IPv6 환경에서의 베이지안 기법을 이용한 침해탐지

Intrusion Detection Using Bayesian Techniques on the IPv6 Environment

구민정, 민병원
영동대학교

Koo Min-Jeong, Min Byoung-Won
Youngdong Univ.

요약

컴퓨터와 통신 기술의 급속한 발전은 사회 전반에 걸쳐 막대한 영향을 미치고 있으며, All-IP망이 도래될 경우 IPv6 환경에서 바이러스와 웜 공격들도 대규모로 증가할 것으로 예상되고 있다. 따라서 IPv6 환경에서 베이지안 기법을 이용한 침해 검출을 제안하였다.

Abstract

The rapidly development of computing environments and the spread of Internet make possible to obtain and use of information easily. The IPv6 environment combined the home network and All-IP Network with has arrived, the damages cased by the attacks from the worm attacks and the various virus has been increased. the In this paper, intrusion detection method using Attack Detection Algorithm Using Bayesian Techniques on the IPv6 Environment.

I. 서 론

컴퓨터와 통신기술의 급속한 발전으로 인터넷 웜의 감염과 해킹이 날로 증가하고 있다. 새롭게 변형되고 다양해지는 침해를 방지하기 위해서는 공격 트래픽에 대한 정확한 분석과 탐지가 우선되어야 한다. 그러나 IPv6 환경으로 전환될 때 발생하는 유해 트래픽에 대한 연구가 미약한 상태이다. 그러므로 IPv6 환경에서 베이지안 기법을 이용하여 공격 트래픽을 모니터링한 후 공격을 탐지하는 분석 알고리즘을 도출하여 IPv6 환경으로 전환되었을 경우 발생하는 공격을 신속하고 정확하게 검출한다. 네트워크상에 관리되는 IPv6 환경에서 사용되는 정상 트래픽의 MIB(Management Information Base)객체의 정상적인 특성을 프로파일로 작성한다.

본 논문에서는 네트워크 트래픽에 대해 열거형 순차 방법으로 정상행위를 경험적으로 추적하여 새로운 침해 트래픽을 모니터링 후 탐지한다.

침해시 사용되는 TCP Flooding, UDP Flooding, ICMP Flooding 공격이나 잠재적인 공격을 효과적으로 탐지할 수 있다.

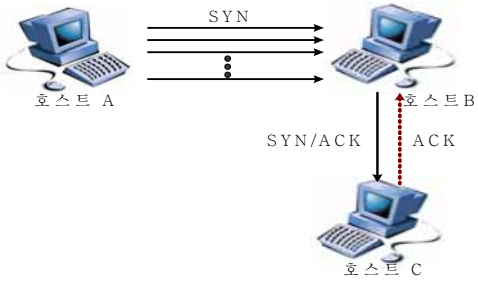
II. IPv6 환경 공격 분석

IPv6 환경의 공격을 탐지하기 위해 침해에 사용되는 행위를 분석하여 TCP Flooding, UDP Flooding, ICMP Flooding 등 공격 패킷의 패턴의 프로파일로 구축한다.

열거형 순차 방법을 이용하여 침해를 모니터링하는 방법은 열거된 순차에 의한 분석으로 Lookahead pairs, tide (time-delay embedding), stide(sequence time- delay embedding) 등이 있는데, 본 논문에서는 빈도 기반의 방법을 이용하여 빈도 분포를 모델로 사용하고 N-gram vector로 분류한다. N-gram vector는 고정된 순차의 정상 트래픽의 TCP MIB, UDP MIB, ICMP MIB MIB 별로 프로파일로 구축하고 만약, 순차가 프로파일에 존재하지 않는다면 침해로 판정하고 총 스트링의 개수에 대해 이상 행위로 간주된 스트링의 개수의 비율이 매우 크다면, 그 트래픽을 비정상으로 판정한다. N-gram vector 기법은 높은 탐지율을 보이나 프로파일의 데이터가 자칫 커질 수 있는 단점을 가지고 있다.

2.1 TCP 플러딩 공격

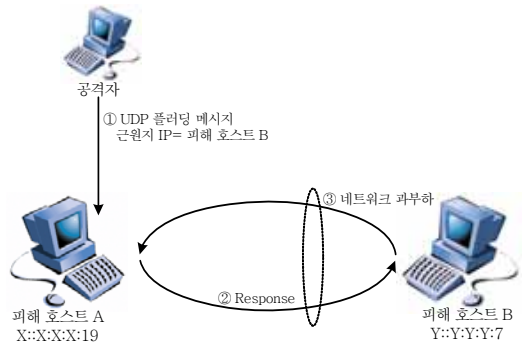
TCP 플러딩 공격은 오래전부터 이루어졌으나 사용자에게 쉽게 접근할 수 있는 SYN 플러딩 공격 소스가 광범위하게 배포되면 네트워크상의 리눅스 및 유닉스 서버에서 빈번하게 발생하고 있다. TCP 플러딩 공격은 TCP의 취약점을 이용한 공격의 형태이며 TCP 연결 설정 중 3중 핸드쉐이킹의 약점을 이용한다. 그림 2-1에 TCP SYN 플러딩 공격을 도시하였다.



▶▶ 그림 2-1. TCP 플러딩 공격

2.2 UDP 플러딩 공격

IPv6 환경에서 UDP 플러딩 공격도 TCP SYN 플러딩 공격과 같이 상위 프로토콜 IPv6에 캡슐화되어 사용됨으로 IPv4에서와 같은 방법으로 공격이 적용된다. UDP 플러딩 공격은 일반적으로 널리 사용되는 프로그램의 포트를 목표로 하는 공격과, 목적지의 포트번호를 7, 31335, 19등 특정 포트 번호로 세팅하여 서브넷의 멀티캐스트 주소 값을 목적지 주소로 보내는 공격들이 있다. 이러한 공격은 UDP 데이터그램과 스푸핑된 근원지 IP 주소 값으로 구성되어 있다. 즉, 목표 포트가 열려 있지 않는다면 커널의 하위 단계에서 패킷이 폐기 되지만 열려 있는 포트라면 커널의 상위 계층의 스택까지 패킷 데이터가 올라가게 되고 그만큼 시스템 자원을 많이 사용하여 서버가 제공하는 서비스에 지장을 초래하게 된다. 그림 2-2는 UDP 플러딩 공격을 도시하였다. 그림에서 보는 바와 같이 IPv6 헤더에 후속 헤더 부분이 UDP를 지칭하는 17로 세팅되고, 브로드캐스팅, 포트번호가 31335, 7, 19번과 같은 특정 포트로 설정하여 공격하는 형태이다.

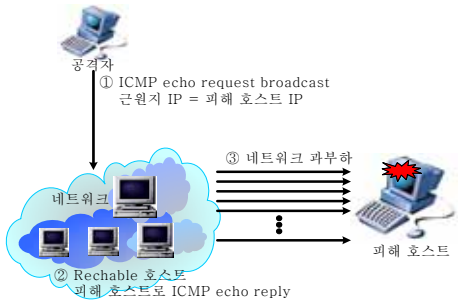


▶▶ 그림 2-2. UDP 플러딩 공격

2.3 ICMP 플러딩 공격

ICMP 메시지는 다양한 공격의 표적이 될 수 있다. ICMP 메시지 공격과 예방책은 다음과 같다.

1) ICMP 메시지는 수신자에게 메시지가 메시지를 처음 발송한 곳이 아닌 다른 곳에서 온 것이라 믿도록 하는 공격을 받을 수 있다. 이러한 공격은 IPv6 인증 방식을 ICMP 메시지에 적용함으로써 방지할 수 있다.
2) ICMP 메시지는 메시지 및 그에 대한 응답이 발신자의 의도와는 다른 곳으로 수송되도록 하는 공격을 받을 수 있다. ICMP 체크섬 계산은 악의를 가지고 중간에 가로채어 메시지를 포함하고 있는 IP 패킷에서 목적지 및 발신지 주소를 변경하는 경우에 대한 방어 방식을 제공한다. ICMP 체크섬 필드는 ICMP 메시지 인증 또는 암호화를 통해 변경을 막을 수 있다.
3) ICMP 메시지는 메시지 필드 및 Payload 변경 공격을 받을 수 있다. ICMP 메시지 인증 또는 암호화를 통해 이러한 공격을 막을 수 있다.
4) ICMP 메시지는 그림 2-3과 같이 계속해서 잘못된 IP 패킷을 수송하는 방식으로 서비스 거부 공격에 사용된다.



▶▶ 그림 2-3. ICMP 플러딩 공격

III. 베이지안 기법의 침입 탐지

3.1 베이지안 기법 프로파일

트래픽의 침해를 탐지하기 위해서는 사전 정상행위 정보를 프로파일로 구축하여야한다. 트래픽이 진정한 침해인지 정상인지 파악하는 사후 감사 과정을 수행한다.

연속적인 트래픽에 대하여 (E_1, ..., E_{i-1}, E_i)에 대해서 트래픽 상태의 침입 확률($P(1|E_1, ..., E_i)$)은 결합 확률 함수를 이용하여 다음 같다.

$$P(1|E_1, ..., E_i) = P(1|E_1, ..., E_{i-1}) \frac{P(E_i|N, E_1, ..., E_{i-1})}{P(E_i|E_1, ..., E_{i-1})} \quad (1)$$

위의 식 1로부터 다음과 같이 정의 된다.

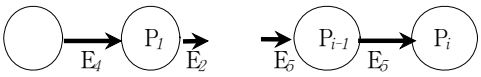
1) 연속적인 트래픽 $E=(E_1, ..., E_{i-1}, E_i)$에 대한 침해 확률값 계산은 $P(1|E_1, ..., E_{i-1}, E_i)$으로 정의한다.
2) P_{j-1} 상태에서 분기시 침입 확률값 계산은 $P_j = P(1|E_j, E_{j-1}, ...)$와 $P_{j+1}=(1|E_j, E_{j-1}, ...)$이고, P_j와 P_{j+1}의 침해 확률 값은 동일한 것으로 정의 한다.
3) P_{k-1}과 P_k의 상태에서 병합시 침해 확률값 계산은 $P_{k-1} = P(N|E_{k-1})$와 $P_k = P(N|E_k)$의 결합확률함수로써, P_{k+1}

$=P(N|P_{k-1})$와 P_k으로 정의한다.

4) 트래픽 과정의 각 상태를 연결하여 concatenation, reverse, prefix, surfix, length, repetition 상태로 표현할 수 있다.

베이지안 네트워크를 이용한 프로파일 방법은 다음과 같은 절차로 이루어진다.

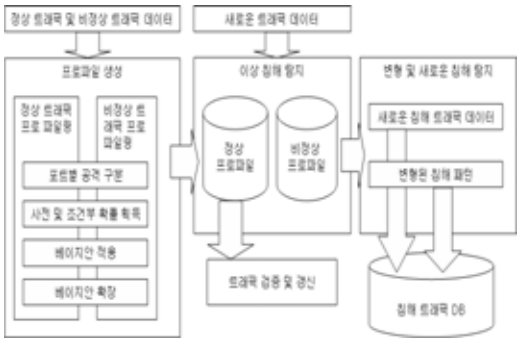
1) 정상 트래픽은 DAG(Direct Arc Graph)를 이용해서 베이지안 네트워크를 생성한다.
2) 생성된 기본 베이지안 네트워크를 MSA(Multiple Sequence Align 알고리즘에 의해 확장된 베이지안 네트워크를 생성한다.
3) 확장된 베이지안 네트워크에서 중복된 반복 부분을 제거하여 최적화된 베이지안 네트워크 프로파일을 생성한다.



▶▶ 그림 3-1. 트래픽의 베이지안 DAG

3.2 베이지안 기법의 침해 탐지

베이지안 기법은 통계적 기법의 침해 탐지로써 입력된 트래픽의 포트별로 TCP, UDP, ICMP별로 구분하고 구분된 데이터로부터 사전 확률 정보를 획득하고 베이지안 확률에 의해 트래픽에 대한 정상 행위 데이터를 클러스터링하여 유사도가 가까운 행위를 베이지안 네트워크를 이용하여 정상 행위를 프로파일한다. 새로운 트래픽에 대해 사전 확률과 사후 확률값을 계산하고 이상 침해를 탐지한다.



▶▶ 그림 3-2. 베이지안 기법의 침해 탐지도

3.3 침해 분류 기법

베이지안 확률값 계산은 사전 확률, 사후 확률, 우도 함수 등을 이용하여 식 2와 같다.

$$P(I|E) = \frac{P(E|I_i)P(I_i)}{P(E)} = P(I)\ \frac{P(I_i)P(E|I_i)}{P(E)} \qquad (2)$$

P(I)는 사전확률로 침해의 발생 빈도에 의해 좌우되고, 침해에 대한 완전한 정보를 제공하지 못하고 P(I|E)은 사전 확률로써 사전 확률P(I)와 우도 함수 P(E|I)의 곱에 이벤트의 확률 P(E)로 나눔으로써 계산된다. 여러 침해로부터 사전 확률 분포의 정보를 얻고 사전 확률 분포의 정보로부터 사후 확률 분포 정보를 도출함으로써 다양한 침해와 변형된 침해를 검출할 수 있다. 베이즈의 정리에 의해 정리해 보면 다음과 같다.

$$P(I|E) = P(\sum_i I_i|E) \qquad (3)$$

$$P(I|E) = \frac{P(E|I)P(I)}{P(E)} = \frac{P(E|I)}{P(E)} \qquad (4)$$

트래픽의 확률값은 P(I|E)가 1에 근사하면 정상트래픽으로 판정이되며 P(I|E)가 0에 근사하면 침해로 판정이 된다.

IV. 결 론

IPv6 환경에서 베이지안 기법을 이용한 침입 검출을 제안하여 네트워크상에 관리되는 IPv6 환경에서 사용되는 정상 트래픽의 MIB(Management Information Base) 객체의 정상적인 프로파일로 작성하였고, 네트워크 트래픽에 대해 열거형 순차 방법으로 정상행위를 경험적으로 추적하고 새로운 침해 트래픽을 모니터링 후 탐지하였다.

차후 프로파일 작업을 세분화 시켜 침해 분석의 다각화 시키는 연구가 필요하다.

▌참 고 문 헌▐

[1] Sreven L. Scotgt, "A Bayesian Paradigm for designing Intrusion Detection Systems To Appear in Computational Statistics and Data Analysis", June, 2002.
[2] H. Wang, D. Zhang, K. G. Shin, "Detecting SYN Flooding Attacks," Univ. of Michigan, 2002.
[3] B. Carpenter, K. Moore, "Connection of IPv6 domains via clouds," RFC 3056, 2001.
[4] J. Case, M. Fedor, M. Schoffstall, J. Davin, "A Simple Network Management Protocol (SNMP)," RFC1157, 1990.
[5] http://www.vsix.net/
[6] http://www.net-snmp.org/
[7] http://ipv6.lghitachi.co.kr/manual/korean/gs4000/HTML/MIBREF/
[8] D. Risteski, A. Kulakov, D. Davcev, "Single Exponential Smoothing Method and Neural Network in One Method for Time Series Prediction," Cybernetics and Intelligent Systems, 2004 IEEE Conference on Vol.2, pp.741-745, 2004.