쿠키 자동인증을 이용한 HTTP DDoS 공격 방어기법

HTTP DDoS Defense Mechanisms using Cookies Auto-Authentication

저자
(Authors)

최상용, 김용민, 노봉남
SangYong Choi, YongMin Kim, BongNam Noh

출처
(Source)

한국정보과학회 학술발표논문집 , 2013.6, 712-714 (3 pages)

발행처
(Publisher)

한국정보과학회
KOREA INFORMATION SCIENCE SOCIETY

URL

http://www.dbpia.co.kr/Article/NODE02217243

APA Style

최상용, 김용민, 노봉남 (2013). 쿠키 자동인증을 이용한 HTTP DDoS 공격 방어기법. 한국정보과학회 학술발표논문집, 712-714.

쿠키 자동인증을 이용한 HTTP DDoS 공격 방어기법

최상용[O1], 김용민[2], 노봉남[3]
[1]한국과학기술원 사이버보안연구센터/전남대학교 정보보호협동과정
[2]전남대학교 문화콘텐츠학부, [3]전남대학교 컴퓨터정보학부
csyong95@kaist.ac.kr, {ymkim, bbong}@jnu.ac.kr

HTTP DDoS Defense Mechanisms using Cookies Auto-Authentication

SangYong Choi[O1], YongMin Kim[2], BongNam Noh[3]
[1]KAIST Cyber Security Research Center/Interdisciplinary of Information Security, Chonnam National University
[2]Dept. of Electronic Commerce, Chonnam National University
[3]Dept.of Electronics Computer Engineering, Chonnam National University

요 약

77DDoS 대란 이후 DDoS 공격은 사회적 위협으로 발전하고 있다. 이러한 위협에 대응하기 위해 다양한 DDoS 방어기법이 연구되고 있으나, DDoS 공격기법이 정교해지고 공격을 수행하는 공격에이전트 또한 더욱 지능화 되어 차단이 더욱 어렵게 되고 있다. 이러한 한계점을 개선하기 위해 본 논문에서는 HTTP 프로토콜에서 사용하는 쿠키 기반의 자동인증 방법을 적용하여 공격 에이전트와 정상 PC를 구분하고, 공격을 방어할 수 있는 방법을 제안한다.

1. 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. 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 NAT환경 내에 악성코드에 감염된 PC에서 발생하는 트래픽과 정상 PC에서 발생하는 트래픽이 혼재할 경우 차단하는 지점에서는 해당 IP 주소를 차단할 것인지 여부를 판단하기가 매우 어렵게 된다.

본 논문에서는 이러한 문제점을 해결하고자 HTTP 프로토콜에서 사용하는 쿠키를 이용하여 매 접속마다 다른 쿠키 값을 요구하는 방식으로 정상 사용자와 비정상 공격에이전트를 구분하는 방법을 제안하고자 한다.

2. 관련 연구

2.1 HTTP DDoS 공격 분류

최근 실제 많이 발생되는 DDoS 공격은 플루딩 형태와 연결공격 그리고 애플리케이션 공격 등 3가지로 분류하고 플루딩 공격에 대해서는 출발지가 변조되었는 지와 변조되지 않았는지 여부에 따라 다시 분류하는 방법을 사용한다[4].

표 1. DDoS 공격 분류

분류	특징	공격유형
Flooding 공격	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 공격	HTTP공격	HTTP Daemon 개수 이상 초과
	과다 TCP Connection	Application의 input queue 마비
Application 공격	Application 특성 이용	FTP공격, Time 공격, VoIP주소공격, Email 등

그러나 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 공격의

712

성공률을 높이기 위해 HTTP 프로토콜을 이용한 OSI 7계층 형태로 변화하고 있다. OSI 7계층 DDoS 공격에 대한 세부적인 분류는 표 2와 같이 가능하다[5].

표 2. OSI 7계층 DDoS 공격 분류

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

2.2 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[6], Slowloris[7], Slow Read DDoS[8], Cache-Control DDoS[9] 등이 있다. Slow Attack은 동작하는 형태는 상이하나 공통적인 특징은 대량 트래픽을 발생시키지 않고 소량 트래픽을 발생시키되 세션연결을 지속하는 기법을 사용하여 웹서버의 자원을 모두 소모시키는 방법으로 웹서버의 가용성을 침해한다는 것이다. HTTP 프로토콜을 이용한 공격기술은 2009년 발생된 77DDoS, 2011년 발생된 34DDoS 공격에도 사용되었으며, 향후 지속적인 위협이 될 것으로 예상하고 있다[10],[11].

2.3 DDoS 공격 대응기술

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 방법[12],[13]을 이용하여 DDoS 공격을 차단하고 있다. 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]까지 다양하게 연구되고 있다. 또한 최근 멀티 레이어 DDoS 공격에 효과적으로 대응하기 위한 방안으로 OSI 3계층, 4계층, 7계층 보안장비를 혼합한 다단계 방어기법도 연구되고 있다[5].

2.4 기존 DDoS 공격 대응기술의 한계 및 개선방안

DDoS 공격에 효과적으로 대응하기 위해 지속적으로 많은 연구가 이루어지고 있으나 크게 두 가지 측면에서 한계점이 도출된다.

첫 번째로 지금까지 살펴본 기술들은 IP차단을 기본으로 하고 있다. 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 방법인 시도응답(Challenge-Response) 방식을 기반으로 하는 캡챠를 사용한다. 하지만 캡챠를 사용한 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.

본 연구에서는 이와 같은 문제점을 해결하기 위해 HTTP 쿠키기반 공격 에이전트 탐지 방법을 제안한다. 캡챠와 같은 사용자 개입이 필요한 인증방식으로 인한 불편을 해결하기 위해 사용자의 개입 없이 클라이언트에게 매번 다른 값을 요구하는 HTTP 쿠키를 사용하여 공격 에이전트와 정상 사용자를 구분한다.

3. 쿠키인증 기반 공격에이전트 탐지 방법

본 논문에서 제안하는 쿠키인증 기반 차단 방법은 그림 1과 같이 동작한다.

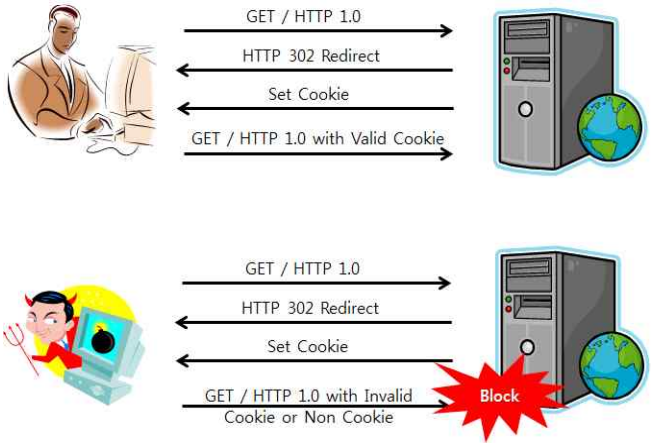

그림 1. Cookie를 이용한 사용자 인증 메커니즘

인증 메커니즘에서 먼저 클라이언트에서 웹서버로 요청되는 모든 값에 대해 쿠키를 보내는 것은 클라이언트의 최초 요청 후 응답에 포함되게 된다. DDoS 공격의 특성 상 세션을 유지한 상태에서 요청을 보내는 것이 아니라 매번 새로운 요청을 보내기 때문에 웹서버의 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

713

유입을 방지하게 된다. 지능화된 공격 에이전트의 경우 *Redirect*를 인지하여 새로운 접속이 이루어 질 때에는 웹 서버에서 보내는 쿠키에 정상적으로 응답을 해야 한다. 만약 쿠키에 정상적인 응답을 하지 못한다면 이는 공격 에이전트로 간주하고 세션을 즉시 종료한다.

사용자 인증을 위해 웹서버에서 클라이언트로 요청되는 쿠키에는 유효성 검증을 위해 두 가지의 방법이 적용된다. 첫 번째 방법은 재사용 방지를 위한 매 요청마다 변하는 서버의 시간을 사용한 Time-Stamp와 두 번째 방법은 전송된 Time-Stamp에 대한 해시 값(Client_Hash)을 요청하게 된다. 즉, 웹서버에서 송신되는 쿠키에 매번 서버의 응답시간을 입력하고 접속자 PC 로 하여금 수신된 시간에 대한 해시 값을 요청하여 쿠키의 재사용을 방지하고 매번 클라이언트가 해시를 계산하게 함으로 공격에이전트에 의한 자동적으로 생성되는 트래픽에 대한 식별이 가능하게 한다. 쿠키를 이용한 사용자 인증 메커니즘은 그림2와 같이 동작하게 된다. *Client_Hash* 생성을 위한 함수는 일반적으로 웹에서 제공하는 MD5 또는 SHA-1 라이브러리를 이용하여 일반적인 상용 브라우저에서 사용이 가능하도록 구현한다.

```
for each request from client
  if not exist Session_ID, Client_Hash in request then
    set-cookie (Session_ID, Client_Hash(Now server time))
    save (Session_ID, Hash(Now server time)) to server
    send 302 Redirection to client
  else if (cookie values in request header (Session_ID,
        Client_Hash) == saved vlues(Session_ID,
        Hash(Now server time)) then
      normal response include set-cookie values
      (Session_ID, Client_Hash(Now server time)) and
      save (Session_ID, Hash(Now server time)) to server
  else Connection Close and Alert Generate
  done
```

그림 2. *Client_Hash* 검증을 통한 비정상 접속 식별 절차

또한 본 논문에서 제안하는 방식은 별도의 전용장비가 필요하지 않으며 웹서버 내에 쿠키인증에 관련된 자바스크립트를 만들어 놓고 사용자 접속 시 자바스크립트만을 호출하면 간단한 방법을 사용할 수 있기 때문에 저비용으로 기본적인 HTTP DDoS 공격방어가 가능할 것으로 예상된다.

4. 결론

본 논문에서는 정상 사용자와 공격 에이전트를 식별하기 위해 매 접속 시 다른 값을 요청하는 일회성 쿠키 인증 방식을 사용하였다. 일회용 쿠키를 기반으로 공격 에이전트와 정상 사용자를 식별함으로 서 공격 에이전트가 맺은 비정상 세션만을 차단할 수 있다. 또한 일회성 쿠키를 사용함으로 공격자가 패킷덤프 등으로 통해 쿠키를 재사용 하는 것을 원천적으로 방지할 수 있다.

또한 NAT와 같은 환경에서 이루어지는 공격에 대해서도 정상 사용자의 가용성을 보장할 수 있을 것이다. 특히 본 논문에서 제시한 메커니즘은 기존 운영 중인 웹 서버의 설정을 크게 변경하지 않고 간단하게 적용이 가능한 방법으로 DDoS 공격방어를 위한 전용장비를 구축하기 힘든 소규모 사이트에서 효과적으로 사용이 가능할 것으로 예상된다. 향후 본 논문에서 제안한 방법을 구현하고 시험하여 제안 알고리즘의 효과성을 검증하는 부분의 연구가 필요할 것이다.

참고문헌

[1] 장창백, “CDN상에서 지능형 DNS를 이용한 DDoS 공격 방어,” 석사학위논문, 숭실대학교, 2010
[2] 최정민, “DDoS 대응 시스템을 위한 동적 부하분산 알고리즘의 설계,” 석사학위논문, 숭실대학교, 2011
[3] 박성수, “CAPTCHA를 이용한 DDoS 공격 대응에 관한 연구,” 석사학위논문, 동국대학교, 2010
[4] 구자현, “서비스 거부 공격(Denial of Service)의 유형 및 대응,” 주간기술동향, 1377호, pp.6, 2008
[5] 서진원, 곽진, “다단계 방어기법을 활용한 DDoS 방어 시스템 설계,” 정보처리학회 논문지 제22권 제3호, pp. 679-689, 2012
[6] Kelly jackson Higgins, “Researchers To Demonstrate New Attack That Exploits HTTP”, 2010 OWASP AppSec Conference, 2010
[7] Slowloris HTTP DoS, http://ha.ckers.org/slowloris/
[8] Slow Read DDoS, https://community.qualys.com/blogs/securitylabs/2012/01/05/slow-read
[9] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=16316
[10] Ahnlab ASEC Report, http://download.ahnlab.com/asecReport/ASEC_Report_200907.pdf, 2009
[11] 3.4 DDoS 분석보고서, Ahnlab, http://www.ahnlab.com, 2012
[12] Jelena Mirkovic, Peter Reiher, “A Taxonomy of DDoS Attack and DdoS Defense Mechanisms,” ACM SIGCOMM computer Communitions Review, Volume 34, Number 2, pp. 39-54. 2004
[13] Laura Feinstein, Dan Schnackenberg, “Statistial Approaches to DDoS Attack Detection and Response” DARPA Information Survivability confference and Exposition, pp. 303-314, 2003
[14] 백남균, “웹 서비스 특성 기반 성능평가지표를 통한 효율적인 DDoS대응 기업에 관한 연구,” 박사학위논문, 숭실대학교, 2011
[15] 이대섭, 이동호, “Content-Length 통제기반 HTTP POST DDoS 공격 대응 방법 분석,” 정보보호학회논문지 제 22권 4호, pp. 809-817, 2012
[16] 김동맹, “DDoS 공격 대응을 위한 정보시스템 최적화 방안연구,” 석사학위논문, 건국대학교, 2012
[17] RFC 2616 - Hypertext Transfer Protocol — HTTP/1.1

714