분산 서비스 거부 공격 대응을 위한 Secure-NIC 시스템 설계 및 구현

김병구, 김대원, 오진태, 장종수, 김익균
한국전자통신연구원
e-mail : {bkkim05, dwkim77, showme, jsjang, ikkim21}@etri.re.kr

Design and Implementation of Secure-NIC System for DDoS Attack Response

Byoungkoo Kim, Daewon Kim, Jin-tae Oh, Jong-soo Jang, Ikkyun Kim
Electronics Telecommunications Research Institute

요 약

인터넷의 발전과 더불어 네트워크 상에서의 침입 시도가 갈수록 증가되고 다변화되고 있으며, 특히, 네트워크나 서버의 가용성을 위협하는 형태의 서비스 거부(DoS: Denial of Servie) 공격이 최근 급증하고 있다. 따라서, 본 논문에서는 인터넷 서버의 정상적인 서비스 제공을 방해하는 형태의 분산 서비스 거부(DDoS: Distributed Denial of Service) 공격으로부터 서버를 보호하고 원활한 서비스를 제공하기 위한 Secure-NIC 시스템의 설계 및 구현에 대해서 설명한다. 이는 "CISGDP : CPU-Independent Service Guaranteed DDoS Protection" 이라는 설계 개념하에서, 각종 인터넷 서버에 장착되어 DDoS 공격 등의 네트워크 공격에 대하여 서버의 고유 서비스가 지속적으로 보장될 수 있도록 자체 보안 기능을 NIC(Network Interface Card) 형태로 제공한다.

1. 서론

인터넷 기반 서버의 가용성을 위협하는 형태의 DDoS 공격이 최근 급증하고 있으며, 이러한 공격의 형태는 주요 웹사이트나 루트 DNS 서버에 대한 공격처럼 국가나 인터넷 기반체계를 대상으로 매우 광범위하게 전개되고 있는 실정이다. 과거에는 DDoS 공격의 대상으로서 네트워크 인프라 마비를 목표로 하는 사례도 있었으나, 최근에는 금전적인 갈취나 정치적 목적으로 특정 서비스를 제공하는 서버를 직접 공격하는 사례가 대세를 이루고 있다.

본 논문은 서버의 정상적인 서비스를 방해하는 형태의 DDoS 공격으로부터 서버를 보호하고 원활한 서비스를 제공하기 위한 NIC 형태의 DDoS 공격 차단 기술로써, 악의적인 사용자의 공격 시도에 대하여 서버의 성능 감소 없이 원천적으로 차단하는 방법에 관한 것이다. 이는 악의적인 사용자의 행위에 대하여 네트워크 인터페이스 카드에 내장된 고속 DDoS 대응 로직을 통하여 비정상적인 공격 행위들을 근본적으로 차단함으로써 서버의 CPU 부하 증가가 전혀 없도록 서버를 보호하게 한다. 따라서, 정상적인 사용자의 응용 서비스 사용은 원활하게 제공하면서, 악의적인 사용자의 서버 접근을 식별, 실시간으로 차단하는 방법을 제공한다. 본 논문에서 제안한 방법의 주요 장점은 리눅스 및 윈도우 등 OS 제약 사항에 관계없이 투명하게 제공될 수 있으며, 서버의 고유 서비스를 제공함에 있어 성능적 오버헤드가 전혀 없는 구조로 고성능 공격 방어 처리를 보장한다는 것이다.

본 논문의 구성은 2 장에서 DDoS 공격 대응 시스템들에 대한 기존의 연구 결과 및 동향들에 대해서 살펴보고, 3 장에서 DDoS 공격 대응을 위한 Secure-NIC 시스템의 설계 내용에 대해서 설명한다. 4 장에서는 설명된 기술의 구현 결과 및 테스트 환경을 보여주며, 마지막으로 5 장은 결론 및 향후 계획에 대해 기술한다.

2. 관련 연구

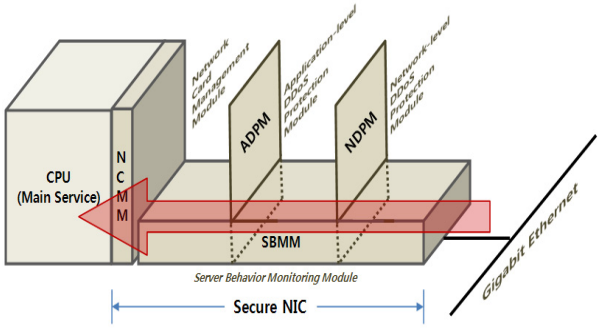
DDoS 공격의 종류를 구분해 보면, 크게 네트워크 프로토콜 취약점을 이용하는 네트워크 레벨의 공격과 응용 계층의 취약점을 이용하는 공격으로 나눌 수 있다. 응용계층 레벨의 공격의 대표적인 것이 HTTP GET flooding 공격[1]이며, 네트워크 레벨 공격 중 TCP 와 관련된 공격은 TCP SYN floodng, TCP flag flooding (ACK, FIN, RST 필드 등) 공격, TCP 연결 설정 공격 등이 있으며, 이는 전체 DDoS 공격의 90%를 차지한다[2]. 이 중에서도 TCP SYN flooding 공격은 대표적인 공격 방법으로서, 단순한 공격 기법임에도 불구하고 명확한 대응방법이 없는 게 현실이다. 최근에는 UDP/ICMP flooding 공격 또한 많은 이슈로 등장하고 있지만 UDP, ICMP 트래픽의 대역폭 조절[3], Random Dropping[4] 이외에 뚜렷한 방안이 제시되지 못하고 있는 실정이다.

2009 년 7.7 DDoS 공격 사고와 2010 년 3.4 DDoS 공격과 같이 최근 DDoS 공격은 그 형태가 다양한 유형의 공격 조합을 이용하기 때문에 한 가지 대응 방

법이 DDoS 공격을 방어할 수 있는 경우는 없다고 할 수 있고, 여전히 TCP 프로토콜을 이용한 네트워크 공격이 큰 비중을 차지하고 있는 현실이다. 특히, 네트워크나 서버의 가용성을 위협하는 형태의 서비스 거부 공격이 최근 급증하고 있다. 따라서, 호스트 단에서의 네트워크 보안 기능에 대한 요구가 증가하고 있으나, DDoS 공격 방어, 고급 보안 기능 등이 탑재된 형태의 시스템이나 제품은 현재까지 전무한 상황이다.

3. Secure-NIC 시스템 설계

Secure-NIC 시스템은 "CISGDP : CPU-Independent Service Guaranteed DDoS Protection" 이라는 설계 개념 하에서, 각종 인터넷 서버에 장착되어 DDoS 공격 등의 네트워크 공격에 대하여 서버의 고유 서비스가 지속적으로 보장될 수 있도록 자체 보안 기능을 NIC 형태로 제공할 수 있는 구조를 갖는다. (그림 1)은 이와 같은 개념을 갖는 Secure-NIC 시스템의 전체 구조를 보인다.



(그림 1) Secure-NIC 시스템 구조

Secure-NIC 시스템은 상기의 그림과 같이 4 개의 기능 모듈로 구성된다. 각 기능 모듈은 개념적으로 유사한 기능을 수행하는 블록들의 모음으로써, 다음과 같은 기능을 갖는다.

- NDPM(Network-level DDoS Protection Module) : 네트워크 레벨의 DDoS 공격에 대응하기 위한 기능 모듈로써, TCP SYN Cookie 기능을 이용한 SYN flooding 공격 대응 및 기타 TCP flag flooding 공격, UDP/ICMP flooding 공격에 대한 대응 기능을 갖는다.
- ADPM(Application-level DDoS Protection Module) : 어플리케이션 레벨의 DDoS 공격에 대응하기 위한 기능 모듈로써, HTTP GET flooding, DNS flooding 과 같은 서비스 응용에 대한 DDoS 공격 대응 기능을 갖는다.
- SBMM(Server Behavior Monitoring Module) : 서버의 서비스 상태를 Watchdog 형태로 모니터링하여 이상 유무를 탐지하여 대응하는 기능 모듈로써, 하드웨어 로직을 우회한 비정상 행위들을 탐지, 대응하는 기능을 갖는다.
- NCMM(Network Card Management Module) : 정규 네트워크 인터페이스 카드로써의 기본적인 전달 및 관리 기능을 제공하기 위한 기능 모듈로써, 시스템 전반에 대한 제어 기능을 갖는다.

상기와 같은 하드웨어 기반의 기능 모듈들을 통해서, Secure-NIC 시스템은 서버 CPU 의 부하 증가 없는 DDoS 대응 기능을 제공하게 된다. 또한, 하드웨어를 통한 탐지가 불가능한 형태의 미래의 공격에 대해서, 서버 모니터링 기능을 추가함으로써 대응토록 하였다. 이와 같은 NIC 형태의 시스템 구조는, 특정 서버로의 DDoS 공격 상황에서도 정상적인 사용자에게 해당 서버의 서비스가 지속적으로 원활하게 제공될 수 있다는 장점을 제공한다.

4. Secure-NIC 시스템 구현 및 운영 환경

본 논문에서 설명한 NIC 기반의 DDoS 공격 대응 기술은 CPU 의 부하 없이 DDoS 공격에 효율적으로 대응하기 위해서 개발되었다. 즉, 기가비트 이더넷 환경과 같은 고속 네트워크 환경에서의 보다 정확한 DDoS 공격 탐지 기법을 제공하고, 이를 통해 서버의 원활한 서비스를 제공하고자 하였다. 본 연구진에서는 이를 바탕으로 한 프로토타입으로써 Secure-NIC 시스템을 개발하였다. 기본적으로 Secure-NIC 시스템의 하드웨어 로직은 Xilinx FPGA 상에서 도작하도록 구현되었으며, CPU 를 통한 제어가 가능토록 하였다. (그림 2)은 Secure-NIC 시스템의 일환으로 제작된 프로토타입 보드를 나타내며, 이를 여러 웹 호스팅 서비스를 위한 테스트 서버들에 장착하여 지속적으로 시험 운용하고 있다.

(그림 2) Secure-NIC 보드

5. 결론 및 향후 연구 방향

본 논문에서는 기가비트 이더넷 환경과 같은 고속 네트워크 환경에 적합한 보안 제어 기능을 제공하기 위한 기반 기술로써, 하드웨어 기반의 NIC 형태를 갖는 DDoS 공격 대응 기술을 설명하였다. 또한, 이러한 기술의 필요성과 수행 기법들에 대해서 간략히 설명하였다. 무엇보다도, 이러한 기술을 갖는 Secure-NIC 시스템을 통해서 여러 DDoS 공격 행위들을 탐지하고 차단하는 기능을 제공하고자 하였다. 본 논문에서 제안한 Secure-NIC 시스템은 리눅스 및 윈도우 등 OS 제약 사항에 관계없이 투명하게 운영될 수 있으며, 서버의 고유 서비스를 제공함에 있어 성능적 오버헤드가 전혀 없는 구조로 고성능 DDoS 공격 대응 기법을 제공할 수 있다.

앞으로는 여러 시험을 통해서 나오는 문제점들을

보완하고, 보다 정확한 DDoS 공격 탐지 기능을 제공하기 위한 기법들을 연구해 나가고자 한다. 이외에 실제 웹 호스팅 서버들에 실 장착하여 운영함으로써, 안정성을 검증해 나가고자 한다.

참고문헌

[1] Wei Zhou Lu, and Shun Zheng Yu, “A HTTP flooding detection method based on browser behavior,” 2006 International Conference on IEEE Computational Intelligence and Security, vol 2, pp. 1151-1154, Nov. 2006.

[2] D. Moore, G. Voelker, and S. Savage, “Inferring internet denial of service activity,” Proceedings of USENIX Security Symposium ’2001, Aug. 2001.

[3] J. Udhayan and R. Anitha, “ Demystifying and rate limiting ICMP hosted DoS/DDoS flooding attacks with attack productivity analysis,” Advanced Computing Conference, IACC 2009. IEEE International, pp. 558-564, Mar. 2009.

[4] L. Ricciulli, P. Lincoln, and P. Kakkar, “TCP SYN flooding defense,” In Comm. Net. and Dist. Systems Modeling and Simulation Conf. (CNDS' 99), 1999 Western MultiConf. (WMC' 99), Jan. 1999.