한다. 앱별 데이터 전송량 변화율은 <Figure 3>과 같이 안드로이드가 제공하는 ACCESS_NETWORK_STATE 서비스를 이용하여 구현하였다. DDoS 공격 침입 탐지·차단 앱은 <Figure 5>의 화면으로 DDoS 공격을 탐지 시작한다. DDoS 공격 침입 탐지·차단 앱은 앱별 데이터 전송량 변화율을 확인하여 설정된 시간 동안 변화가 없는 경우에 탐지 앱을 <Figure 6>과 같이 사용자에게 통보하고 차단을 요청한다. 스마트폰의 전원이 켜진 이후, 앱별 전송되는 총 데이터 전송량(TDT : Total Data Traffic)을 수집하고 <Formula 1>과 같이 앱별 시간당(Δt) 데이터 전송량의 변화율 산출하여 산출된 변화율이 특정 범위(DT : DDoS Tolerance) 내에 지속된 시간을 카운트하여 DDoS 공격 가능성을 예측한다.

$$\frac{\frac{TDT_t}{\Delta t}}{\frac{TDT_{(t-1)}}{\Delta(t-1)}} \times 100 < DT$$

〈Formula 1〉 Detection Formula for DDoS Attack APP

4.2 구현 앱 테스트

선제적 DDoS 공격 침입 탐지 · 차단 앱의 효과를 검증하기 위해 <Figure 7>과 같은 사설 LTE 개발환경에서 DDoS 공격 침입 탐지 · 차단 테스트 환경을 구성하여 DDoS 공격과 차단과정에서 서버 자원이 변화되는 과정을 확인하였다. DDoS 공격을 발생시키기 위해 <Figure 8>와 같은 가상의 DDoS 공격 발생 앱을 구현하였다. 구현 앱은 사설 LTE 앱스토어 역할과 DB 역할을 하는 서버로 지속적인 HTTP 요청을 보내는 DDoS 공격을 수행한다. DDoS 공격 침입 탐지 · 차단 앱은 DDoS 공격이 의심되는 앱을 탐지하여 사용자에게 통보하고 차단시킴으로써 DDoS 공격을 선제적으로 탐지 · 차단됨을 확인하였다. 원칙적으로 DDoS 공격은 여러 대의 단말기에서 동시 다발적으로 공격을 하는 것이 기본이지만 사설 LTE 테스트 환경상의 제약으로 하나의 단말기에서 쓰레드 방식으로 동시에 다중 단말기에서 요청을 보내는 것을 가정하였고 가상 DDoS 공격 발생 앱이 이를 구현하였다.



〈Figure 7〉 DDoS Attack Test Scenario

〈Figure 8〉 DDoS Attack App

4.3 테스트 결과

DDoS 공격 악성 앱이 설치된 단말기에서 서버로 50ms마다 HTTP 서비스를 10개씩 다중으로 요청하였다. 즉, 서버가 1초에 약 200개의 HTTP 서비스 요청을 받는 효과와 같다. DDoS 공격의 영향과 차단 효과를 검증하기 위해 서버의 HTTP 서비스 요청과 메모지 자원 사용량 변화를 확인하였다. DDoS 공격이 구동되면서 서버의 메모리 자원 사용과 HTTP 서비스 요청이 급격히 증가한 것을 <Figure 9>와 같이 확인하였다. 하지만 단말기에서 지속적으로 데이터 트래픽이 발생됨을 사용자에게 통보하고 악성 앱을 차단시킴으로써 <Figure 10>과 같이 서버의 메모리 사용이 다시 안정화됨을 확인하였다.

〈Figure 9〉 Http Request and Memory Usage during DDoS Attack Detection

〈Figure 10〉 Http Request and Memory Usage after DDoS Attack Protection

5. 결 론

지금까지 DDoS 공격에 대한 보안대책은 네트워크 인프라와 특정 서버에 DMZ를 설정하는 방어적인 침입 탐지 · 차단 정책이었다. 하지만 모

바일 단말기와 앱의 급증, 안드로이드의 활성화로 악성코드도 동시에 증가하였다. 특히 DDoS 공격은 다양화되고 진화됨으로 DMZ 단계에서 DDoS 공격을 탐지하여 차단하는 것은 한계가 있다. 본 논문에서는 선제적으로 단말기 단계에서부터 DDoS 공격을 탐지하여 차단하는 정보보안을 제안하고 프로토타입 구현을 통해 그 효과를 증명하였다.

최근 국방 및 공공기관에서는 모바일 네트워크를 구축하여 국가 안보와 재난 통제 서비스를 추진하고 있다. 하지만 DDoS 공격으로 네트워크와 서비스가 무력화되면 제 역할을 할 수 없을 것이다. 그러므로 선제적으로 단말기 단계에서 DDoS 공격 탐지・차단 앱은 필수적으로 설치하여 대처할 수 있는 방안일 것이다. 또한 최근 데이터 통신 소요가 증가되면서 모바일 단말기에서 무제한으로 데이터 통신을 사용하는 사용자가 있지만 아직도 많은 사용자는 제한된 데이터 통신량을 사용하고 있으므로 자신의 단말기가 DDoS 공격의 Bot으로 악용되어 필요 이상의 데이터 통신이 발생함을 인지시킬 수 있는 도구가 필요하다.

일반적으로 침입탐지 시스템을 구현하기 위해 다양한 침입탐지 기법이 연구되는데 그 종류에는 비정상 행위 탐지(Anomaly Detection), 오용 탐지(Misuse Detection), 명세기반 탐지(Specification-based Detection)가 있다. 이 중에서 명세기반 탐지는 알려지지 않은 공격에 대한 탐지와 오탐율이 낮은 침입 탐지기법으로 이것을 선제적 DDoS 공격 침입·탐지에 적용하여 학술적으로 표현하는 연구가 필요하다. 현재 구현된 DDoS 공격 탐지・차단 앱은 임의의 DDoS 변화율과 데이터 전송 유지 시간으로 프로토타입을 구현하였지만 일반적인 파일 전송과 온라인 게임 트래픽을 분석하여 적용 기준을 제시하는 연구가 요구된다. 끝으로 선제적 DDoS 공격 침입 탐지・차단이 DMZ 단계에서 DDoS 공격을 탐지하여 차단하는 기존의 DDoS 공격 대응 방법보다 효과가 있음을 실증적으로 검증하는 연구가 추가적으로 가능하다.

References

Android Developers, Manifest.permission, 2015, http://developer.android.com/intl/ko/reference/android/Manifest.permission.html(Accessed 2016/02/01).

Cecui, DDoS Attack Defense List, 2014, http://www.cronyit.co.kr/img/brochure/SECUI_MFD.pdf(Accessed 2016/02/01).

Choi, Y.R., J.Y. Jeong, B.C. Park, and W.G. Hong, “System for Mobile Application Level Traffic Monitoring and Analysis”, *KNOM Review*, Vol.14, No.2, 2011, 10-21.

(최영락, 정재윤, 박병철, 홍원기, “응용 레벨 모바일 트래픽 모니터링 및 분석을 위한 시스템 연구”, *Knom Review*, 제14권, 제2호, 2011, 10-21.)

Enck, W., P. Traynor, P. McDaniel, and T. La Porta, “Exploiting Open Functionality in SMS-Capable Cellular Networks”, *In Proceedings of the 12th ACM Conference on Computer and Communications Security ACM,* 2005, 393-404.

Eom, J.H., S.S. Choi, and T.Y. Jeong, *Between Versions Introduction*, Hongreung Science Publishers, 2012.

(엄정호, 최성수, 정태명, *사이버전 개론*, 홍릉과학출판사, 2012.)

Institute for National Security Strategy(INSS), North Korean Nuclear Issue and the Korean Peninsula Trust Process, 2013, http://www.inss.re.kr/inss/attach/getFile.do?fileId=5761(Accessed 2016/02/01).

(국가안보전략연구소, 북핵문제와 한반도 신뢰프로세스, 2013, http://www.inss.re.kr/inss/attach/getFile.do?fileId=576).

Jeong, J.G., “*Do it! Android App Programming*”, Aegis Publishing, 2016.

(정재곤, “*Do it! 안드로이드 앱 프로그래밍*”, 이지

스퍼블리싱, 2016.)

John, P., “DDoS Attacks Advancing Enduring Survey”, SANS, 2014.

Kim, S.G., J.H. Oh, and C.T. Im, “Abnormal Flooding Detection Technologies in the LTE Mobile Data Networks”, *Journal of Korea Information and Communications Society General Conference,* 2014, 878-879.

(김세권, 오주형, 임채태, “LTE 모바일 망에서의 비정상 데이터 플루딩 탐지 기술”, *한국통신학회 종합 학술 발표회 논문집(하계),* 2014, 878-879.

Kim, Y.R., Eye News 24 News, 2014, http://news.inews24.com/php/news_view.php?g_serial=861593&g_menu=020310(Accessed 2016/02/01).

(김영리, 손전등 앱 개인정보 유출… “내 폰도 털렸나?”, 아이뉴스24뉴스, 2014/11/06, http://news.inews24.com/php/news_view.php?g_serial=861593&g_menu=020310).

NIA, “DDoS Strategies and Policy Planning”, 2010.
(NIA, “DDoS 대응전략 및 정책계획”, 2010.)

Seong, M.J. and E.G. Im, “Android Malware Network Packet Analysis Specific Action”, *Journal of the Korea Information Science 2014 Korea Computer Conference*, 2014, 104-106.

(성명재, 임을규, “안드로이드 악성코드의 네트워크 패킷 특정행동 분석”, *한국정보과학회 2014 한국컴퓨터종합학술대회 논문집,* 2014, 104-106.)

Traynor, P., W. Enck, P. McDaniel, and T. La Porta, “Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks”, *IEEE/ACM Transactions on Networking,* Vol.17, No.1, 2009, 40-53.

Zhao, B., C. Chi, W. Gao, S. Zhu, and G. Cao, “A Chain Reaction DoS Attack on 3G Networks : Analysis and Defenses”, *In Infocom,* 2009, 2455-2463.

About the Authors

Dae Hwan Kim (neohwan@naver.com)

Major Dae Hwan Kim is currently a head of Information Systems Department at Military Transport Command. He received the master's degree in Computer and Information Science from Korea National Defense University (KNDU) in 2005. and completed Ph.D course in Military Science (Computer Engineering) from KNDU in 2014. He worked for Air Force Headquarters Information Systems Planning Department with battlefield system integration and then. His current research interests include Android, Intrusion Detection, LTE, etc.

Soo Jin Lee (cyberkma@gmail.com)

Professor Soojin Lee is currently a Professor of Department of Computer Engineering, Korea National Defense University (KNDU). He received his master's degree. in Computer Science from Yonsei University in 1996. He received Ph.D in Computer Science from Korea Advanced Institute of Science and Technology (KAIST) in 2006. His current research interests include Intrusion detection systems, Cryptography, Cyber warfare, and Cyber security policy.