Journal of The Korea Society of Computer and Information
Vol. 18, No. 8, August 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.8.095

일회성 세션 키 기반 HTTP DDoS 공격 방어기법

최 상 용*, 강 익 선*, 김 용 민**

One-time Session Key based HTTP DDoS Defense Mechanisms

Sang-Yong Choi*, Ik-seon Kang*, Yong-Min Kim**

요 약

2009년 77DDoS 대란 이후 DDoS 공격은 사회적 위협으로 발전하고 있다. 이러한 위협에 대응하기 위해 다양한 DDoS방어기법이 연구되고 있으나, DDoS 공격기법 또한 더욱 정교해지고 있다. DDoS 공격의 형태는 과거 네트워크계층의 대용량 트래픽 공격에서 최근에는 애플리케이션 계층의 소량의 정교한 형태(Slow DDoS Attack)로 변하고 있으며 공격을 위한 공격에이전트 또한 더욱 지능화 되고 정상 PC와 구분이 모호하여 차단이 더욱 어렵게 되고 있다. 정상PC와 지능화된 공격에이전트 구분을 위해 최근 사용되는 사용자인증시스템(CAPTCHA)의 경우 인증과정에서 사용자의 개입이 필요하며, 특히 NAT 환경에서 IP 기반 차단 방법은 정상사용자의 트래픽까지 동시 차단될 수 있다. 본 논문에서는 HTTP 프로토콜에서 사용하는 쿠키를 활용한 일회성 세션 키 기반 인증방법을 적용하여 공격 에이전트와 정상 PC를 구분, HTTP DDoS 공격을 효과적으로 차단하기 위한 방어기법을 제안한다.

▸ Keywords : DDoS 공격, 쿠키, 방어, 인증

Abstract

DDoS attacks have became as a social threat since 2009 7.7 DDoS turmoil. Even though defence techniques have been developing to provide against those threats, they become much more sophisticate. In recent years, the attack form of DDoS is changing from high amount of traffic attack of network layers to highly sophisticate small amount of application layers. To make matters worse, attack agent for the attack has became very intelligent so that it is difficult to be blocked since it can't be distinguished from normal PCs. In the user authentication system(such as CAPTCHA) User intervention is required to distinguish normal PCs and intelligent attack agents

•제1저자 : 최상용 •교신저자 : 김용민
•투고일 : 2013. 7. 9, 심사일 : 2013. 7. 21, 게재확정일 : 2013. 8. 2
* 한국과학기술원 사이버보안연구센터(KAIST Cyber Security Research Center)
** 전남대학교 문화콘텐츠학부 전자상거래전공(Dept. of Electronic Commerce, Chonnam National University)

and in particular, in a NAT environment, IP-based blocking method can be cut off the normal users traffic at the same time. This research examined defense techniques which are able to distinguish between agent and normal PC and effectively block ways the HTTP DDoS offense applying one-time session key based authentication method using Cookie which is used in HTTP protocol to protect web sever from sophisticate application layer of DDoS.

▸ Keywords : DDoS Attack, Cookie, Defense, Authentication

I. 서 론

최근 눈부신 정보기술의 발전은 국민들의 삶의 질을 전반적으로 향상시켰지만 초고속 통신망의 발전은 해커의 공격 위협 또한 증가시킨 것이 사실이다. 초고속 통신망의 확산은 국내 전체 PC가 공격의 도구가 될 수 있다는 사실을 보여주었으며, 그 대표적인 예가 2009년 7월 7일 발생된 77DDoS이다. 과거 DDoS 공격은 해커의 실력 과시 또는 특정 조직의 금전적 이익 등을 위하여 시도되었으나, 77DDoS를 기점으로 DDoS 공격이 사회혼란 조장 등 핵티비즘의 성격으로 발전할 가능성이 있다는 것을 보여주는 계기가 되었다. 특히, 정부기관 등 대국민 서비스를 중시하는 조직과 금융기관 등 24시간 서비스를 필요로 하는 조직에서는 DDoS 공격의 적절한 방어가 보안신뢰도 측정의 기준이 될 만큼 중대한 목표로 떠올랐다. 또한 77DDoS를 기점으로 DDoS 공격은 다양한 계층의 공격이 조합된 혼합공격으로 발전하였으며, 이를 방어하기 위해 DDoS 사이버대피소[1-2], 사용자 인증시스템(CAPTCHA)[3] 등 여러 가지 메커니즘이 연구되기 시작하였다. 하지만 대부분의 대응방법이 궁극적으로 IP 주소차단을 기반으로 하고 있어 IP주소가 부족한 IPv4 환경에서 일반적으로 사용하는 NAT(*Network Address Translation*) 환경 내에 악성코드에 감염된 PC에서 발생하는 트래픽과 정상 PC에서 발생하는 트래픽이 혼재할 경우 정상 사용자에게 선의의 피해를 줄 우려가 있으며, 사용자 인증시스템(CAPTCHA)의 경우 시도-응답(Challenge-Response) 방법을 사용하여 정상사용자 인증을 위해 사용자의 개입이 필요한 불편함이 존재한다.

본 논문에서는 이러한 문제점을 해결하고자 HTTP 프로토콜에서 사용하는 쿠키를 이용하여 매 접속마다 다른 세션 키를 요구, 정상 사용자와 비정상 공격에이전트를 구분하는 방법을 제안하고자 한다. 또한 IP주소 기반의 차단으로 인한 역

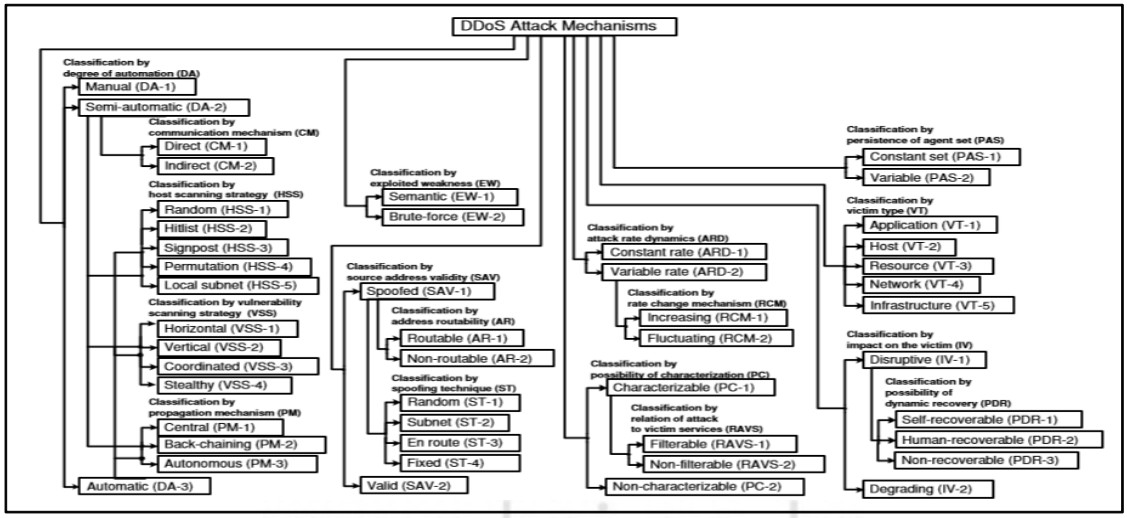

그림 1. DDos 공격 메커니즘 분류[4]
Fig. 1. Classification of DDoS Attack Mechanism[4]

효과를 방지하기 위해 사용자 세션을 인증하고 인증 받지 못하는 세션을 강제종료 시키는, 세션통제 방법을 이용하여 DDoS 공격으로부터 웹서버를 보호할 수 있는 방법을 제안하고자 한다. 본 논문에서 제안하는 방식은 세션기반 접근통제를 수행하기 때문에 IP 주소기반 접근통제에 비해 보다 정밀한 통제가 가능하여 같은 IP 주소라 할지라도 정상 사용자가 발생시키는 트래픽과 비정상 공격에이전트가 발생시키는 트래픽을 구분할 수 있어 DDoS 공격에 대한 효과적인 방어를 제공한다.

본 논문의 2장에서는 기존에 알려진 DDoS 공격과 이를 방어하기 위한 관련된 연구내용을 살펴보고, 3장에서는 본 논문에서 제안하는 일회성 세션 키 기반 방어 메커니즘을 설명하며, 4장에서는 제안하는 알고리즘을 시험하여 제안 메커니즘의 효과를 검증한 후 5장 결론에서 본 연구결과의 활용방안과 향후 연구방향을 제시한다.

II. 관련 연구

관련 연구에서는 알려진 DDoS 공격의 방법과 기존에 연구되고 있는 DDoS 차단 기술에 대해 분석한다.

1. DDoS 공격

1.1 DDoS 공격 분류

DDoS 공격의 이론적인 분류는 그림 1과 같이 다양한 기준에 따라 분류하게 된다. Jelena와 Peter[4]는 DDoS 공격을 공격방법의 자동화 여부, 사용된 취약점, 출발지 IP 주소 변조 여부, 동적 공격규모, 특성화 가능성, 공격 에이전트 규모, 피해여부, 피해영향 등에 따라 분류하였다. 먼저 자동화 여부에 따라 수동, 반자동, 자동 공격으로 구분할 수 있으며, 취약점을 이용하느냐에 따라서는 무작위 공격(플루딩 공격)과 취약점 이용공격으로 나눌 수 있다. 출발지 IP주소변조 여부에 따라서는 변조된 출발지 공격과 변조되지 않은 출발지로 구분할 수 있으며, 특징점이 있는지 여부는 공격을 감지할 만한 특정 문자열 등의 공격을 정의할 수 있는 지로 구분한다. 그리고 대부분 알려진 바와 같이 공격 에이전트가 존재하는 경우 에이전트 수가 고정적인지 가변적인지가 중요한 분류의 기준이 되며, 피해형태에 따라 네트워크 대상, 호스트 대상, 리소스 대상, 애플리케이션 대상, 인프라 스트럭쳐 대상으로 나눌 수 있다. 마지막으로 피해의 영향에 따라 서비스에 일부 영향을 주는 경우와 파괴되는 경우로 구분한다. 이와 같은 분류는 전체적으로 공격자의 특징과 피해여부에 따라 분류한 것으로서 최근과 같이 특정부분이 다양화된 공격방법을 모두 포괄하기에는 일정부분 한계가 있다.

표 1. DDoS 공격 분류
Table 1. Classification of DDoS Atack

공격분류	특징	공격유형
Flooding Attack	Non-Spoofing	SYN Flooding
		ACK Flooding
		SYN/ACK Flooding
		FIN Flooding
		RST Flooding
		UDP Flooding
		ICMP Flooding
		TCP/UDP/ICMP 혼합
	Spoofing	SYN Flooding
		ACK Flooding
		SYN/ACK Flooding
		FIN Flooding
		RST Flooding
		UDP Flooding
		ICMP Flooding
		TCP/UDP/ICMP 혼합
		TCP/IP주소 Null 공격
Connection Attack	HTTP	HTTP Daemon 개수 이상 초과
	과다 TCP Connection	Application의 input queue 마비
Application Attack	Application 특성 이용	FTP공격, Time 공격, VoIP주소공격, Email 등

또 다른 분류방법으로는 위와 같이 복잡한 분류법을 사용하지 않고 보다 현실적으로 실제 많이 발생되는 공격을 기준으로 분류하는 방법이다[5]. 이 방법은 공격을 표 1과 같이 플루딩 형태와 연결공격 그리고 애플리케이션 공격 등 3가지로 분류하고 플루딩 공격에 대해서는 출발지가 변조되었는 지와 변조되지 않았는지 여부에 따라 다시 분류하는 방법을 사용하였다. 하지만 77 DDoS를 포함한 최근 발생되는 DDoS 공격은 공격자의 입장에서는 보다 쉽게 이용할 수 있고, 공격의 영향을 즉각적으로 줄 수 있는 동시에 탐지가 어려운 공격을 선호하고 있다. 이와 같은 기준에 따르면 대용량의 과다한 트래픽을 발생시키는 것과 같은 OSI 3계층 또는 OSI 4계층의 공격은 탐지와 차단이 상대적으로 쉽기 때문에 최근의 공격은 HTTP 프로토콜을 이용한 OSI 7계층 형태로 변화하고

있다. OSI 7계층 DDoS 공격에 대한 세부적인 분류는 표 2와 같이 가능하다[6].

표 2. OSI 7계층 DDoS 공격 분류
Table 2. OSI 7 Layer DDoS Attack Classification

DDoS 공격 방법	프로토콜
Valid/InValid HTTP GET Flooding	HTTP
GET with CC	HTTP
저 대역폭 HTTP DDoS	HTTP
Fragmented HTTP Header Attack	HTTP
DNS Query Flooding	DNS
Telnet Flooding	Telnet
FTP PASV DoS	FTP

1.2 최근 DDoS 공격 특징

최근 DDoS 공격의 특징은 새로이 등장하는 HTTP DDoS 공격방법을 살펴보면 쉽게 알 수 있다. 최근 발견되는 소량의 트래픽으로 시스템의 가용성에 치명적인 손상을 줄 수 있는 공격방법을 Slow Attack이라 하며 대표적으로 Slow HTTP POST DDoS[7], Slowloris[8], Slow Read DDoS[9], Cache-Control DDoS[10] 등이 있다. Slow Attack은 동작하는 형태는 상이하나 공통적인 특징은 대량 트래픽을 발생시키지 않고 소량 트래픽을 발생시키되 세션연결을 지속하는 방법을 사용하여 웹서버의 자원을 모두 소모시켜 웹서버의 가용성을 침해한다는 것이다. HTTP 프로토콜을 이용한 공격기술은 2009년 발생된 77DDoS, 2011년 발생된 34DDoS 공격에도 사용되었으며, 향후 지속적인 위협이 될 것으로 예상하고 있다[11-12].

2. DDoS 공격 대응기술

살펴본 바와 같이 DDoS 공격은 OSI 7계층 중 가장 많이 사용되는 3계층, 4계층 그리고 7계층이 전체적으로 사용되기 때문에 이에 대한 탐지 및 차단 기술 또한 다양하게 연구되고 있다. DDoS 공격은 전통적으로 그 특성이 대용량의 트래픽을 과다하게 발생시키거나 다수의 공격 에이전트가 동시에 피해시스템으로 트래픽을 발생시키는 등 정상트래픽과 구분할 수 있는 특성들이 존재하였다. 이러한 특성을 기반으로 과거의 접근법은 공격에이전트 식별, 에이전트별 용량제한, 특정 공격패턴 필터링 등의 방법을 이용하여 DDoS 공격을 차단하고 있다[4][13]. 하지만 앞서 살펴보았듯이 최근의 DDoS 공격은 점차 정교해지고 있어 이와 같은 통계적 분석방법으로는 정확한 탐지와 차단에 한계가 있다.

최근의 연구결과에 따르면 DDoS 공격 차단방법은 TCP/IP의 트래픽 특성을 이용한 대응방법[14-15]과 트래픽을 분산시켜 과부하를 방지하는 방법[1-2] 그리고 DDoS 공격으로 부터 감내력을 높이기 위한 정보시스템 보안설정 등의 방법[16]이 제시되고 있으며, 공격에이전트와 정상 사용자를 정확하게 구분하기 위해 캡챠(CAPTCHA)와 같은 사용자 인증방법을 이용하는 방법[3][17]까지 다양하게 연구되고 있다. 또한 최근 멀티 레이어 DDoS 공격에 효과적으로 대응하기 위한 방안으로 OSI 3계층, 4계층, 7계층 보안장비를 혼합한 다단계 방어기법도 연구되고 있다[6].

III. HTTP DDoS 방어 기법

1. 기존 DDoS 공격 대응기술의 한계 및 개선방안

1.1 DDoS 대응기술의 한계

DDoS 공격에 효과적으로 대응하기 위한 기존의 연구내용은 크게 두 가지 측면에서 한계점이 도출된다. 첫 번째로 지금까지 살펴본 기술들을 분석한 결과 대응 방법에서의 대표적인 기술은 트래픽의 특성과 프로토콜의 특성을 분석하여 비정상적인 사용자를 식별하고 차단하는 방식을 사용한다. 이것은 성능 면에서는 효과적인 차단 성능을 보일지는 모르지만 NAT와 같은 환경 내에서 정상 사용자가 차단을 당할 수 있는 가능성이 존재한다. 두 번째로 공격 에이전트와 정상 사용자를 명확하게 구분하기 위해 사용할 수 있는 가장 확실한 방법은 시도-응답(Challenge-Response) 방식이다. 시도-응답 방식은 사용자에게 특정 질의를 던진 후 응답하게 하는 방법으로 대표적으로 캡챠(CAPTCHA)가 있다. 이와 같은 방법은 사용자에게 매번 다른 요청을 하므로 공격에이전트와 정상 사용자를 구분하기에 타당하나, 사용자에게 특정한 값을 입력하는 행위 즉, 웹 서핑 중에 사용자의 개입을 요구하는 불편과 최근의 이미지 프로세싱의 발전 등으로 인해 정확한 식별의 한계점이 존재한다.

1.2 개선방안

본 연구에서는 이와 같은 문제점을 해결하기 위해 HTTP 쿠키기반 일회성 세션 키를 사용한 세션기반 통제방식 DDoS 공격 방어 방법을 제안한다. 캡챠(CAPTCHA)와 같은 사용자 개입이 필요한 인증방식으로 인한 불편을 해결하기 위해 사용자의 개입 없이 클라이언트에게 매번 다른 값을 요구하는 HTTP 쿠키를 사용하여 공격 에이전트와 정상 사용자를 구분

하고, 식별된 공격 에이전트에 대해서는 IP를 차단하는 방법을 지양하고 연결된 세션만을 강제 종료하는 방법으로 NAT 환경에서의 정상 사용자의 접속을 보장한다.

2. HTTP 쿠키의 개념

HTTP 프로토콜은 웹서버와 사용자(웹브라우저)간에 정보를 전달할 수 있다. 일반적으로 웹브라우저는 파라미터를 사용하여 웹서버에 정보를 전달한다. 반대로 웹서버가 웹브라우저에 정보를 전달하는 방법에는 쿠키를 사용하게 된다. 웹브라우저의 요청에 의해서 응답을 하는 웹서버는 필요에 따라서 쿠키를 웹브라우저에게 응답과 같이 전송하게 되면 웹브라우저는 다음 요청 시 웹서버에서 전달된 쿠키에 따라 동작하게 된다[18].

HTTP 쿠키에는 일반적으로 웹서버의 세션을 유지하기 위해 *Session ID*를 생성하여 전송할 수 있다. *Session ID*는 웹브라우저와 웹 서버간의 인증을 위해 사용할 수 있으며, 새로운 세션이 성립되더라도 웹 서버는 *Session ID*를 확인하여 동일 세션이라는 것을 알 수 있다. 하지만 *Session ID*의 한계점은 재사용이 가능하다는 점이다. 즉, 공격자는 트래픽 모니터링 또는 웹 서버로부터 전송된 *Session ID*를 재사용하여 동일 세션을 지속적으로 유지할 수 있다. 즉, 클라이언트의 접속을 인증하는 기능은 존재하나 정상 사용자와 공격 에이전트를 구분할 수는 없다.

3. 공격에이전트와 사용자를 구분하는 방안

최근 DDoS 공격에 사용되는 공격에이전트의 특징은 네트워크 측면에서 단일 패킷을 기반으로 정상 사용자와 구분하기가 매우 어렵다는데 공격방어의 근본적 한계점이 존재한다. 이와 같은 지능화된 공격에이전트와 정상 사용자를 부분하는 방법에 대해 본 논문에서는 다음과 같은 두 가지 방법을 사용한다.

그 첫 번째 방법은 접속 시 웹 서버에서 쿠키를 사용자에게 전송하여 사용자로부터 전송되는 쿠키 값의 유효성을 검증한다. HTTP 쿠키는 웹서버와 정상 브라우저 간 상호작용이 이루어져야 하는데 공격에이전트의 경우 RFC2616[19]에서 정의하고 있는 HTTP 요청과 동일한 형태로 패킷을 생성할 수는 있지만, 웹서버와 브라우저 간 상호작용이 필요한 웹서버에서 전송되는 쿠키에 대해 정상적으로 응답하지 못한다.

두 번째 방법은 공격자가 패킷을 분석하여 쿠키 응답을 재사용하는 것을 방지하기 위해 웹서버에서 브라우저로 보내는 쿠키를 매번 다르게 요청한다. 응답내용 분석 등의 방법을 이용하여 해커가 웹서버에서 전송되는 쿠키에 대해 응답 값을 생성하여 전송하더라도 매번 다르게 일회성 쿠키를 보내게 된다면 공격 에이전트는 정상 브라우저와 동일하게 동작할 수 없을 것이다.

4. 쿠키를 이용한 HTTP DDoS대응 메커니즘

본 논문에서 제안하는 쿠키기반 일회성 세션 키를 사용한 사용자 인증 메커니즘은 그림 2와 같이 동작한다. 먼저 클라이언트에서 웹서버로 요청되는 모든 값에 대해 쿠키를 보내는 것은 클라이언트의 최초 요청 후 응답에 포함하게 된다. 그 다음으로 웹 서버의 부하를 최소화하기 위해 최초 요청 시 요청된 현재 페이지로 *HTTP 302 Redirect*를 하게 된다. *Redirect*의 경우 유지된 세션을 즉시 종료시키기 때문에 지능화 되지 않은 공격 에이전트의 경우 세션이 즉시 끊어지고 추가적인 트래픽 유입을 방지하게 된다. 지능적인 공격 에이전트의 경우 *Redirect*를 인지하여 새로운 접속이 이루어 질 때에는 웹서버에서 보내는 쿠키에 정상적으로 응답을 해야 한다. 만약 쿠키에 정상적인 응답을 하지 못한다면 이것은 공격 에이전트로 간주하고 세션을 즉시 종료한다.

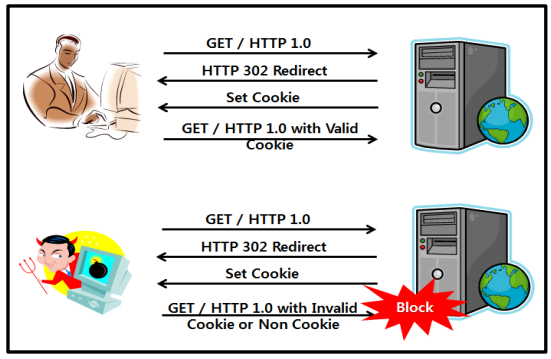

그림 2. 쿠키를 이용한 사용자 인증 메커니즘
Fig. 2. User Authentication Mechanism using Cookies

사용자 인증을 위해 생성하는 일회성 세션 키는 일반적으로 쿠키에서 사용하는 *Session ID*와 서버시간(Time-Stamp)의 쌍으로 구성된다. 웹서버의 응답내용에는 Session ID, 서버시간 그리고 수신된 서버시간에 대한 해시값(*Clinet-Hash*)을 계산하도록 하는 명령이 포함되어 있다. 정상 사용자 또는 공격 에이전트는 최초 접속 시 *HTTP 302 Redirect*가 이루어지므로 세션이 한번 종료된다. 하지만 정상 사용자에 대한 서비스는 지속적으로 유지되어야 하기 때문에 정상 사용자의 재접속에 대해서는 *SessionID*를 이용하여 유지시키고 *Session ID*와 쌍으로 전송되는 매번 바뀌는 서버시간에 대한 해시 값을 비교하여 세션 키의 재사용을 방지

한다. 매번 브라우저가 해시를 계산하게 함으로 공격에이전트에 의해 자동적으로 생성되는 트래픽에 대한 식별이 가능하게 한다. 쿠키 인증을 위한 모듈은 그림 3과 같이 *Set Module*, *Check Module* 그리고 *Session Management Module* 3개로 구성된다.

*Set Module*은 최초 클라이언트의 요청에 대해 *Set-Cookie*를 세팅하는 모듈이다. 클라이언트 요청 해더에 *Session ID*, *Client Hash*가 없을 경우 *Set Module*이 클라이언트에게 쿠키를 세팅하고 클라이언트가 요청한 페이지를 재요청 하게끔 *HTTP 302 Redirect*를 전송 한다. *Check Module*에서는 클라이언트에서 전송되는 *Session ID*와 *Client_Hash*가 서버에 저장된 값과 일치하는지를 비교하여 일치하는 경우 정상 페이지를 응답하고, 일치하지 않는 경우 해당 세션을 종료시킨다. 정상 페이지로 응답할 때에는 다음 요청 시 비교를 위해 해당 클라이언트로 현재 서버시간을 전송하고 업데이트 한다. *Session Management Module*은 클라이언트의 각 세션에 대한 *Session ID*와 클라이언트로 보내 준 서버시간을 최신으로 유지하고 무결성을 관리하는 역할을 한다.

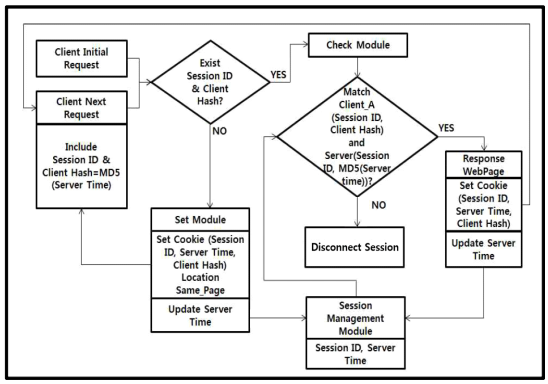

그림 3. 일회성 세션 키 인증 절차
Fig. 3. Authentication Process for One-time Session Key

IV. 구현 및 분석

1. 구현환경

본 논문에서 제안하는 메커니즘을 시험하기 위한 구성은 그림 4와 같다. 공격 대상이 될 웹 서버 1식과 공격 에이전트 5식 그리고 정상 사용자 PC 1대로 구성되어 있다. NAT환경에서도 제안한 메커니즘이 정상적으로 동작함을 보이기 위해 클라이언트 환경은 NAT환경으로 구성하였다.

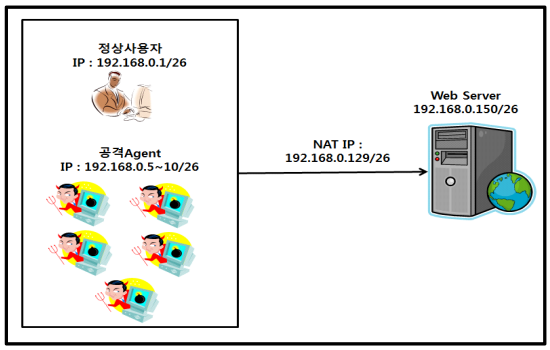

그림 4. 시험 환경 구성
Fig. 4. Configuration for Test

Slow Attack 상황에서 정상 사용자와 공격 에이전트를 식별하여 공격 에이전트만의 세션을 종료하는 것을 검증하기 위해 공격은 *Cache-Control DDoS* 유형으로 초당 2회의 연결을 지속적으로 유지하였다. 시험은 인증모듈 적용 전 · 후 동일하게 실시하였다. 공격상황에서 웹 서버의 가용성 점검을 위해 매 시험 시 매초마다 세션상태(*ESTABLISH, Time-Wait*)를 점검하고, 인증 모듈 적용 전후 정상 서비스 여부를 확인하기 위해 정상 사용자 PC 요청에 대해 일반적으로 패킷분석에

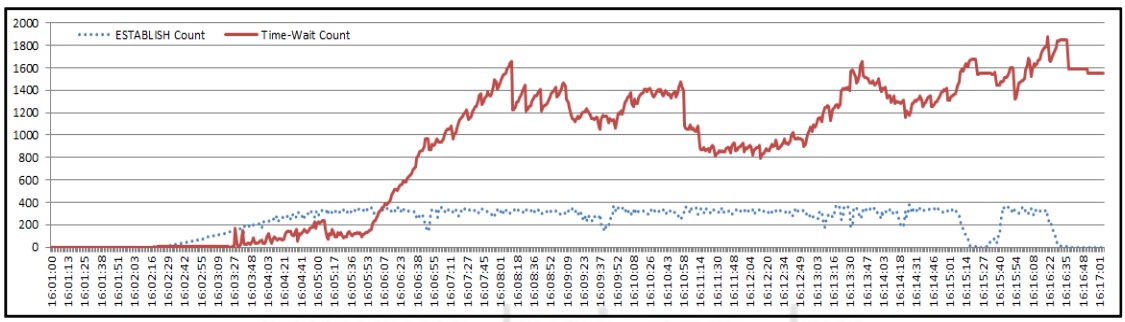

그림 5. 공격상황 세션 상태
Fig. 5. Session Status Under Attacks

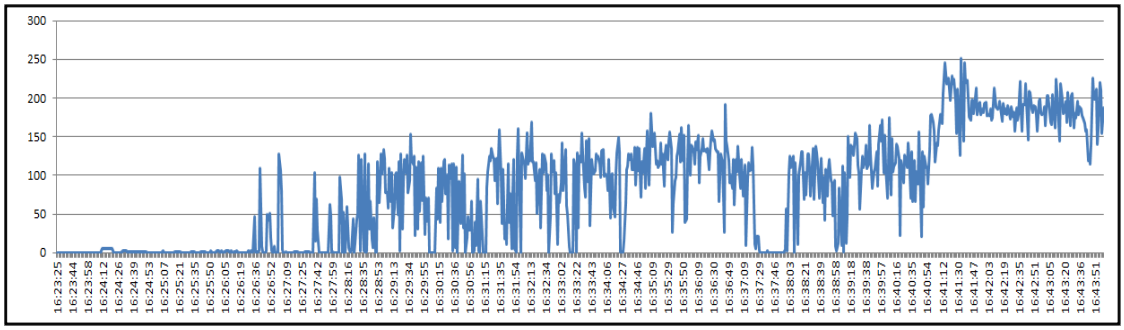

그림 6. 공격상황 : 인증모듈 적용 후 ESTABLISH 상태
Fig. 6. Under Attacks : ESTABLISH Status After Deploy Authentication Module

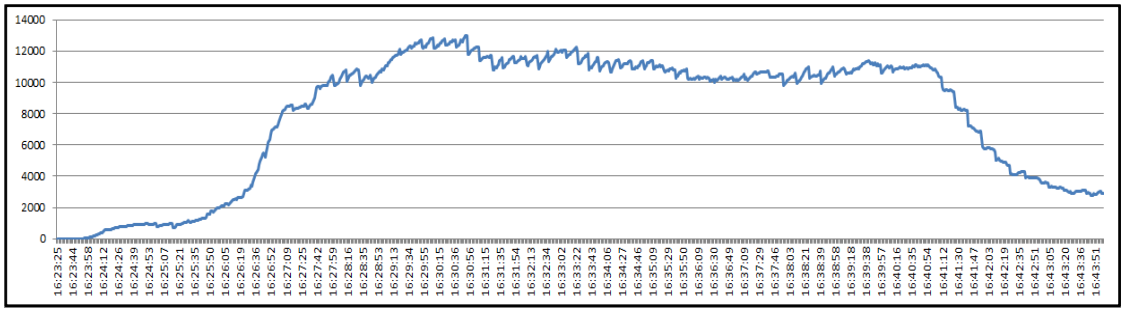

그림 7. 공격상황 : 인증모듈 적용 후 Time-Wait 상태
Fig. 7. Under Attacks : Time-Wait Status After Deploy Authentication Module

가장 많이 활용될 뿐 아니라 TCP 세션별 플로우를 직관적으로 확인할 수 있는 와이어샤크(WireShark) 도구를 이용하여 웹서버와 주고 받는 패킷의 내용을 확인하였다.

2. 시험결과

먼저 쿠키기반 일회성 세션 키 인증모듈을 설치하지 않은 상태에서 공격을 시도 하였을 때의 상황을 살펴보자. 그림 5에서 보이는 것처럼 웹서버의 *ESTABLISH* 상태는 공격이 지속된 시간 동안 300 ~ 350개 내외를 유지하며 웹서비스가 정상적으로 제공되지 않았다.

Time-Wait 상태는 초기 *ESTABLISH* 상태보다 작은 값을 유지하다가 일정 시간이 지난 후 증가하고 있으나 총 수가 1,000 ~ 1,800개 정도 사이에서 변화하고 있다. 이 같은 증상은 공격 에이전트의 연결요청에 대해 웹 서버에서 받아들일 수 있는 최대 연결 수를 유지하고 있다가 공격 에이전트가 연결을 종료했을 시점에 *Time-Wait* 상태로 천이되고 있음을 보여준다. 즉, 웹 서버는 공격 에이전트에 수동적으로 반응하는 전형적인 DDoS 상황을 보여준다고 할 수 있다.

반면, 일회성 세션 키 인증 모듈을 적용하였을 때의 웹서버의 상태를 보면 그림 6과 같이 *ESTABLISH* 상태는 초기에 순간적으로 100 ~ 150개 사이에서 변화하고 있으나 세션이 지속적으로 끊어지는 현상을 보여주고 있다. 이와 같은 증상은 웹 서버에 설치된 일회성 세션 키를 사용한 인증 모듈이 인증을 통과하기 못하는 세션을 강제로 종료하고 있는 것으로 분석된다. 즉, 지속적으로 공격 트래픽이 유입되고 있으나 전반적인 서비스 상태는 안정적으로 제공되는 것으로 분석된다.

특히 일회성 세션 키 인증 모듈이 적용된 후 *Time-Wait* 상태는 그림 7과 같이 최대 12,000개 까지 증가하고 있다. 공격 상황에서 웹 서버가 인증을 통과하지 못하는 세션을 강제 종료 하는 과정에서 발생되는 증상으로 분석되며, 공격 트래픽에 대해 웹 서버가 능동적으로 대응하고 있는 것으로 분석된다.

공격 상황에서 *NAT* 환경 내에 있는 정상 사용자 PC의 트래픽을 와이어샤크를 이용하여 분석한 결과는 다음과 같다. 정상 사용자 PC는 그림 8과 같이 *3-Wah Handshake* 이후에 *GET* 요청, 응답에 대한 분석 후 동일 세션으로 2차 *GET* 요청이 이루어지고, 이에 대해 웹 서버에서 세션을 인증하고 *Success*로 응답하고 있다. 또한 동일한 세션으로 지속적인 통신이 이루어지고 있는 것으로 분석된다. 즉 그림 3의 인증

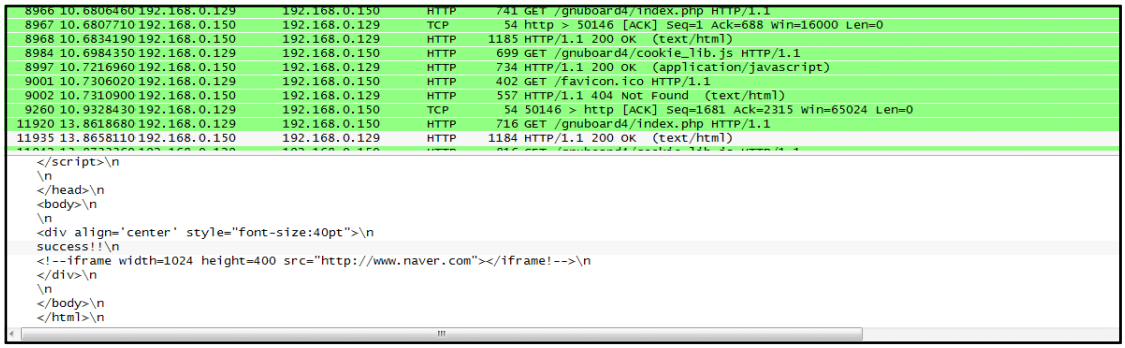

그림 8. 정상 사용자 통신 패킷
Fig. 8. Communication Packets of Normal Users

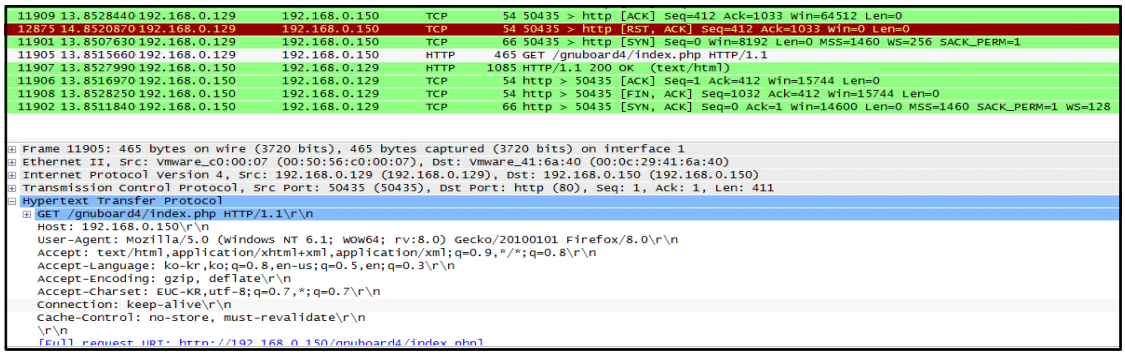

그림 9. 공격 에이전트 통신 패킷
Fig. 9. Communication Packets of Attack Agents

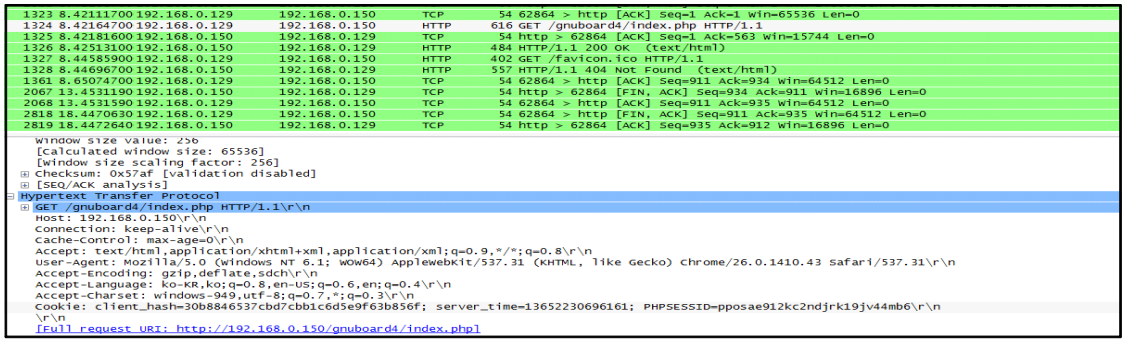

그림 10. 비정상 접속 통신 패킷
Fig. 10. Communication Packets of Abnormal Access

절차가 정상적으로 이루어진다.

반면, 공격 에이전트의 경우에는 그림 9와 같이 초기 *GET* 요청 후 추가적인 접속이 이루어지지 않는다. 이는 공격 에이전트는 웹 서버의 *Redirect* 응답에 대해 인지하지 못하여 추가적인 접속이 이루어지지 않으며 세션은 자동으로 종료되는 것으로 분석된다.

그림 3의 초기 Session_ID와 Client_hash 검사 모듈을 통과하기 위해 공격자가 임의로 Client_hash와 Session_ID를 생성하는 방법으로 패킷을 조작하는 경우에도 그림 10과 같이 웹 서버에서 응답되는 패킷은 *FIN*으로 종료되고 있다.

본 논문에서 제안한 일회성 세션키 기반 인증방법과 기존의 HTTP DDoS 대응방법의 특징을 비교하면 아래 표 3과

같이 정리할 수 있다.

표 3. HTTP DDoS 대응방법 비교
Table 3. Comparing HTTP DDoS Responses Method

대응방법	특징 (차단기반)	장점	단점
트래픽 특성 이용 차단	비정상 패킷 구분(IP기반)	차단기능 우수	NAT환경 정상IP 차단
트래픽 분산	트래픽을 별도의 공간으로 우회/분산 (IP기반)	백본 가용성 확보	NAT환경 정상IP 차단
캡챠 (CAPTCHA)	사용자 확인 (IP기반)	정상/비정상 사용자 구분 우수	사용자 개입으로 인한 불편
일회성 세션키 기반방어 (제안기법)	일회성 세션키 생성 (세션기반)	사용자 개입 없이 정상/비정상 구분, NAT환경 정상IP 가용성 보장	HTTP에 한정/ 대량 공격 시 효과적 적용 방안 연구 필요

V.결론

본 논문에서는 정상 사용자와 공격 에이전트를 식별하기 위해 매 접속 시 다른 값을 요청하는 일회용 세션 키 인증 방식을 사용하였다. 시험 결과 본 논문에서 제안한 메커니즘은 정상 사용자와 공격 에이전트를 효과적으로 식별하여 공격 에이전트가 생성한 세션을 종료시키는 방법으로 정상 사용자에 대한 서비스 가용성을 보장하고 웹 서버를 DDoS 공격으로부터 보호할 수 있음이 검증되었다. 또한 NAT와 같은 환경에서 이루어지는 공격에 대해서도 정상 사용자의 가용성을 보장할 수 있음이 검증되었다. 특히 본 논문에서 제시한 메커니즘은 기존 운영 중인 웹 서버의 설정을 크게 변경하지 않고 간단하게 적용이 가능한 방법으로 DDoS 방어를 위한 전용장비를 구축하기 힘든 소규모 사이트에서 효과적으로 사용이 가능할 것으로 예상된다.

다만 본 논문에서 제시한 메커니즘은 HTTP 프로토콜을 이용한 DDoS 공격을 제외한 OSI 3계층, 4계층 공격에 대해서는 능동적으로 대응하는데 한계가 있다. 또한 애플리케이션으로 동작하는 특성상 대규모 사이트를 대상으로 하는 대량 공격에 대해서는 방어성능에 한계가 있을 것으로 예상된다. 따라서 향후 본 논문에서 제안한 메커니즘을 확장하여 대규모 DDoS 공격에 대해서도 효과적으로 대응 할 수 있는 하드웨어기반 고성능 시스템의 연구가 필요하다.

참고문헌

[1] Changbaek Jang, "Using CDN Technique Smart DNS of DDoS Attack Protection," Master's Thesis, Soongsil University, 2010.

[2] Jungmin Choi, "Design of dynamic load balancing algorithm for anti-DDoS system," Master's Thesis, Konkuk University, 2011.

[3] SungSoo Park, "A Study on CAPTCHA-Based Mitigation of DDoS Attacks," Master's Thesis, Dongguk University, 2010.

[4] Jelena Mirkovic, Peter Reiher, "A Taxonomy of DDoS Attack and DdoS Defense Mechanisms," ACM SIGCOMM computer Communitions Review, Vol. 34, No. 2, pp. 39-54. April. 2004

[5] Jahyun Koo, "Type and Response for Denial of Service," *Institute for Information Technology Advancement, Weekly Technical Trends,* Vol. 1377, Dec. 2008.

[6] Jinwon Seo, "The Design of Anti-DDos System using Defense on Depth," Journal of Korea Institute of Information Security and Cryptology Vol. 22, No. 3, pp. 679-689, July, 2012.

[7] Kelly jackson Higgins, "Researchers To Demonstrate New Attack That Exploits HTTP", 2010 OWASP AppSec Conference, Nov. 2010

[8] Slowloris HTTP DoS, *http://ha.ckers.org/slowloris/*

[9] Slow Read DDoS, https://community.qualys.com */blogs/securitylabs/2012/01/05/slow-read*

[10] secunuews, http://www.ahnlab.com/kr/site */securityinfo/secunews/secuNewsView.do?menu_dist=2&seq= 16316*

[11] Ahnlab ASEC Report, http://download.ahnlab *.com/ asecReport/ASEC_Report_200907.pdf,*

[12] 3.4 DDoS Analysis Report, http://www. *ahnlab .com*

[13] Laura Feinstein, Dan Schnackenberg, "Statistial Approaches to DDoS Attack Detection and Response" DARPA Information Survivability conference and Exposition, pp. 303-314, April.

2003
〔14〕 Namgyun Baek, " A Study on Efficient DDoS Attack Defense Scheme Using Performance Measurement Metrics based on Web Protocol's Features," PhD thesis, Soongsil University, 2011.
〔15〕 Daeseop Lee, "Analysis of Defense Method for HTTP POST DDoS Attack base on Content-Length Control," Journal of Korea Institute of Information Security and Cryptology, Vol. 22, No. 4, pp. 809-817, August. 2012.
〔16〕 Dongmaeng Kim, "A Study of Information System Optimization for DDoS Attaks resopnse" Master's Thesis, Konkuk University, 2012.
〔17〕 Jonggap Jeung, "A client-based DDoS attack defense mechanism through user authentication" Master's Thesis, Korea University, 2012.
〔18〕 RFC 2109 - HTTP State Management Mechanism
〔19〕 RFC 2616 - Hypertext Transfer Protocol — HTTP/1.1

저 자 소 개

최 상 용
2000: 한남대학교 수학과.
2003: 한남대학교 컴퓨터공학과 공학석사
2012~현 재: 한국과학기술원 사이버보안연구센터 선임연구원
2009~현 재: 전남대학교 대학원 정보보호협동과정
관심분야: 네트워크 보안, 악성코드, 해킹
Email : csyong95@gmail.com

강 익 선
2012: 제주대학교 컴퓨터공학과
2012~현 재: 한국과학기술원 사이버보안연구센터 연구원
관심분야: 시스템 및 네트워크 보안
Email : ikseon1026@gmail.com

김 용 민
2002: 전남대학교 전산통계학과 박사
2004: 여수대학교 정보기술학부 전임강사
2006~현 재: 전남대학교 문화콘텐츠학부 부교수
관심분야: 시스템 및 네트워크 보안 전자상거래 보안 등
Email : ymkim@jnu.ac.kr