情報保護學會論文誌
第16卷 第4號, 2006. 8

IPv6 환경에서 비정상 IPSec 트래픽 대응 보안 시스템 설계*

김 가 을,† 고 광 선, 경 계 현, 강 성 구, 엄 영 익‡
성균관대학교

Design of a Security System to Defeat Abnormal IPSec Traffic in IPv6 Networks*

Kaeul Kim,† Kwangsun Ko, Gyehyeon Gyeong,
Seong-Goo Kang, Young Ik Eom‡
Sungkyunkwan University

요 약

IPv6 네트워크에서는 기본 보안 메커니즘인 IPSec 메커니즘을 사용함으로써, 통신 양자 간에 전송되는 데이터에 대한 무결성 및 기밀성을 보장하고, 데이터와 통신 주체에 대한 인증을 실시할 수 있다. 그러나 IPSec 메커니즘을 악용하여 대량의 비정상 트래픽(세션설정 단계 또는 통신 단계의 비정상 IPSec 트래픽)을 전송하였을 경우, IPSec 메커니즘 자체에서 해당 패킷을 차단하는 데 한계가 있다. 본 논문에서는 IPv6 네트워크 환경에서 IPSec 메커니즘의 ESP 확장헤더에 의해 암호화된 패킷의 비정상 여부를 복호화 없이 IPSec 세션테이블과 설정테이블을 이용하여 탐지함으로써, 성능향상을 가질 수 있는 효과적인 보안 시스템에 대한 설계 내용을 보이고자 한다. 또한 설계는 단계적 대응 메커니즘[1,2]를 기반으로 한다.

ABSTRACT

The IPSec is a basic security mechanism of the IPv6 protocol, which can guarantee an integrity and confidentiality of data that transmit between two corresponding hosts. Also, both data and communication subjects can be authenticated using the IPSec mechanism. However, it is difficult that the IPSec mechanism protects major important network from attacks which transmit mass abnormal IPSec traffic in session-configuration or communication phases. In this paper, we present a design of the security system that can effectively detect and defeat abnormal IPSec traffic, which is encrypted by the ESP extension header, using the IPSec Session and Configuration table without any decryption. This security system is closely based on a multi-tier attack mitigation mechanism which is based on network bandwidth management and aims to counteract DDoS attacks and DoS effects of worm activity.

Keywords : *IPSec, IPv6, Intrusion Prevention System, Security*

Ⅰ. 서 론

IPv6(Internet Protocol version 6)[3] 네트워크에서 IPSec(IP Security) 프로토콜은 기본 보안 메커니즘으로 사용할 수 있도록 정의되었으며, IPSec 프로토콜을 적용할 경우 통신 양자 간에 전송되는 데

접수일: 2006년 6월 2일 ; 채택일: 2006년 7월 28일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학IT 연구센터 육성지원 사업의 결과로 수행되었음
† 주저자, zfall@ece.skku.ac.kr
‡ 교신저자, yieom@ece.skku.ac.kr

이터에 대한 무결성 및 기밀성을 보장하고, 데이터와 통신 주체에 대한 인증할 수 있다[4]. 그러나 IPSec 프로토콜을 악용하여 대량의 비정상적인 세션설정 요청 메시지를 전송하거나 IPSec 보안이 적용된 패킷에 비정상적인 데이터를 포함하여 전송하였을 경우, IPSec 프로토콜 자체에서 해당 패킷을 대응하는 데에는 한계가 있다. 또한 불특정 다수의 사용자 간에 통신을 하는 경우와 성능 제한이 있는 임베디드 기기 간 통신할 경우를 고려하면, 보안이 필요한 특정 컴퓨팅 환경에서만 IPSec 프로토콜이 사용될 가능성이 높다. 따라서 IPSec 프로토콜이 적용되지 않는 컴퓨팅 환경에서는 지금까지 개발되어 사용된 보안 기술에 IPv6 프로토콜 특성을 반영함으로써 효과적인 IPv6 기반 보안 시스템 개발이 가능하지만, IPSec 프로토콜이 적용된 컴퓨팅 환경 중에서 특히 ESP (Encapsulating Security Payload)[5] 확장헤더를 사용한 환경에서는 악의적인 데이터가 암호화된 패킷에 포함되어 전송될 가능성이 존재하기 때문에 기존에 사용된 보안 기술로는 이러한 공격에 대응하기 어렵다.

이러한 컴퓨팅 환경에 사용할 수 있는 보안 기술로 가장 많이 언급하고 있는 기법으로는 ESP 확장헤더를 암호화/복호화 하는 과정에서 사용된 키를 보안 시스템과 IPSec 통신 주체 간에 공유하는 방법이다. 그러나 이 기법은 보안 시스템에서 해당 패킷에 대한 암호화 및 복호화 과정을 통하여 패킷 유해성 유무를 확인하기 때문에 패킷 전송지연 문제가 발생할 수 있으며, 통신 주체 간 보안(IPSec 프로토콜이 전송모드로 동작하였을 경우)을 보장한다는 IPSec 프로토콜의 기본 원칙에도 다소 위배된다.

따라서 본 논문에서는 IPSec 프로토콜의 ESP 확장헤더에 의해 암호화된 악의적인 패킷을 제어할 수 있는 보안 시스템에 대해 설계한 내용을 보이고자 한다. 설계된 보안 시스템은 ESP 확장헤더에 포함되어 있는 SPI(Security Parameter Index)와 sequence number 항목을 기반으로 세션 테이블을 구성하여 IPSec 프로토콜을 악용한 대량의 비정상 트래픽에 대한 대응이 가능하다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 살펴보고, 3장에서 IPSec 프로토콜이 적용된 패킷을 악용한 공격의 특성을 알아본다. 4장에서는 해당 보안 시스템에 대한 설계 내용과 보안 시스템의 대응 시나리오에 대해 기술한다. 5장에서 설계된 보안 시스템과 기존 보안 시스템 간 비교 및 평가하고, 6장에서는 결론 및 향후 연구 내용을 각각 기술한다.

II. 관련 연구

IPv6 네트워크에서 비정상 IPSec 트래픽을 차단하기 위하여 지금까지 연구된 기법은 크게 두 부류로 나눌 수 있다. 첫 번째는 기존 IPv4 네트워크에서 사용되던 방식으로 IP 헤더정보와 상위계층 정보를 이용하여 오용행위 또는 비정상행위를 탐지하여 대응하는 기법(IP 헤더정보 기반 보안 시스템)이고, 두 번째는 IPSec 세션설정 및 통신을 담당하는 호스트 또는 보안 게이트웨이와 보안 시스템 간 IPSec 통신에 사용되는 키를 공유하여 해당 공격을 대응하는 기법[6](키 분배 기반 보안 시스템)이다.

IP 헤더정보 기반 IPv6 보안 시스템은 암호화된 IPSec 트래픽 자체를 처리하지 못하거나 처리하더라도 기본 헤더 정보인 송/수신 IP 주소만으로 비정상 IPSec 트래픽을 탐지하게 된다. 송/수신 IP 주소만으로 공격을 탐지하는 방법은 분산서비스거부공격과 같이 여러 호스트에서 하나의 목표 호스트로 대량의 트래픽을 발생시키는 공격이 이루어지면 정상적인 호스트의 트래픽까지 탐지되어 차단될 수 있는 단점이 존재한다.

키 분배 기반 IPv6 보안 시스템은 ESP 확장 헤더가 적용된 암호화된 데이터를 공유한 키로 복호화하여 탐지하고 대응한다. 하지만 이러한 시스템은 키를 분배하기 위해서 추가적인 IPSec 통신을 연결하거나 키 값을 직접 복사해주어야 하고 IPSec 종단 간 보안이 깨지는 단점이 존재한다. 추가적인 IPSec 통신을 연결할 경우, 보안 시스템에서 다른 키로 암호화하는 과정을 수행해야 하기 때문에 처리 시간이 늘어나고 키 값을 직접 전달할 경우, 해당 IPSec 세션의 키로 다시 암호화 과정을 수행하지 않는다면 내부의 악의적인 사용자가 패킷의 내용을 볼 수 있기 때문에 IPSec의 기밀성이 깨진다.

III. 공격 특성

IPSec 프로토콜 기반 통신에서 공격이 발생할 수 있는 시점은 크게 IPSec 프로토콜 세션설정 단계와 통신 단계로 구분할 수 있으며, 통신 단계는 다시 보안 구간에 따라서 전송모드와 터널모드로 구분된다[7].

표 1. 세션설정 단계에서 발생할 수 있는 공격 특성

단계	패킷 암호화 여부			공격 방법
	ESP 헤더	상위계층 헤더	페이로드	
Phase 1	X	X	X	Phase 1에 해당하는 비정상 트래픽 대량 전송
Phase 2	X	X	O	Phase 2에 해당하는 비정상 트래픽 대량 전송

본 장에서는 공격발생 시점과 보안 구간에 따라 발생할 수 있는 공격 특성에 대해 기술한다.

1. 세션설정 단계에서 발생할 수 있는 공격의 특성

IPSec 프로토콜에서 세션설정 단계는 UDP의 500번 포트를 이용하는 ISAKMP(Internet Security Association and Key Management Protocol)[8] 프로토콜을 사용하며, 세부적으로 Phase 1(Aggressive 모드, Main 모드)과 Phase 2(Quick 모드)로 나눠진다[9]. 표 1에서 보이는 바와 같이 Phase 1의 패킷은 패킷의 모든 항목들(ESP 헤더, 상위계층 헤더, 페이로드)이 암호화되지 않기 때문에 공격자는 IPSec 세션설정 패킷을 의도적으로 생성할 수 있으며, 생성된 패킷을 대량 전송함으로써 IPSec 세션을 설정하고자 하는 노드를 공격할 수 있다. 또한 Phase 2는 Phase 1에서 교환된 비밀키로 ISAKMP 프로토콜의 페이로드 부분만 암호화되기 때문에, Phase 1과 동일하게 공격자는 악의적인 패킷을 대량 전송함으로써 IPSec 세션을 설정하고자 하는 노드를 공격할 수 있다.

표 2. 통신 단계에서 발생할 수 있는 통신 모드별 공격 특성 (아래 그림 참조)

구분	공격자	공격 대상	공격 방법
전송모드	N_A내 SH_a를 제외한 임의의 호스트	SH_b	암호화된 비정상 IPSec 패킷 대량 전송
터널모드	N_C 내 임의의 호스트 H_e	N_D내 임의의 호스트 H_f	비정상 트래픽 대량 전송 (복호화된 트래픽)
		N_D의 SG_d	암호화된 비정상 IPSec 패킷 대량 전송
	N_C와 N_D에 속하지 않는 임의의 호스트	N_D의 SG_d	암호화된 비정상 IPSec 패킷 대량 전송

* 편의상 아래 그림에서 공격자는 좌측 네트워크에 존재한다고 가정함

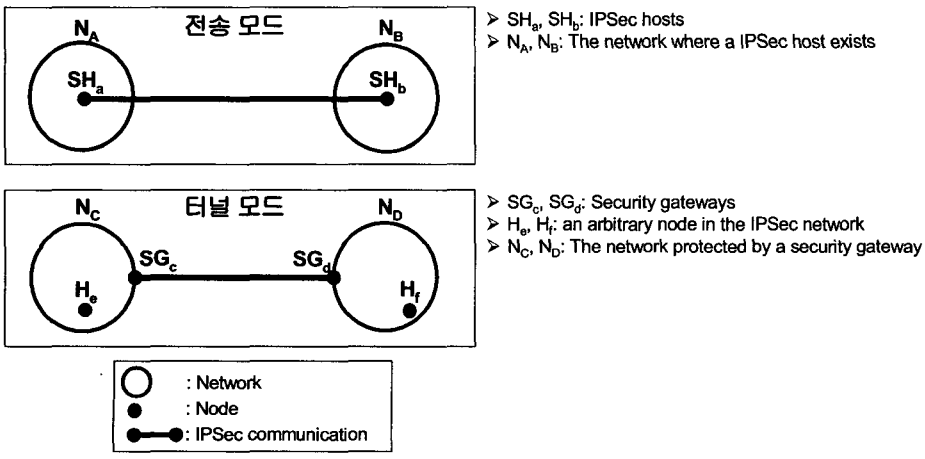

그림 1. IPSec 모드별 네트워크 구조

표 3. IPSec 세션 테이블

출발지 IP 주소	도착지 IP 주소	SPI	Sequence number
X	Y	0x09086FC2	2
Y	X	0x00DFEDF1	4
Z	X	0x020CA801	1

2. 통신 단계에서 발생할 수 있는 공격의 특성

IPSec 세션설정 단계 완료 후, IPSec 프로토콜의 통신 단계에서도 패킷의 페이로드 항목이 암호화되지만, 임의의 IPSec 패킷을 대량으로 전송하는 방식으로 IPSec 통신에 참여하는 노드를 공격할 수 있다. 통신 단계는 전송모드와 터널모드로 구분할 수 있으며, 각 모드별 발생할 수 있는 공격 특성을 표 2에서 보인다.

표 2에서 보이는 바와 같이, 전송모드는 주로 호스트와 호스트 사이에 단-대-단 보안을 요구할 때 사용되며, IPSec 통신을 수행하는 양단의 노드에서만 패킷의 내용을 확인할 수 있다. 따라서 공격자는 IPSec 통신을 수행하는 호스트(그림에서 SH_a)를 제외한 임의의 호스트가 될 수 있으며, IPSec 호스트(그림에서 SH_b)에 암호화된 비정상 IPSec 패킷을 대량으로 전송하는 공격이 가능하다. 터널모드는 주로 네트워크와 네트워크 간 보안을 요구할 때 사용되며, IPSec 패킷은 보안 게이트웨이(그림에서 SG_c와 SG_d)에서 암호화 및 복호화 과정이 수행된다. 따라서 공격자는 IPSec 통신 내부 네트워크(그림에서 N_c)에 존재하는 경우와 IPSec 통신에 참여하지 않는 외부(그림에서 N_c와 N_d에 속하지 않는 외부 호스트)에 존재하는 경우가 있다. 공격자의 위치가 내부 네트워크일 때, 공격 대상이 보안 게이트웨이(그림에서 SG_d)인 경우에는 암호화된 대량의 비정상 IPSec 트래픽을 전송하는 공격이 가능하고, 공격 대상이 내부 네트워크의 호스트(그림에서 H_f)인 경우에는 보안 게이트웨이(그림에서 SG_d)를 거치면서 복호화 되기 때문에 대량의 일반 IPv6 비정상 트래픽을 전송하는 공격이 가능하다. 또한 공격자가 IPSec 통신에 참여하지 않는 외부에 존재할 경우에는 상대방 보안 게이트웨이에 대량의 비정상 IPSec 트래픽을 전송하는 공격이 가능하다.

Ⅳ. 세션테이블 기반 보안 시스템 설계

본 장에서는 2장에서 설명한 특성을 가진 공격을 차단할 수 있도록 IPSec 세션 테이블과 IPSec 설정 테이블을 기반으로 동작하는 보안 시스템을 설계한다.

1. IPSec 세션 테이블과 IPSec 설정 테이블

IPSec 세션 테이블이란 보안 시스템에서 비정상 IPSec 트래픽을 차단하기 위해 IPSec 세션 정보를 관리하는 테이블을 말하며, 정상 IPSec 세션이 공격으로 탐지되지 않도록 하고 IPSec 기술을 악용한 트래픽에 대응하기 위해 사용한다. IPSec 세션 테이블은 표 3과 같이 구성된다.

표 3에서 보이는 IPSec 세션 테이블의 엔트리는 IPSec 패킷의 IP 헤더와 ESP 확장헤더에 존재하는 출발지/도착지 주소, SPI, 그리고 sequence number 항목[5]을 이용하여 생성 및 갱신되고, 관리자가 직접 삭제한다. IPSec 설정 테이블이란 IPSec 세션 테이블의 신뢰도를 높이기 위한 용도로 사용하

표 4. IPSec 설정 테이블

출발지 IP 주소	도착지 IP 주소	모드(Exchange Type)	Count
X	Y	Quick Mode (32)	2
Y	X	Quick Mode (32)	2
Z	X	Aggressive Mode (1)	1

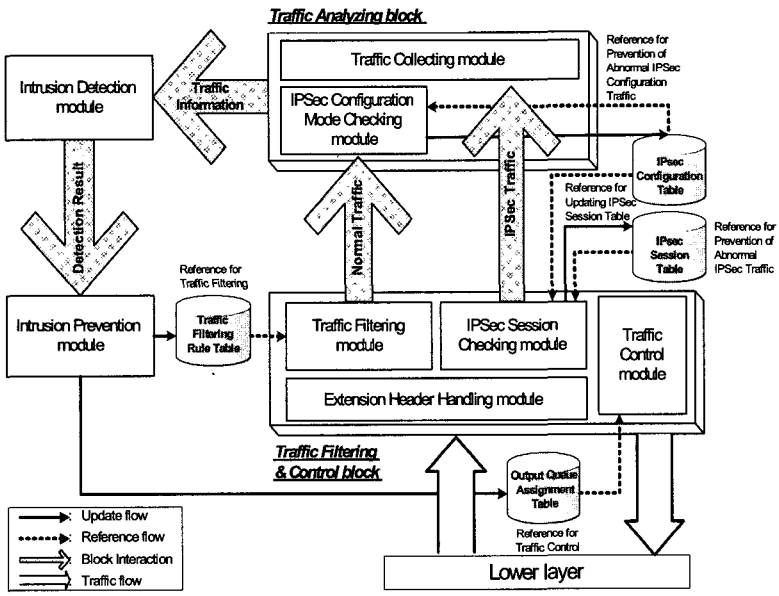

그림 2. 비정상 IPSec 트래픽에 대한 보안 시스템 구조도

기 위하여 IPSec 세션설정 정보를 관리하는 테이블을 말하며 표 4와 같이 구성된다.

표 4에서 보이는 IPSec 설정 테이블의 엔트리는 IPSec 설정 패킷의 IP 헤더에 존재하는 출발지/도착지 주소와, 상위 프로토콜의 ISAKMP 헤더에 존재하는 통신모드, 그리고 이러한 IPSec 설정 패킷이 전달된 횟수를 이용하여 생성 및 갱신되고, 보안 정책에 의해 설정된 타임아웃을 초과한 경우에 삭제된

표 5. 보안 시스템을 구성하는 각 블록 및 모듈에 대한 세부 기능

블 록	모 듈	설 명
트래픽 필터링 및 제어 블록	확장헤더 처리 모듈 (Extension Header Handling module)	· 수신한 트래픽의 확장헤더를 확인하여 일반 트래픽과 IPSec 트래픽으로 구분 - 일반 트래픽*은 트래픽필터링 모듈로 전달 - IPSec 트래픽은 IPSec 세션확인 모듈로 전달
	IPSec 세션확인 모듈 (IPSec Session Checking module)	· IPSec 설정 테이블과 IPSec 세션 테이블을 참조하여 IPSec 세션의 정상 여부 검사 - 정상일 경우, 해당 트래픽을 포워딩하기 위하여 트래픽제어 모듈로 전달하고, IPSec 터널모드의 내부 네트워크 공격을 탐지하기 위하여 해당 트래픽의 복사본을 공격탐지 블록으로 전달 - 비정상일 경우, 해당 트래픽 차단 · IPSec 통신 단계에서 패킷의 sequence number가 1인 경우, 세션 테이블 참조 - 세션설정이 완료된 경우, IPSec 세션 테이블에 세션정보 저장 - 세션설정이 완료되지 않은 경우, 해당 트래픽 차단
	트래픽필터링 모듈 (Traffic Filtering module)	· 일반 트래픽*은 필터링 규칙과 비교하여 해당 패킷의 정상 여부 결정 - 정상일 경우, 해당 트래픽을 IPSec 설정모드 확인 모듈로 전달 - 비정상일 경우, 해당 트래픽 차단
	트래픽제어 모듈 (Traffic Control module)	· 해당 트래픽을 하위 계층으로 전달 - IPSec 트래픽일 경우, IPSec 세션확인 모듈이 전달한 IPSec 트래픽을 하위 계층으로 전달 - 일반 트래픽*일 경우, 출력큐 설정 정보를 기반으로 해당 트래픽의 출력 대역폭 조절하여 하위 계층으로 전달

블 록	모 듈	설 명
트래픽 분석 블록	IPSec 설정모드 확인 모듈 (IPSec Configuration Mode Checking module)	· IPSec 메커니즘이 적용되지 않은 트래픽의 경우, 해당 트래픽을 트래픽분석 모듈로 전달 · IPSec 세션설정 단계에 해당하는 트래픽의 경우, UDP 헤더에서 포트번호가 500번인 패킷(ISAKMP)의 IPSec 설정 모드 정보(Mode Type)를 IPSec 설정 테이블에 저장한 후, 해당 트래픽을 트래픽분석 모듈로 전달
	트래픽수집 모듈 (Traffic Collecting module)	· 입력 트래픽의 비정상 여부를 확인하기 위해 필요한 정보를 수집하여 공격탐지 모듈로 전달
공격탐지 모듈**		· 일반 트래픽과 IPSec 트래픽을 보안 관리자가 설정한 임계값을 기준으로 공격 여부 판단 · 공격으로 판단되거나 의심될 경우, 공격대응 모듈에 규칙 생성에 필요한 정보 전달 - 공격으로 판단될 경우, 트래픽필터링 규칙 생성에 필요한 정보 전달 - 공격으로 의심될 경우, 트래픽제어 규칙 생성에 필요한 정보 전달
공격대응 모듈**		· 공격탐지 모듈로부터 전달받은 정보를 이용하여 트래픽필터링 규칙 또는 트래픽 제어 규칙을 생성하여 트래픽필터링 테이블 또는 출력큐설정 테이블에 각각 저장

* 일반 트래픽은 IPSec 메커니즘이 적용되지 않은 트래픽과 IPSec 세션설정 단계에 해당하는 트래픽을 모두 포함함
** 공격탐지 모듈과 공격대응 모듈의 구체적인 메커니즘은 단계적 대응 시스템[1][2]에 설명됨

다. IPSec 설정 테이블에서 정상적으로 설정 단계를 완료한 세션만이 IPSec 세션 테이블에 추가되기 때문에 IPSec 세션 테이블의 신뢰도를 높일 수 있다.

2. 보안 시스템 설계

본 논문에서 제안하는 비정상 IPSec 트래픽에 대한 보안 시스템의 구조는 그림 2와 같다. 그림 2에서 보이는 바와 같이, 보안 시스템은 크게 트래픽필터링 및 제어 블록(Traffic Filtering and Control block), 트래픽분석 블록(Traffic Analyzing block), 공격탐지 모듈(Intrusion Detection module), 그리고 공격대응 모듈(Intrusion Prevention module)으로 구성되며, 각 모듈들의 세부 기능은

```
When packet comes from Link Layer:
Begin
 [Extension Header Handling module]
 IF Packet is IPSec Packet THEN
 [IPSec Session Checking module]
 IF Packet information exists in IPSec Session table THEN
 GOTO SUBROUTINE
 ELSE
 IF IPSec sequence number is one THEN /* IPSec New Session Check */
 IF Packet information exists in IPSec Configuration Table THEN
 Update IPSec Session Table
 GOTO SUBROUTINE
 ELSE /* Packet did not process the IPSec configuration step */
 DROP packet
 END IF
 ELSE /* Packet is not IPSec session */
 DROP packet
 END IF
 END IF
 [END IPSec Session Checking module]
 ELSE /* IPv6 Packet Handling Routine */
 [Traffic Filtering module]
 IF Packet information exists in Traffic Filtering Rule Table THEN
 DROP packet
 ELSE
```

```
 GOTO FORWARD and Send packet info. to IPSec Configuration Mode Checking module
 [IPSec Configuration Mode Checking module]
 IF Packet is IPSec configuration packet THEN
 Update IPSec Configuration Table
 END IF
 [END IPSec Configuration Mode Checking module]
 END IF
 [END Traffic Filtering module]
 [Intrusion Detection module]
 IF Traffic is detected as intrusion THEN
 [Intrusion Prevention module]
 IF Traffic is detected First THEN
 Update Output Queue Assignment Table
 ELSE
 Update Traffic Filtering Rule Table
 END IF
 [END Intrusion Prevention module]
 END IF
 [END Intrusion Detection module]
 END IF
 [END Extension Header Handling module]
END

SUBROUTINE:
Begin
 IF Packet information exists in Traffic Filtering Rule Table THEN
 Alarm to Manager
 Update Queue Assign Table
 END IF
 GOTO FORWARD and Send packet info. to Intrusion Detection module
END

FORWARD:
Begin
 [Traffic Control module]
 IF traffic information exists in Output Queue Assignment Table THEN
 Forward the traffic to a lower Layer through limited network bandwidth;
 ELSE
 Forward to a lower Layer;
 END IF
 [END Traffic Control module]
END
```

그림 3. 모듈별 보안 시스템의 동작 과정

표 5에서 보이고 구체적인 동작 방식은 그림 3의 알고리즘에서 설명한다.

제안된 보안 시스템은 비정상 IPSec 트래픽을 탐지하고 대응하기 위해서 두 가지 기법을 사용한다. 첫 번째는 앞서 설명된 IPSec 세션 테이블과 설정 테이블을 이용한 탐지 및 대응기법이고 두 번째는 IPSec 임계값을 두어 탐지 및 대응하는 기법이다. 첫 번째 기법은 정당한 IPSec 세션을 등록하고 등록되지 않은 IPSec 트래픽에 대해 탐지하고 대응하는 방법이고 두 번째 기법은 공격자가 IPSec 내부 네트워크에 위치한 경우나 패킷 헤더정보를 정상 IPSec 세션과 동일하게 위조한 경우에 IPSec 세션 테이블이나 설정 테이블 만으로는 공격을 탐지하기 어렵기 때문에 공격탐지 모듈에 IPSec 트래픽의 임계값을 두어 이 임계값을 넘을 경우, 탐지하고 대응하는 방법이다.

그림 3에서 보이는 모듈별 보안 시스템의 동작과정을 기반으로 IPSec 세션설정 단계와 IPSec 통신 단계에서 발생할 수 있는 각 공격에 대한 대응 시나리오는 표 6과 같다. 표 6의 Ⓐ, Ⓒ, Ⓓ 시나리오에

표 6. IPSec 단계별 공격 대응 시나리오

구 분		공격자 위치	공격방법	대응 시나리오
Ⓐ 세션설정 단계		외부 네트워크	비정상 트래픽 대량 전송	① IPSec 세션설정 단계에 해당하므로 일반 트래픽으로 구분됨 ② 트래픽분석 블록의 IPSec 설정모드확인 모듈에서 IPSec 설정 테이블을 참조하여 정상 IPSec 세션설정 트래픽 여부 확인 후 공격탐지 모듈에 패킷정보 전달 ③ 공격탐지 모듈에서 임계값을 이용하여 탐지 ④ 공격대응 모듈에서 대응규칙 생성 ⑤ 트래픽필터링 모듈 및 트래픽 제어 모듈에서 단계적 대응
통신 단계	터널 모드	Ⓑ 내부 네트워크	암호화된 IPSec 비정상 트래픽 대량 전송	① 공격탐지 모듈에서 IPSec 임계값을 이용하여 탐지 및 관리자에게 경고 ② 공격대응 모듈에서 대응규칙 생성(트래픽제어) ③ 트래픽제어 모듈에서 부분적 대응 (해당 트래픽의 대역폭 감소)
		Ⓒ 외부 네트워크	암호화된 IPSec 비정상 트래픽 대량 전송	트래픽필터링 및 제어 블록의 IPSec 세션확인 모듈에서 IPSec 세션 테이블을 참조하여 정상 IPSec 세션 여부 확인 및 대응
	전송 모드	Ⓓ 외부 네트워크	암호화된 IPSec 비정상 트래픽 대량 전송	트래픽필터링 및 제어 블록의 IPSec 세션확인 모듈에서 IPSec 세션 테이블을 참조하여 정상 IPSec 세션 여부 확인 및 대응

해당하는 공격 대응 기법은 그림 4에서 보이고, 표 6의 Ⓑ 시나리오에 해당하는 공격 대응 기법은 그림 5에서 보인다.

먼저 공격자가 IPSec 세션설정 단계에 해당하는 트래픽을 악용하여 비정상 트래픽을 대량으로 전송할 경우, 해당 IPSec 세션설정 트래픽은 암호화되지 않기 때문에 설정 정보를 유지하는 IPSec 설정 테이블을 이용하여 대응이 가능하다. 예를 들어, 위조된 임의의 IPSec 설정단계 트래픽이 모두 Phase 1에 해당하지만 실제 IPSec 설정 테이블은 Phase 2의 트

X	Y	0x09086FC2	2
Y	X	0x00DFEDF1	4
Z	X	0x020CA801	1
.	.	.	.

X	Y	32	2
Y	X	32	2
Z	X	1	1
.	.	.	.

CASE	Packets	대응결과	IPSec Session Table	IPSec Configuration Table
#1	Source IP : Y Destination IP : X SPI : 0x00DFEDF1 Sequence #: 5	전달	테이블 갱신	IPSec 통신 단계 패킷이므로 설정테이블과 비교하지 않음
#2	Source IP : B Destination IP : X SPI : 0x0100CF11 Sequence #: 10	차단	테이블에 존재하지 않음	IPSec 통신 단계 패킷이므로 설정테이블과 비교하지 않음
#3	Source IP : A Destination IP : X SPI : 0x09086FC2 Sequence #: 1	차단	테이블에 존재하지 않음 Seq. #1이기 때문에 설정 테이블 참조	테이블에 존재하지 않음
#4	Source IP : Z Destination IP : X Mode : 32	차단	IPSec 설정 단계 패킷이므로 세션테이블과 비교하지 않음	응답이 가지 않았음에도 불구하고 다음 설정 단계 패킷이 전달됨
#5	Source IP : C Destination IP : X Mode : 1	전달	IPSec 설정 단계 패킷이므로 세션테이블과 비교하지 않음	테이블 갱신

그림 4. 세션 테이블과 설정 테이블을 이용한 대응 기법 (대응 시나리오 Ⓐ, Ⓒ, Ⓓ)

Y	X	0x00DFEDF1	4
.	.	.	.

Packets		IPSec 임계값	대응 결과	IPSec Session Table
Source IP : Y Destination IP : X	SPI : 0x00DFEDF1 Sequence #: 5	이하	전달	정상 IPSec 세션
Source IP : Y Destination IP : X	SPI : 0x00DFEDF1 Sequence #: 6	이하	전달	정상 IPSec 세션
... ...		... ...	... ...	... ...
Source IP : Y Destination IP : X	SPI : 0x00DFEDF1 Sequence #: 924	이하	전달	정상 IPSec 세션
Source IP : Y Destination IP : X	SPI : 0x00DFEDF1 Sequence #: 925	이하	전달	정상 IPSec 세션
Source IP : Y Destination IP : X	SPI : 0x00DFEDF1 Sequence #: 926	이상	관리자에게 경고 단계적 대응	테이블 삭제

그림 5. IPSec 통신 내부 공격자에 의한 공격 또는 IPSec 헤더를 정상적인 세션으로 조작한 대량의 비정상 IPSec 트래픽 대응 기법 (대응 시나리오 Ⓑ)

래픽을 기다린다면 이러한 공격 트래픽은 IPSec 설정 테이블과 비교한 후 차단이 가능하다. 또한 공격자가 IPSec 통신 단계의 터널모드에서 암호화된 IPSec 비정상 트래픽을 대량으로 전송할 경우, IPSec 세션확인 모듈에서 세션 테이블과 비교하여 트래픽의 세션 정보가 존재하지 않는다면 탐지되어 차단하거나 그림 5와 같이 공격탐지 모듈에서 IPSec 임계값 이상의 트래픽이 전송되면 탐지되어 대응한다. 전자의 경우는 공격자가 외부 네트워크에 위치한 경우이고, 후자의 경우는 공격자가 내부 네트워크에 위치하거나 IPSec 헤더 정보를 정상적인 세션으로 조작한 경우이다. 그리고 공격자가 IPSec 통신 단계의 전송모드에서 암호화된 IPSec 비정상 트래픽을 대량으로 전송할 경우, IPSec 세션확인 모듈에서 세션 테이블을 참조하여 정상적인 세션이면 하위 계층과 공격탐지 모듈로 전달하고, IPSec 세션 테이블에 해당 트래픽에 대한 세션 정보가 없다면 해당 트래픽을 차단한다.

이와 같이 동작하는 보안 시스템을 리눅스를 이용하여 구현할 경우, netfilter와 CBQ(Class based Queue)를 이용할 수 있다. 리눅스 시스템에서는 IPv6 프로토콜을 지원하는 netfilter6 프레임워크를 제공[10]하며, netfilter6 프레임워크가 제공하는 5개의 훅 포인트를 이용하여 네트워크로 수신되는 IPSec 트래픽과 출력 IPSec 트래픽에 대한 작업을 실시할 수 있다. 따라서 본 논문에서 제안하는 보안 시스템은 netfilter6 프레임워크 상에 커널 모듈 프로그래밍 기법으로 구현할 수 있으며, 구현된 보안 시스템은 응용계층에 구현되는 보안 시스템보다 매우 효율적으로 동작할 수 있다[11,12]. 또한 트래픽에 대한 단계적 대응을 위하여 리눅스 커널에서 지원하는 CBQ 메커니즘을 사용할 수 있다. CBQ 메커니즘은 서비스품질보장 기술을 지원하기 위해 제공되는 큐의 한 종류로서 하나의 출력 큐 대신에 여러 개의 큐를 두어 각 큐에 트래픽을 조절한다. CBQ 메커니즘은 각 큐에 트래픽을 할당하여 특정 트래픽이 네트워크 대역폭 전체를 독점하지 않도록 함으로써 서비스품질을 보장한다[13].

V. 기존 기법과 비교

본 장에서는 기존에 제안되었던 IP 헤더 기반 보안 시스템, 키 분배 기반 보안 시스템, 그리고 본 논문에서 제안하는 보안 시스템 간 비교를 실시한다. 평가 항목은 크게 보안성과 성능 항목으로 분류할 수 있으며, 각각 세부 항목으로 구분하여 비교한다. 자세한 내용은 표 7에서 보인다.

성능 항목의 실시간 처리는 대량의 비정상 트래픽 공격의 실시간 탐지 및 대응 가능성에 대한 것으로 보안 시스템에서 실시간으로 트래픽을 처리하지 못한

표 7. IP 헤더 기반 보안 시스템, 키 분배 기반 보안 시스템, 제안하는 보안 시스템 간 비교

평가 항목 \ 분류		IP 헤더 기반 보안 시스템	키 분배 기반 보안 시스템	제안하는 보안 시스템
보안성	IPSec 기술을 이용하지 않은 대량의 비정상 트래픽	오용행위 또는 비정상행위 대응기법을 이용할 경우 가능	오용행위 또는 비정상행위 대응기법을 이용할 경우 가능	공격탐지 모듈과 공격대응 모듈을 이용하여 대응 가능
	IPSec 설정단계를 악용하는 트래픽	오용행위 또는 비정상행위 대응기법을 이용할 경우 가능	오용행위 또는 비정상행위 대응기법을 이용할 경우 가능	IPSec 설정 테이블을 이용하여 대응 가능
	IPSec 전송모드를 악용하는 트래픽	불가능	분배된 키를 이용하여 대응 가능	IPSec 세션 테이블을 이용하여 대응 가능
	IPSec 터널모드 트래픽 (공격자가 외부네트워크에 존재하는 경우)	불가능	분배된 키를 이용하여 대응 가능	IPSec 세션 테이블을 이용하여 대응 가능
	IPSec 터널모드 트래픽 (공격자가 내부네트워크에 존재하는 경우)	불가능	분배된 키를 이용하여 대응 가능	부분적으로 가능*
성능	실시간 처리	높음	낮음 (복호화 및 암호화 과정 반복)	높음
	세션 재설정 지연시간	없음	있음 (키 분배시간 소요)	없음
	동일 시스템 간 부하분산	용이	어려움 (키 분배 필요)	어려움 (IPSec 세션 테이블과 IPSec 설정 테이블 공유 필요)

* 공격자가 내부 네트워크에서 공격할 경우, 같은 IPSec 터널을 이용하여 다른 호스트까지 공격으로 판단할 수 있으므로 단계적 대응 기법으로 대응할 수 있음

다면 보안 시스템이 보호하는 전체 네트워크의 성능이 저하될 뿐만 아니라 대량의 비정상 트래픽 공격에 대응하기 어렵다. IPSec 트래픽을 처리하기 위해서 키를 전달받는 보안 시스템[3]에서는 IPSec 패킷마다 복호화해서 탐지한 후 다시 암호화를 해야 하기 때문에 실시간 처리가 어렵지만 제안 보안 시스템은 IPSec 패킷에 대한 복호화 및 암호화 과정이 없기 때문에 실시간 처리가 가능하다. 세션 재설정 지연시간이란 IPSec 세션의 재설정 시에 지연되는 시간을 의미한다. IPSec 세션은 주기적으로 재설정을 수행하는데 이러한 재설정 시에 보안 시스템에서 지연되는 시간이 생기면 전체 네트워크의 성능이 저하된다. 표에서 보이는 바와 같이 IPSec 키 분배 기반 보안 시스템만 지연 시간이 생기는데 이는 재설정 과정에서 생성되는 키를 보안 시스템에 재분배해야 하기 때문이다.

동일 시스템 간 부하분산이란 동일한 시스템을 두 대 이상 운용함으로써 각 시스템의 부하를 분산하여 시스템의 성능을 향상시키는 방법이다. 표에서 보이는 바와 같이 IP 헤더 기반 보안 시스템은 상태 정보를 유지하지 않기 때문에 부하분산이 용이하지만 키 분배 기반 보안 시스템은 IPSec 통신상의 키를 각각의 시스템에 분배해야 하는 어려움이 있다. 제안 시스템도 IPSec 세션 테이블과 설정 테이블을 각각의 시스템에서 유지하며 서로 동기화시켜야 하기 때문에 부하분산에 어려움이 있다.

보안성 항목은 IPv6 네트워크 환경에서 일어날 수 있는 대량의 비정상 트래픽 공격을 분류하고 각 공격별로 보안 시스템이 공격에 대응 가능한가를 기술한다. IPSec 설정단계 패킷을 위조하여 대량의 트래픽을 발생시켜 전송하는 공격이 가능하며 IPSec 설정단계 패킷 자체가 암호화되지 않기 때문에 제안 보안 시스템 및 기존 보안 시스템에서 모두 대응이 가능하다. IPSec 통신이 전송모드일 경우, 대량의 비정상 IPSec 트래픽을 발생시키는 공격이 가능하다. 기본 헤더 기반의 IPv6 보안 시스템은 이러한 공격 패킷이 암호화되어 있기 때문에 기본적으로 대응이 불가능하다. 암호화되지 않는 기본 헤더 정보만을 가지고 탐지를 수행할 수 있지만 이러한 공격 탐지는 IP 주소만을 이용하기 때문에 정확도가 떨어지

고 오탐지 가능성이 존재한다. IPSec 키를 전달받는 보안 시스템은 트래픽을 복호화 하여 공격을 탐지하고 대응한다. 본 논문에서 제안하는 보안 시스템은 IPSec 세션 테이블을 유지하기 때문에 임의의 IPSec 트래픽이 IPSec 세션 테이블의 정당한 세션인지 확인하여 탐지하고 대응한다.

IPSec 통신이 터널모드일 경우에 공격자의 위치에 따라 두 가지 공격 형태로 나눌 수 있다. 공격자가 외부 네트워크에 위치한다면 전송모드와 공격의 형태가 동일하기 때문에 각 시스템의 대응 여부도 동일하다. 공격자의 위치가 내부 네트워크일 경우, 제안 보안 시스템은 IPSec 세션 테이블 만을 이용하기 때문에 이러한 공격에 대응하기 어렵다. 이 경우에는 침입을 탐지하여 관리자에게 경고한 후 트래픽의 대역폭을 낮추는 부분적인 대응만 수행한다. 기본 헤더 기반 IPv6 보안 시스템은 IPSec 트래픽을 처리할 수 없기 때문에 터널모드 상의 공격에 모두 대응하기 어렵고, IPSec 키를 전달받는 IPv6 보안 시스템은 패킷을 복호화 하여 탐지하므로 터널모드 상의 공격에 모두 대응이 가능하다.

이와 같이 본 논문에서 제안하는 보안 시스템은 실시간 처리가 가능하고 세션 재설정 지연시간이 없으며, 대량의 IPv6 비정상 트래픽 전송 공격뿐만 아니라 다양하게 적용되는 IPSec 기술을 악용한 대량의 비정상 트래픽 전송 공격까지 대응이 가능하다. 또한 IPSec 트래픽을 따로 처리함으로서 일반적인 IPv6 비정상 트래픽 공격에 의한 정상적인 IPSec 트래픽의 오탐지를 낮추는 장점이 있다.

Ⅵ. 결 론

IPv6 프로토콜의 기본 보안 기술인 IPSec 기술을 악용하여 대량의 비정상 트래픽(세션설정 단계 또는 통신 단계의 비정상 IPSec 트래픽)을 전송하였을 경우, IPSec 기술 자체에서 해당 패킷을 차단하는데 한계가 있다. 본 논문에서는 IPv6 네트워크 환경에서 IPSec 메커니즘의 ESP 확장헤더에 의해 암호화된 패킷의 비정상 여부를 사전에 확인함으로써, 성능향상을 가질 수 있는 효과적인 보안 시스템에 대한 설계 내용을 보였다. 이 보안 시스템은 단계적 대응 시스템[1][2]를 기반으로 하며, 추가적으로 IPSec 설정 테이블과 IPSec 세션 테이블을 이용하여 동작한다. 향후에는 본 논문에서 제안한 보안 시스템을 리눅스 시스템에 구현하고 성능을 평가하여, IP 헤더 기반 보안 시스템 및 키 분배 기반 보안 시스템 간 실질적인 비교를 하고자 한다.

참 고 문 헌

[1] K. Ko, E. Cho, T. Lee, Y. Kang, and Y. I. Eom, "The Abnormal Traffic Control Framework based on QoS Mechanisms," Lecture Notes in Computer Science, #3280, Oct. 2004.

[2] 조은경, 고광선, 이태근, 강용혁, 엄영익, "리눅스 Netfilter 프레임웍과 CBQ 라우팅 기능을 이용한 비정상 트래픽 제어 시스템 설계," 정보보호학회논문지, 한국정보보호학회, Vol. 13, No. 6, Dec. 2003, pp. 129-140

[3] S. Deering and B. Hinden , RFC2460: Internet Protocol, Version 6 (IPv6) Specification, Dec. 1998.

[4] S. Kent, and R. Atkinson, RFC2401: Security Architecture for Internet Protocol, Nov. 1998.

[5] S. Kent, and R. Atkinson, RFC2406: IP Encapsulating Security Payload (ESP), Nov. 1998.

[6] A. Triulzi, "Intrusion Detection and IPv6," Proc. of the Conference Security and Protection of Information 2003, Apr. 2003, pp. 15

[7] W. Stallings, Network Security Essentials, Prentice Hall, 2nd Ed., 2003.

[8] D. Maughan, M.Schertler, M. Schneider, and J. Turner, RFC2408: Internet Security Association and Key Management Protocol (ISAKMP), Nov. 1998.

[9] N. Doraswamy and D. Harkins, IPSec The New Security Standard for the Internet, Intranets, and Virtual Private Networks, Prentice Hall, 1999.

[10] P. Loshin, IPv6 : Theory, Protocol, and Practice, Morgan Kaufmann, 2nd Ed., 2004.

[11] A. Rubini and J. Corbet, Linux Device Driver, O'Reilly, 2nd Ed.,

2002.
[12] K. Wehrle, et al, The Linux Network Architecture, Prentice Hall, 2005.
[13] S. Floyd and V. Jacobson, "Link-sharing and Resource Management Models for Packet Networks," IEEE/ACM Transactions on Networking, Vol. 3, No. 4, 1995.

〈著者紹介〉

김 가 을 (Kaeul Kim) 학생회원
2005년 2월: 성균관대학교 컴퓨터공학과 졸업
2005년 3월~현재: 성균관대학교 컴퓨터공학과 석사과정
〈관심분야〉 정보보호, IPv6, 리눅스

고 광 선 (Kwangsun Ko) 학생회원
1998년 2월: 성균관대학교 정보공학과 졸업
2004년 8월: 성균관대학교 전기전자및컴퓨터공학부 석사
2004년 9월~현재: 성균관대학교 컴퓨터공학과 박사과정
〈관심분야〉 정보보호, 리눅스, 네트워크

경 계 현 (Gyehyeon Gyeong) 학생회원
2006년 2월 호서대학교 컴퓨터공학부 컴퓨터공학전공 졸업
2006년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 석사 과정
〈관심분야〉 리눅스 커널, 시스템 보안, IPv6 네트워크 보안

강 성 구 (Seong-Goo Kang)
2005년 2월: 성균관대학교 컴퓨터공학과 졸업
2005년 3월~현재: 성균관대학교 컴퓨터공학과 석사과정
〈관심분야〉 유닉스, 리눅스, 실시간 운영체제

엄 영 익 (Young Ik Eom) 종신회원
1983년 2월: 서울대학교 계산통계학과 졸업
1985년 2월: 서울대학교 전산과학과 석사
1991년 8월: 서울대학교 전산과학과 박사
2000년 9월~2001년 8월: Dept. of Info. and Comm. Science at UCI 방문교수
1993년 3월~현재: 성균관대학교 정보통신공학부 교수
〈관심분야〉 분산 컴퓨팅, 이동 컴퓨팅, 이동 에이전트, 시스템 보안, 운영체제, 내장형 시스템