2006년도 대한전자공학회 하계종합학술대회 제29권 제1호

IPsec의 보안상 문제점과 해결방안

김정현*, 원유집*, 임을규**
한양대학교 전자통신컴퓨터공학부*
한양대학교 정보통신대학 컴퓨터전공**

A security problem and its solution in IPsec

Junghyun Kim*, Youjip Won*, Eulgyu Im**
Department of Electronics and Computer Engineering, Hanyang University*
The College of Information and Communications, Hanyang University**
E-mail : *junghyun@ece.hanyang.ac.kr, *yjwon@ece.hanyang.ac.kr, **imeg@hanyang.ac.kr

Abstract

In this paper, we describe a security problem of IPsec. And we propose a solution for this problem. The problem is a fragility of IPsec Gateway which is used in tunnel mode. The role of IPsec Gateway is encrypting or decrypting IPsec packets. Because of the role of IPsec Gateway, IPsec Gateway suffers overhead for decrypting numerous packets. Adversaries can easily attack IPsec Gateway using a DDoS attack. To solve this problem, we propose the “Priority based Random Packet Drop” method. In this method, the white list which is a list of normal users is created. After that, according to the frequency of uses, the method marks priorities of random drops to the white list. If anomalous traffic appeared, this method will drop many packets which consist of anomalous traffic. In simple experiment, we show our solution is proper to defend IPsec Gateway. For this experiment, we use empirical backbone traffic which includes DoS attacks.

I. 서론

인터넷 표준인 IPv4 의 문제점을 해결시켜 줄 것으로 기대되는 IPv6 가 발표되었다[1]. IPv6 에는 IPv4 에서 고려되지 않았던 보안 기술이 포함되었는데, 이를 IPsec (IP security)라고 한다[2]. IPsec 의 모드에는 전송모드 (transport mode)와 터널모드(tunnel mode)가 있는데, 터널모드가 일반적을 사용된다. 터널모드를 위해서는 IPsec gateway 가 필요하다. 주목해야 할 것은 DDoS 공격에 대한 IPsec gateway 의 취약성이다. IPsec gateway 는 IPsec 의 터널모드에서 패킷 암호화를 처리하기 때문에, 대량의 트래픽이 발생할 경우 처리시간이 급격히 증가하게 된다. 이것은 DDoS 공격을 위해 충분한 조건이다[3]. IPsec gateway 가 다운될 경우, 해당 네트워크의 모든 컴퓨터는 외부와 통신이 불가능하게 된다. 본 논문에서는 IPsec gateway 의 DDoS 공격에 대한 취약성에 대해 살펴보고, 해결책을 제시할 것이다. 실험에서는 실제로 발생한 DoS 공격을 대상으로 제안한 방법을 검증하였다.

II. 본론

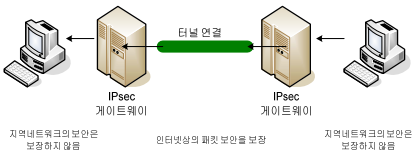


그림 1 IPsec gateway 의 구성

IPsec 은 VPNs(Virtual Private Networks)를 위한 암호화 프로토콜의 집합이다[1][2]. IPsec 은 전송모드 또는 터널모드로 동작하며, 터널모드가 많이 사용된다. 그림 1 에서 볼 수 있듯이, 터널모드에서는 IPsec gateway 를

두고 암호화된 패킷을 주고 받을 수 있도록 한다. 이때 패킷의 IP 헤더는 완전히 암호화되어 보호되며, 새로 추가된 IPsec 헤더에는 IPsec gateway 주소만 표현된다. 따라서 공격자가 패킷을 가로챈 후, 트래픽을 볼 수 없게 한다. 이때 IPsec gateway 의 역할은 원본 패킷을 받아서 암호화하고 새로운 IP 헤더를 포함시키는 것이다. 이러한 IPsec gateway 의 동작 과정에서 비교적 많은 연산이 필요하다. 이것은 DoS(또는 DDoS)공격 대상이 되기에 충분하다[3]. IPsec gateway 앞에 일반적인 방화벽을 사용 할 수 없다[2]. 방화벽은 IPsec gateway 에 의해 해독된 트래픽에 대해서만 필터링을 수행할 수 있기 때문이다. 결국 딜레마에 빠지게 된다. 즉, IPsec 은 보안을 위해서 사용되지만, DDoS 공격은 IPsec gateway 를 쉽게 무력화시킬 수 있으므로 또다른 보안문제가 발생된다.

본 논문에서는 지금까지 많은 연구들이 DoS(또는 DDoS)공격을 바라봤던 관점[2]과 다른 관점으로 해결책을 제시한다. DDoS 공격이 발생했을 때, 이상트래픽(anomalous traffic)을 쉽게 구분할 수 있는 방법은 존재하지 않는다. 이상트래픽은 정상패킷(normal traffic)으로 구성되기 때문이다. 본 논문에서는 "IPsec gateway 가 감당할 수 없는 트래픽이 유일될 때, 이상트래픽이 발생했다" 라고 가정한다. 가정에 의해 이상트래픽이 발생되었다고 판단되면, 그림 2 의 "우선순위 기반 랜덤 패킷 버림 알고리즘"을 사용해서 IPsec gateway 가 정상 서비스를 유지할 수 있는 트래픽만 유입되도록 한다. 임의의 기간 동안 패킷의 통계정보를 이용하여 정상적 서비스를 받는 source address 목록인 화이트리스트를 작성한다. 감당할 수 없는 트래픽이 발생하면 화이트리스트에 포함되지 않은 패킷 위주로 패킷을 버린다. 1 차 버림이 충분하지 않을 경우, 화이트리스트에 포함되는 패킷을 우선순위에 따라 버림한다. 버림 할 우선순위는

$$priority = \frac{packet\_frequency\_for\_1sec\_of\_attack\_period}{(packet\_frequency\_at\_whitelist) \div 3600}$$

로 표현한다. 우선순위 값이 1 이상이면 버림 대상이다.

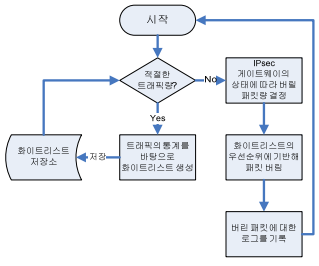
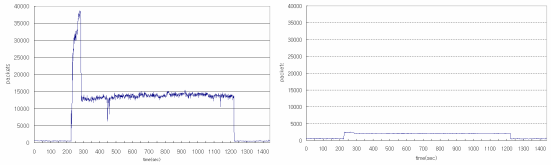


그림 2 우선순위 기반 랜덤 패킷 버림 알고리즘

Ⅲ. 실험

제안한 알고리즘에 대한 검증을 위해, 실제로 발생한 DoS 공격을 대상으로 실험했다. 이 데이터는 국외에서 국내로 유입되는 UDP 트래픽이며 Multiple Ports UDP flooding 공격[3]을 포함하고 있다. 공격은 수십분 동안 지속되었다. 매초마다 제안한 알고리즘이 얼마나 적절히 DoS 공격 패킷을 버리는지 관찰하였다. 그림 3 (a)에 비해서 그림 3 (b)에서는 많은 양의 트래픽이 버려진 것을 확인할 수 있다. 화이트리스트에 저장된 정상 패킷은 모두 통과시켰으며, 대부분의 공격 패킷이 버려진 것을 확인할 수 있었다.



(a) 적용 전 (b) 적용 후

그림 3 알고리즘 적용 결과

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 IPsec gateway 의 보안상 취약점을 설명하였고, 해결책을 제시하였다. IPsec 은 주로 터널모드로 사용되며, 이때는 IPsec gateway 가 필요하다. 주목했던 문제점은 IPsec gateway 가 DoS 공격에 취약하다는 점이다. IPsec gateway 는 보안을 위해 존재하지만 어쩔 수 없이 공격에 노출될 수 밖에 없는 딜레마가 발생한다. 이에 대한 해결책으로 본 논문에서는 " 우선순위 기반 랜덤 패킷 버림 알고리즘 " 을 제안하였다. 실제로 발생한 DoS 공격 트래픽을 대상으로 제안한 알고리즘의 정당성을 검증하였다. 향후 과제로는 IPsec gateway 에 대한 실제 실험을 수행하는 것이다.

참고문헌

[1] IETF, "The "next generation" protocol," in www.ipv6.org.

[2] R. R. Panko, Corporate Computer and Network Security: Prentice Hall, 2004.

[3] D. Moore, G. M. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," presented at The 2001 USENIX Security Symposium, 2001.