김일성종합대학학보 주체108(2019)년
정보과학 제65권 제3호

IP속임DoS공격방지를 위한 모호추론방법과 IKEv2규약설계

심윤거, 박명숙

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《통신망의 보안능력을 결정적으로 높여야 합니다.》

IP속임을 리용한 봉사거부(DoS)공격은 봉사기에 대한 공격자의 자원소모공격으로 볼수 있으며 이러한 자원소모공격들에서 공격자는 봉사제공자의 CPU 또는 기억기 혹은 망대역폭을 소모시키려고 노력한다.

IP속임DoS공격을 방지하기 위하여 선행연구[2]에서는 매 파케트들이 경로기를 통과할 때마다 IP머리부의 식별자마당에 경로기식별자와 같은 정보를 추가하였다. 그러나 이 방법은 TCP/IP규약과 경로기의 동작과정에 대한 변경을 요구하므로 실현하기 힘든 결함을 가지고있다.

이러한 부족점을 퇴치하기 위하여 선행연구[4]에서는 HTTP요청통보문이 가지고있는 HTTP User Agent와 HTTP요청메쏘드 등의 정보들을 리용하여 DoS공격을 막기 위한 모호추론방법을 제기하였다.

이 방법은 HTTP규약의 특성에 기초하고있는것으로 하여 IKE와 같은 다른 규약에 적용하기가 힘들다.

IKEv2규약[1, 3]에서는 공격자들이 합법적인 VPN송신측(VPN말단 또는 VPN관문)과 VPN수신측(VPN관문 또는 VPN말단)사이의 통신을 도청한데 기초하여 IP속임공격을 진행하는 경우 이러한 파케트들을 려과하여야 하는 문제가 제기된다. 이 경우에 모호리론을 리용한 일반적인 IP속임DoS공격방지와 함께 IKE초기교환단계에서의 신뢰성검사를 도입하면 DoS공격을 방지할수 있다.

론문에서는 VPN수신측에서 모호추론을 리용하여 IKE초기교환요청통보문들에 대한 IP속임DoS공격검출 및 처리를 진행한 다음 IKEv2규약에 추가한 시간정보에 대한 검사 혹은 미끄럼창문검사를 진행하여 최종적으로 공격파케트들을 정확히 검출하는 방법을 제안하였다.

1. IP속임DoS공격방지를 위한 모호추론의 한가지 방법

일반적으로 IP속임을 리용한 DoS공격에서는 공격자가 자기의 IP주소를 봉사기가 신뢰할수 있는 합법적인 VPN송신측의 IP주소로 위조하여 대량 요청을 보낸다. 이 경우 봉사기는 원천지IP주소를 리용하여 공격파케트를 분류하는 종래의 방법을 사용할수 없게 된다.

모호추론방법은 합법적인 IP주소를 가지고 들어오는 파케트들가운데서 DoS공격파케트를 분류하는데 리용될수 있다.

론문에서는 IP속임공격을 방지하기 위하여 다음의 세가지 인자를 공격검출을 위한 모호추론의 주요인자로 설정하였다.

① 파케트들의 도착시간간격 F_{ATI}

일반적으로 DoS공격이 진행되는 경우 공격자는 요청파케트들을 대량 생성하여 봉사기에로 전송한다. 이때 봉사기에 도착하게 되는 공격파케트개수가 순식간에 증가하게 되며 그렇게 되면 파케트들의 도착시간간격이 정상수값보다 작아지게 된다.

② IP주소의 출현빈도률 F_{IPF}

합법적인 사용자는 주기적으로 요청을 진행하므로 이때 요청파케트의 IP주소는 일정한 출현빈도률을 가진다.

그러나 공격자가 IP속임공격에 리용하는 합법적인 IP주소공간이 상대적으로 제한된것으로 하여 공격파케트의 IP주소출현빈도률은 일정하지 않다.

③ 파케트의 수명값 F_{TTL}

일반적으로 파케트가 경로기를 지날 때마다 IP머리부의 *TTL*값은 하나씩 줄어들며 목적지에 도달하기 전에 0이 되면 중간경로기에서 자동적으로 제거된다. 서로 다른 원천지에서 목적지에 도착한 파케트의 *TTL*값은 일반적으로 서로 다르므로 IP속임공격에서는 공격자로부터 전송된 파케트와 합법적인 사용자로부터 전송된 파케트를 비교하면 IP주소는 같지만 *TTL*값은 서로 다르다.

론문에서는 IP속임공격시에 요청파케트들의 공격가능성을 평가하기 위하여 세가지 인자에 기초한 맘다니모호체계를 다음과 같이 구성하였다.

R_1: if x_1 is P_{11}, x_2 is P_{12}, x_3 is P_{13} then z is Q_1
R_2: if x_1 is P_{21}, x_2 is P_{22}, x_3 is P_{23} then z is Q_2
⋮
입력 : x_1 is P_1, x_2 is P_2, x_3 is P_3

결론 : z is Q'

$R_1, R_2, \cdots$: 모호규칙

P_1 : $P_1 = \{p \mid p \in (0,\ T_{\max})\}$ 인 도착시간간격모임

P_2 : $P_2 = \{p \mid p \in (0,\ N_{\max})\}$ 인 IP출현빈도률값모임

P_3: $P_3 = \{p \mid p \in (0, \Delta_{\max})\}$ 인 TTL편차값모임

x_1, x_2, x_3(입력값): $x_1 \in P_1,\ x_2 \in P_2,\ x_3 \in P_3$ 을 만족시키는 매 파케트의 인자값

Q' : 최종적인 결론으로써 파케트의 공격가능성을 나타낸다.

P_1, P_2, P_3 모임구간을 $\{Low, Medium, High\}$로 분할하고 학습자료에 기초하여 학습을 진행하여 매 인자에 대한 모호성원함수를 얻는다.(그림 1의 ㄱ)－ㄷ))

입력 $\{x_i \mid i = 1, 2, 3\}$ 에 대한 공격가능성은 그림 1과 같이 추론할수 있다. 여기서 입력값은

$$x_1 = Low,\ x_2 = Medium,\ x_3 = High$$

이다.

주어진 입력에 대하여 다음의 추론결과를 얻는다.

$$\left.\begin{array}{l}\mu_{F_{ATI}}(x_1) = High \\ \mu_{F_{IPF}}(x_2) = \text{Medium} \\ \mu_{F_{TTL}}(x_3) = High\end{array}\right\} \Rightarrow \mu(x) = High$$

웃식과 같이 주어진 입력에 대한 추론결과는 *High* 즉 공격가능성이 높다는 결론이 얻어진다.(그림 1의 ㄹ))

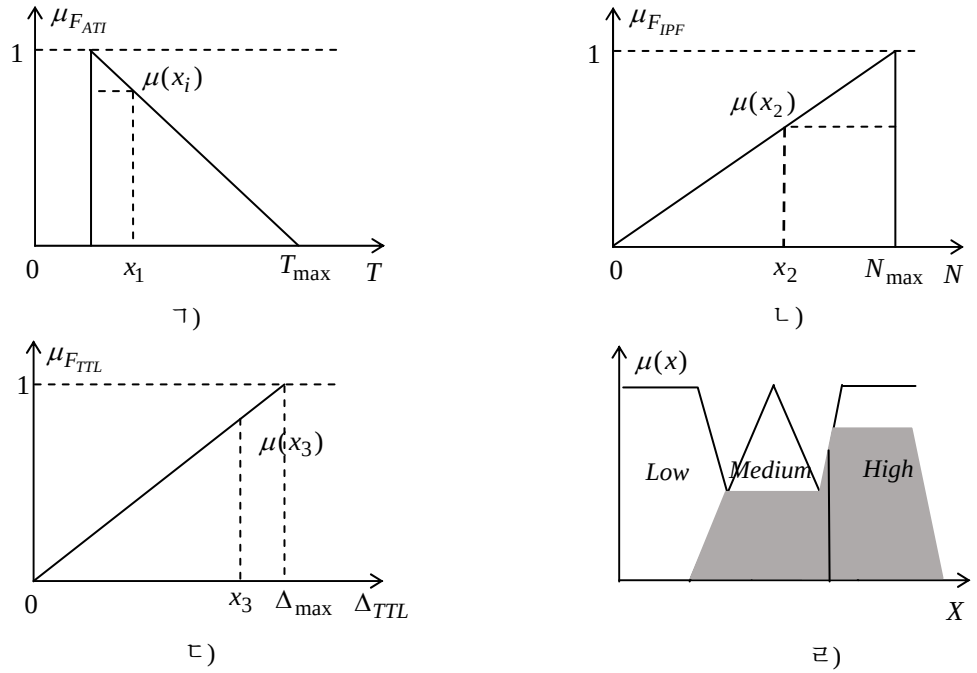

그림 1. IP속임DoS공격파케트검출을 위한 모호추론과정

ㄱ) 도착시간간격에 따르는 모호성원함수, ㄴ) IP주소의 출현빈도률에 따르는 모호성원함수,
ㄷ) *TTL*값의 차이에 따르는 모호성원함수, ㄹ) 세가지 인자로부터 추론된 최종적인 공격가능성

론문에서는 이와 같은 모호추론을 리용한 공격검출단계를 거친 파케트들가운데서 공격가능성이 높은 파케트들을 삭제하고 나머지 파케트들에 대하여 다음단계의 검사를 진행한다. 만일 체계의 보안요구가 매우 엄격한 경우에는 모호추론단계에서 공격가능성이 매우 낮은 파케트만을 골라 다음단계의 려과를 진행하면 된다.

2. IKEv2초기교환과정에서 IP속임공격검출방법

IKEv2에서 VPN수신측은 자기가 규정한 범위내의 IP주소를 원천지IP주소로 하는 파케트만을 통과시키므로 IP주소범위밖의 사용자로부터 전송된 파케트들은 보통 주소령역검사단계에서 삭제된다.

모호추론단계를 거친 파케트들에 대한 IP속임공격검출방법은 다음과 같다.

① 시간정보를 리용한 공격검출방법

VPN수신측에서는 수신한 파케트의 허가번호마당을 복호화하여 얻어진 시간(T_i)과 현

재시간과의 차이를 보고 수신한 파케트가 공격파케트인가 아닌가를 알수 있다.

시간정보를 포함한 IKEv2열쇠교환과정은 다음과 같다.(그림 2)

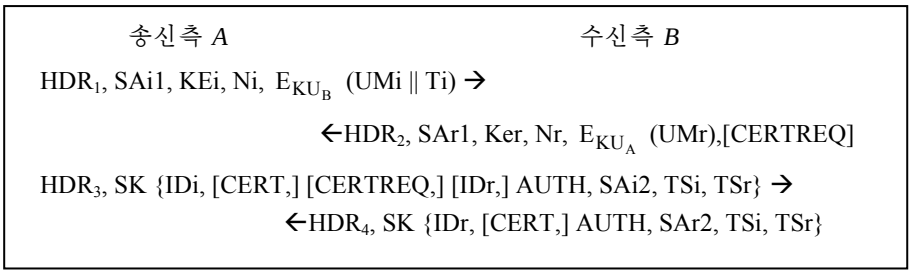

그림 2. 시간정보를 포함한 IKEv2열쇠교환과정

먼저 송신측 *A*는 IKE_SA_INIT요청통보문의 뒤에 장치정보로부터 생성된 허가번호와 요청통보문송신시간을 수신측의 공개열쇠로 암호화한 허가번호자료부 $(UMi+Ti)^{KU_B} \bmod n$을 덧붙인다.

다음 수신측은 수신한 통보문의 허가번호자료부를 자기의 비밀열쇠로 복호화하여 얻어지는 허가번호와 시간에 대한 검사를 진행하여 DoS공격을 검출한다.

② 미끄럼창문을 리용한 공격검출방법

IKE초기교환과정에서 공격파케트들은 이미 도청한 합법적인 파케트들의 복사본이므로 VPN수신측에 들어오는 파케트들에 일정한 크기 w를 가지는 미끄럼창문을 도입하여 공격이 진행될 때마다 창문을 이동시키면서 창문안의 파케트들가운데 같은 파케트가 있는가를 검사하여 공격을 검출한다.

IKE초기교환에서는 ISKMP통보문의 SPI값만 달라져도 봉사기가 응답을 진행하지 않으므로 창문안에서의 비교검사는 8B크기를 가지는 SPI값에 대해서만 진행하여도 충분하다.

론문에서 제안한 방법의 우점은 다음과 같다.

① 모호추론을 리용한 IP속임DoS공격방지

제안한 모호추론방법은 공격자가 자기의 IP주소를 합법적인 사용자의 IP주소로 위조하여 진행하는 DoS공격을 검출할수 있게 한다.

론문에서 제안된 인자들을 리용한 모호추론방법은 IP속임을 리용하는 일반적인 DoS공격방지에 일반화할수 있다.

② IKE초기열쇠교환단계에서의 DoS공격방지

공격자가 합법적인 열쇠교환과정에 송수신되는 요청파케트를 도청하여 그것을 그대로 속임공격에 리용하는 경우 열쇠교환요청파케트의 허가번호마당에 추가한 시간정보 혹은 수신측의 미끄럼창문을 리용하여 이러한 속임공격파케트를 검출할수 있게 한다.

3. 결 과 분 석

선행한 IKEv2규약[3]과 론문에서 제안한 방법을 비교하였다.(표)

표에서 보는것처럼 론문에서는 IKE_SA_INIT초기교환과정에 IP속임DoS공격을 완전히

방지하였다. 또한 종전의 COOKIE방법대신에 시간정보를 리용한 엄격한 려과를 진행함으로써 정당한 VPN의뢰기의 봉사를 원만히 제공하면서도 DoS공격을 방지하였다. 그리고 미끄럼창문을 리용하여 임의의 모든 망봉사들에 대한 DoS공격을 방지하였다.

표. 보안성능비교

규약명	IP속임DoS공격방지	완전복제공격방지	공격요청파케트검출확률/%
선행한 IKEv2	일부 지원됨	불가능	10(쿠키리용)
제안된 IKEv2	완전히 지원됨	가능	90이상(시간정보리용)

맺 는 말

모호추론을 리용하여 IP속임DoS공격을 검출하기 위한 일반적인 방법과 시간정보를 리용하여 IKEv2초기교환과정에 발생할수 있는 IP속임DoS공격을 방지할수 있는 방법을 제안하여 공격검출성능을 개선하였다.

참 고 문 헌

[1] **김일성**종합대학학보(자연과학), 63, 4, 4, 주체106(2017).

[2] G. Velmayil, Dr. S. Pannirselvam; Computer Network and Information Security, 5, 47, 2013.

[3] C. Kaufman et al.; RFC 5996, 29, 2010.

[4] Stavros N. Shiaeles, Maria Papadaki; The Computer Journal, 58, 4, 892, 2015.

주체108(2019)년 5월 5일 원고접수

A Fuzzy Reasoning Method and IKEv2 Protocol Design for Preventing IP Spoofing DoS Attack

Sim Yun Go, *Pak Myong Suk*

In this paper, we propose a method to detect DoS attack packets in IKE request messages coming into VPN server by using fuzzy reasoning method and then finally detect doubt packets by using time information which is added in IKEv2 protocol.

Key words: IP Spoofing, DoS(Denial of Service), IKEv2, fuzzy reasoning