韓國 컴퓨터情報學會 論文誌
第10卷 第1號, 2005. 3.

2005-3-1-1-4

침해사고 대응을 위한 능동적 역추적 기법에 관한 연구

박 명 찬*, 박 영 신**, 최 용 락***

A Study on the Active Traceback Scheme Responding to a Security Incident

Myung-Chan Park *, Young-Shin Park**, Yong-Rak Choi ***

요 약

현재의 침입차단, 침입탐지 등의 보안강화시스템은 공격자에 대하여 해당 트래픽만을 차단하는 수동적인 방어 시스템으로 실제 공격자에 대한 능동적인 대응이 부족하여 재공격 및 우회공격에 취약하다. 또한, 현재의 역추적 기술은 수작업을 통한 로그정보 수집 및 추적으로 인해 많은 시간과 인력이 필요하여 능동적 대응이 불가능하다. 본 논문에서는 현재의 인터넷 환경에 적용 가능하며, 재공격 및 우회공격에 대응하기 위하여 IP헤더에 마크를 삽입하여 추적하는 TCP 연결 역추적 기법을 제안한다. 제안된 기법은 기존 네트워크 구성요소의 수정이 불필요하고, 응답패킷에 XOR 연산 기법을 적용하여 마킹되는 정보의 양과 자원의 오버헤드를 줄일 수 있다.

Abstract

Current security reinforcement systems are passive defense system that only blocks filter to all traffic from the attacker. So, Those are weak re-attack and Stepping Stones attack because active response about attacker is lacking. Also, present techniques of traceback need much time and manpower by log information collection and trace through the personal inspection and active response is lacking. In this paper, We propose technique for TCP connection traceback that can apply in present internet and trace to inserted marking on IP header to correspond re-attack and Stepping Stones attack. Therefore, Proposed technique is unnecessary correction of existing network component and can reduce size of marked information and overhead of resources.

▸ Keyword : traceback / XOR operation / header marking / security incident

• 제1저자 : 박명찬
• 접수일 : 2005.01.07, 심사완료일 : 2005.02.26
* 대전대학교 컴퓨터공학과 대학원 ** 대전대학교 컴퓨터공학과 대학원 *** 대전대학교 컴퓨터공학과 교수

Ⅰ. 서 론

최근 많은 연구기관과 보안업체들은 인터넷상에서 발생하는 각종 침해사고로부터 시스템 및 네트워크를 보호하기 위하여 침입차단 및 침입탐지 등의 다양한 보안강화시스템을 개발하여 운용하고 있다. 하지만 현재 사용 중인 각종 보안강화시스템은 자신이 속한 도메인 내로 침입하는 공격을 어떻게 탐지할 것인가와 탐지된 공격을 어떻게 효율적으로 차단하여 자신의 도메인을 잘 보호할 것인가에 초점이 맞추어져 있다. 즉, 사전에 정의한 일정 규칙에 따라 네트워크로 들어오는 트래픽이 불법적인 침입인지 아닌지를 판단하고 불법적인 침입인 경우에만 해당 트래픽만을 차단하는 수동적인 방어 시스템이다. 이러한 시스템은 실제 공격자에 대한 능동적인 대응을 하지 못하므로 공격자가 차단된 도메인을 제외한 인터넷을 자유롭게 이용할 수 있을 뿐만 아니라 다른 공격 기술이나 공격 루트를 이용하여 재차 공격을 재개할 수 있는 문제가 있다.

또한, 최근 해킹공격의 형태는 공격자의 위치를 숨기기 위해 보안이 취약한 시스템들을 해킹한 후 대상 시스템을 침입하는 우회공격을 이용한다. 우회공격으로 피해를 받은 기관은 공격자뿐만 아니라 경유 시스템으로 이용된 기관에게도 책임을 묻고 피해보상을 요구하는 경향이 있다. 특히 최종 피해 기관이 중요 정보통신기반이면 경유지로 이용된 기관은 책임을 면하기 어려워진다. 따라서 불법적인 침해사고를 일으키는 공격자를 실시간으로 역추적하여 근원지를 탐지하고, 공격경로로 이용된 취약한 시스템들을 파악하여 신속하게 복구 및 보안하는 능동적인 대응이 수행되어야 한다.

본 논문에서는 현재의 인터넷 환경에 적용 가능하며, 우회공격에 대하여 능동적으로 대응하기 위한 네트워크 기반의 TCP 연결 역추적 기술을 적용한 능동적 역추적 기법을 제안한다. 본 논문의 구성은 2장에서 기존 역추적 기술의 종류 및 특징을 기술하고, 각 역추적 기술의 문제점을 분석한다. 3장에서는 네트워크 기반의 TCP 연결 역추적 기술을 적용한 능동적 역추적 기법을 제안하고, 4장에서는 기존 제안된 SWT(Sleepy Watermark Tracing)기법과 비교하여 성능을 평가한다.

Ⅱ. 관련 연구

2.1 역추적 기술

네트워크상의 실제 위치를 탐색하는 기술을 역추적이라 하며, 침입자의 확인과 증거 확보를 위한 분석 작업을 자동으로 수행하여 공격자의 위치를 탐지하기 위한 시스템을 역추적 시스템이라 한다[1][2]. 역추적 기술은 IP 주소가 변경된 패킷의 실제 송신지 위치를 추적하는 IP 패킷 역추적 기술과 공격자가 자신의 위치를 숨기기 위해 우회 공격을 시도하는 경우 공격자를 추적하는 TCP 연결 역추적 기술로 분류된다.

2.2 IP 패킷 역추적 기술

IP 주소가 변경된 패킷은 악의적으로 사용되는 경우가 대부분이며 주로 DoS 공격이나 DDoS 공격에서 사용된다[3][4][5][6]. 이렇게 IP 주소가 변경되는 경우는 TCP 연결을 유지할 수 없는 취약점이 있어 일방적인 패킷 송신으로 공격이 가능하다. 이러한 공격에 대응하기 위하여 네트워크로 전송되는 패킷에 라우터 정보를 표시하는 패킷 마킹 기법을 이용한다[6]. 패킷 마킹기법은 네트워크에서 패킷이 전송되는 동안 경유한 모든 라우터의 IP 주소를 패킷에 마킹한다. 이후, 침해사고 발생시 마킹된 패킷을 받은 피해 호스트로부터 마킹된 라우터 주소 정보를 바탕으로 패킷이 지나온 경로를 재구성하여 실제 공격자의 근원지를 찾아가는 기법이다. 현재 제안된 IP 패킷 역추적 기술에는 노드 추가 기법, 노드 샘플링 기법, 에지 샘플링 기법 등이 있다[1][6]. IP 패킷 역추적 기술의 경우 전송되는 패킷에 각각의 라우터 주소 정보를 계속 첨부해야 하기 때문에 라우터에 과부하를 초래할 수 있다. 또한, 패킷 내에 라우터 주소를 입력할 공간에 대한 문제도 발생할 수 있다.

2.3 TCP 연결 역추적 기술

공격자는 침입시도의 성공 여부와 상관없이 최대한 자신에 대한 정보를 감추기 위해 여러 다른 시스템들을 경유하는 공격을 수행한다. 이러한 우회공격에서 경유된 시스템들로부터 정보를 획득하여 이를 바탕으로 실제 공격자의 위치

를 역추적 하는 시스템을 우회공격 근원지 역추적 혹은 연결체인 역추적 기술이라 한다[7]. TCP 연결 역추적 기술은 네트워크상의 모든 호스트로부터 정보를 수집하여 추적하는 호스트 기반과 네트워크상에서 송수신되는 패킷에서 정보를 수집하여 공격자를 추적하는 기법으로 분류할 수 있으며 〈표 1〉과 같다[8].

표 1. TCP 연결 역추적 기술 분류
Table. 1 Technique classification of TCP chain Traceback

	Passive	Active
Host-based	DIDS CIS AIAA	Caller ID
Network-based	Thumbprint-based Timing-based Sequence Number-based	IDIP CITRA AN-IDR SWT

Host-based는 각 호스트로부터 수집한 정보를 기반으로 한 추적을 의미하고, Network-based는 연결 체인에서 애플리케이션 레벨의 내용은 변하지 않는 네트워크 연결 특성을 기반으로 역추적을 수행하는 기술이다. Passive(수동적)는 피해 시스템에서 수동적인 모니터와 네트워크 트래픽을 비교하여 공격자를 추적하는 기술을 의미한다. 이 기술은 모든 들어오고 나가는 연결정보의 비교가 필요하다. 그러나 현재의 개방된 인터넷 환경의 특징(연결정보의 변조 및 삭제)으로 인한 연결정보의 신뢰성에 대한 문제가 제기될 수 있다. Active(능동적)는 사용자가 요구하는 기능을 수행할 수 있는 프로그램 코드를 패킷으로 구성하여 전송하는 방식으로 Passive 방식에 비해 신뢰성을 제공한다.

2.4 호스트 기반 연결 역추적 기술

네트워크상의 각 호스트에 역추적을 위한 모듈을 설치하여 호스트에서 발생하는 로그정보 등을 자동으로 분석하여 공격자의 근원지를 찾는 기술이다[8]. 하지만 공격자를 역추적 하기 위해 네트워크상의 모든 호스트에 역추적 모듈을 설치해야 하며, 만약 역추적 경로 상의 하나의 시스템이라도 어떤 문제에 의해서 로그정보를 얻을 수 없다면 역추적 자체가 불가능하게 되는 단점을 갖고 있다. 또한, 개방된 인터넷 환경에서의 로그정보에 대한 신뢰성 문제가 제기될 수 있다. 이로 인해 현재의 네트워크 환경에서 적용하는 것은 거의 불가능하다.

2.5 네트워크 기반 연결 역추적 기술

네트워크상에서 송수신되는 패킷의 위치를 확인할 수 있도록 역추적 모듈을 설치하고 패킷에서 추적 정보를 추출하여 공격자의 근원지를 파악하는 방법이다[8]. 현재 제안되고 있는 방법은 대부분 송수신 되는 패킷을 확인할 수 있는 위치에서 공격 연결을 조사하는 방법과 동일한 연결 체인에 속하는 연결을 추출하여 역추적을 수행하는 방법을 취하고 있다[9]-[12]. 그러나 이 방법은 네트워크상의 패킷들로부터 얻는 각종 연결 정보들을 역추적 시스템들과 공유하는데 생성되는 정보의 순서관계 및 동기화가 매우 어렵고, 네트워크상에서 발생하는 모든 연결에 대한 정보를 지속적으로 보유하고 있어야 하는 문제로 인해 현재의 인터넷에 적용하여 사용할 수 있는 전체 시스템은 아직 제안되지 못했다.

2.6. SWT(Sleepy Watermark Tracing)

SWT는 현재 가장 활발히 연구가 진행되고 있는 TCP 연결 역추적 기술로써 침입에 대한 응답패킷에 워터마크를 삽입하여 역추적을 수행하는 방법이다[13][14].

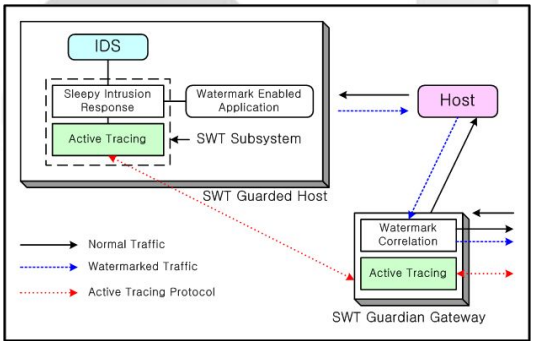

그림 1. Sleepy Watermark Tracing
Fig. 1 Sleepy Watermark Tracing

(그림 1)은 SWT의 구성도를 나타낸다. SWT 역추적 기법은 guardian gateway와 guarded host가 존재하며 서로 연동한다. 최초 침입이 발생하기 전까지 추가적인 동작을 하지 않는 일반적인 상태(Sleepy)로 존재하다가 guarded host 내의 IDS에서 침입을 탐지하면, 침입으로 판명된 패킷에 대하여 워터마크를 삽입하여 응답패킷을 전송하고, 이와 동시에 guardian gateway의 active tracing 모듈이 워터마크가 삽입된 패킷을 찾아가면서 역추적을 수행한다. SWT 역추적 기법은 공격에 대한 응답패킷을 이용하여 공

격자의 위치를 추적하기 때문에 빠르고 정확한 역추적이 가능하다. 그러나 Active 네트워크에서 사용 가능하므로 현재의 인터넷 환경에 적용하는데 어려움이 있고, 공격자가 암호화된 연결을 사용하는 경우 데이터에 워터마크를 삽입할 수 없어 역추적이 불가능하다는 단점이 있다[15]-[18].

위와 같은 네트워크 기반 연결 역추적 기술을 현재의 인터넷에 적용하여 사용할 수 있는 전체 시스템은 아직까지 제안되지 못했다. 다만 네트워크상에서 얻을 수 있는 패킷으로부터 어떤 정보를 활용해야 공격 연결과 동일한 연결에 속하는가를 판단할 수 있을지에 대한 알고리즘만이 제안되고 있는 상황이다. 이는 네트워크상의 패킷들로부터 얻게 되는 각종 연결 정보들을 네트워크상에 존재하는 역추적 시스템들과 공유하는데 생성되는 정보의 순서관계 및 동기화가 매우 어렵고, 네트워크상에서 발생하는 모든 연결에 대한 정보를 지속적으로 보유하고 있어야 하는 문제가 발생할 수 있기 때문이다.

III. 능동적 역추적 기법

3.1 능동적 역추적 기술의 고려사항

본 논문에서 제안하는 능동적 역추적 기술은 우회공격에 대한 대응 기술로써 제안되었다. 우회공격은 공격자 자신이 피해 시스템에 직접 공격하는 것이 아니라 여러 호스트들을 경유하여 공격함으로써 자신의 위치를 감추는 방법을 사용한다. 우회공격으로 침해사고가 발생한 피해 시스템에서 공격자의 실제 위치를 파악하기 위해서는 경유지를 역으로 추적하는 방법을 이용한다. 제안된 역추적 기법은 다음의 사항을 고려하여 제안되었다. 먼저, 공격자가 우회공격을 통해 침입하는 경우 공격 패킷에 대한 응답 패킷은 지나온 경유지의 역방향으로 전달된다. 이와 같은 연결특성을 이용하여 응답 패킷의 IP 헤더에 마크를 삽입하는 조작을 통하여 공격자를 추적한다. 즉, 우회공격의 연결특성을 이용한다. 두 번째는 호스트에 비해 상대적으로 침해사고가 적은 게이트웨이 측에 역추적 시스템을 지원하는 모듈을 설치하여 중간 경유 호스트의 도움 없이 역추적을 수행한다. 즉, 경유 호스트 및 기존 호스트의 시스템을 변경하지 않도록 하기 위해 도메인 경계의 게이트웨이에 역추적 시스템을 설치한다. 세 번째는 공격자의 공격 패킷에 대해 실시간 대응하는 응답 패킷의 IP 헤더에 마크를 삽입하는 역추적 게이트웨이를 이용하여 실시간 역추적을 수행한다.

3.2 제안된 패킷 마킹 기법

본 논문에서 제안하는 능동적 역추적 기법은 보안강화시스템과 연동하여 침입정보를 전달받아 공격자의 실제 위치를 추적하는 역추적 기법이다. (그림 2)는 제안된 패킷 마킹 기법을 적용한 능동적 역추적 기술을 나타낸다.

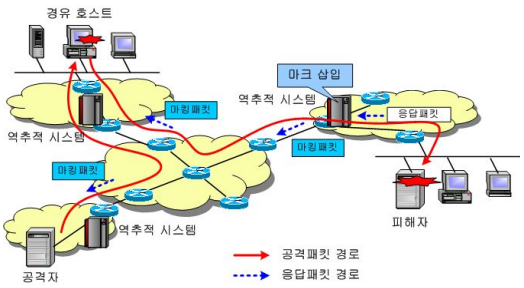

그림 2. 능동적 역추적 개념도
Fig. 2 Active Traceback conception

(그림 2)와 같이 공격자의 우회공격에 대하여 피해 시스템의 보안강화시스템에서 공격을 판단하면 해당 공격 패킷에 대한 응답패킷을 Capture한다. 이후 Capture된 응답패킷의 IP 헤더에 존재하는 Source IP와 Option 필드를 추출하여 XOR 연산을 수행하고, 그 결과 값을 Option 필드에 새롭게 삽입한다. 이 과정을 경유하는 호스트에서 수행하여 응답패킷을 최종 공격자 호스트로 전송하여 공격자를 찾아낸다. 즉, XOR 연산을 통해 모든 공격경로에 존재하는 경유 호스트의 주소를 XOR 연산하여 IP 헤더의 Option 필드에 마킹한다. 이후, 마킹한 응답패킷에서 공격경로를 재설정하기 위해 XOR 연산의 (A⊕B)⊕B = A라는 특성을 이용한다.

최종 공격자의 위치에서 마킹된 옵션필드를 추출하고, 이 값에 공격경로를 따라 XOR 연산을 하면 경유된 호스트들과 실제 패킷이 피해 호스트로부터 보내졌음을 확인할 수 있다. 따라서 공격자의 공격경로와 실제 공격자의 위치를 판단할 수 있다. XOR 연산의 특성을 이용한 패킷 마킹과 재설정을 도식화하면 (그림 3)과 같다.

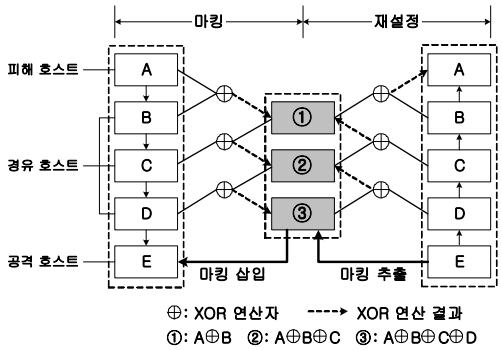

그림 3. XOR 연산을 이용한 마킹과 재설정
Fig. 3 XOR Marking and disjunction

제안된 패킷 마킹 기법은 IP 헤더의 TL(Total Length) 값을 검사하여 1492(1500Byte에서 옵션필드에 마킹을 추가할 8Byte를 감산)이하인 경우에만 마킹 작업을 수행한다. 즉, 네트워크상에서 전송될 수 있는 패킷의 최대 전송 단위 MTU(Maximum Transmission Unit: 1500Byte)값을 고려하여 4Byte의 마킹 정보 필드와 2Byte의 Sequence Number 필드, 그리고 Padding으로 구성한 8Byte를 할당한다. Sequence Number 필드는 동일한 Source IP와 Destination IP가 존재하므로 이를 구별하기 위해 사용된다. (그림 4)는 IP 헤더의 마킹 위치 및 구조를 나타낸다.

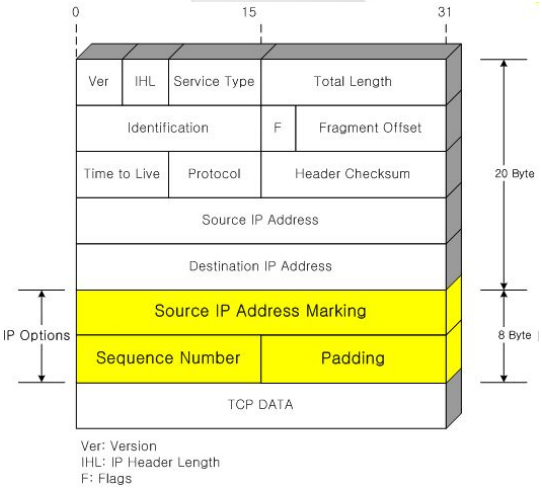

그림 4. IP 헤더의 마킹 위치
Fig. 4 Marking position of IP Header

Ⅳ. 비교평가

본 제안 기법은 평가를 위해서 기존 TCP 연결 역추적 기술 중 현재 가장 활발히 연구가 진행되고 있으며, 제안 기법에서 제시하는 패킷 마킹 기법과 유사한 워터마킹 기법을 적용한 SWT 역추적 기법을 대상으로 하였다. 두 기법은 TCP 연결 역추적 기술 중 네트워크 기반의 능동적 역추적 기술로 분류할 수 있으며, IDS와 연동하여 침입탐지정보를 전달받아 동작하는 방식을 사용한다. 〈표 2〉는 SWT와 제안기법에서 사용하는 마킹 기법의 차이점을 마킹에 사용될 정보 및 패킷 내의 마킹 위치 그리고 마킹 방법으로 분류하여 평가한다. 을 적용환경, 역추적 기법, 마킹 정보, 마킹 위치, 마킹 방법, 암호화된 연결 역추적 등으로 평가하였다.

두 기법의 가장 큰 차이점은 적용 환경에 있어 SWT는 기존 네트워크 환경이 아닌 Active 네트워크라는 특정한 환경을 기반으로 기존 환경에서는 적용 불가능하다. 제안기법의 경우는 기존 네트워크 환경에 적용 가능하여 추후 역추적 시스템 개발에 적용할 수 있다. 두 기법의 경우 IDS 또는 보안강화시스템과 연동이 가능하며, 이들 시스템의 침입탐지 정보를 이용하여 응답 패킷에 마킹을 삽입하는 기법을 이용하는 방식에서는 비슷하나, 실제적으로 마킹을 위한 정보 및 마킹위치, 방법에 있어 큰 차이점이 있다.

표 2. SWT와 제안방식의 성능평가
Table. 2 Performance valuation of SWT and Proposal method

평가항목	SWT	제 안 기 법
적용 환경	Active 네트워크 전용	기존 네트워크 적용
역추적 기법	IDS 연동에 의한 공격 응답 패킷에 워터마킹	보안강화시스템 연동에 의한 응답 패킷의 마킹
마킹 정보	다른 문자들과 구별되는 랜덤 값	경유하는 모든 호스트들의 주소를 XOR 연산한 값
마킹 위치	패킷의 데이터 영역을 사용	IP 헤더의 옵션필드 사용
마킹 방법	데이터 다음에 가상의 null 스트링 문자를 사용하여 마킹	Source IP와 옵션필드를 XOR하여 결과 값을 마킹
암호화된 연결역추적	데이터 영역에 워터마크를 삽입하므로 암호화 된 연결인 경우 역추적이 불가능	SSL(Secure Sockets Layer)이나 SSH(Secure SHell)를 이용하는 연결에서도 역추적 가능

SWT의 경우는 워터마킹을 위해 다른 문자들과 구별되는 워터마크를 랜덤 값을 이용하여 생성한다. 그러나 이 경우 랜덤한 값이 중복되지 않도록 계속 생성해야 하는 문제가 발생한다. 반면, 제안 기법에서는 경유하는 모든 호스트들의 주소를 XOR 연산을 통하여 마킹함으로 중복에 대한 문제를 고려하지 않아도 된다. 생성된 정보에 대한 마킹 위치의 경우 SWT는 패킷의 데이터 영역을 사용하는데 이 영역을 사용하기 위해서는 데이터의 크기를 알고 있어야 하는 문제가 발생한다. 제안 기법의 경우는 IP 헤더의 옵션필드를 사용하는데 있어 패킷의 TL 값이 1492Byte 이하인 경우에만 사용할 수 있는 특징이 있다.

마킹 방법에 있어서도 SWT는 데이터 다음에 가상의 null 스트링 문자를 사용하여 마킹하는데 이때도 데이터의 크기와 마킹 가능한 크기를 알 수 있어야 하는 문제가 있다. 제안 기법은 Source IP와 옵션필드를 XOR하여 그 결과 값을 마킹함으로 8Byte의 고정된 값만 사용함으로써 경유지가 아무리 많아도 추적에는 항상 고정된 크기만을 사용한다. 또한, SWT는 워터마크를 삽입하기 위해 데이터 영역을 사용하므로 공격자가 암호화된 연결을 사용하게 되면 역추적이 불가능하지만, 제안 기법은 응답패킷에서 IP 헤더의 옵션필드를 사용하므로 암호화된 연결에서도 적용 가능하다는 장점을 가진다.

V. 결론

본 논문에서는 우회공격에 대한 능동적 대응을 위하여 TCP 연결 역추적 기술 중 네트워크 기반의 능동적 역추적 기법을 제안하였다. 제안된 능동적 역추적 기법은 우회공격의 경우 공격 패킷에 대한 응답 패킷은 경유한 역방향으로 전달되는 우회공격의 연결특성을 이용하여 응답 패킷의 IP 헤더에 각 경유지 Source IP를 XOR 하여 마킹한다. 마킹된 패킷은 최종 공격지 앞단에서 검출되어 XOR 재설정에 의해 공격자를 추적하는 방식을 이용한다. 즉, XOR 연산의 (A⊕B)⊕B = A라는 특성을 이용한다. 제안된 기법은 기존 네트워크 구성 요소의 수정이 필요 없으며, 로그 기록 방식에 비해 전달되는 모든 패킷을 저장하지 않고 공격에 대한 응답패킷 정보만을 Capture하여 저장하므로 기록되는 정보의 양과 자원의 오버헤드를 줄일 수 있다. 또한, 공격경로로 이용된 경유 호스트를 파악할 수 있어 시스템 관리자가 취약성을 가진 시스템에 대해 신속한 대응을 취할 수 있는 장점을 가진다.

본 제안 기법은 공격 호스트가 역추적 동작을 감지하거나 임의의 사건으로 인해 피해 호스트와 연결이 종료될 경우는 공격 호스트를 탐지하기 어렵다. 즉, 본 구현은 연결형 공격에서는 효율적이지만 그렇지 않은 경우는 문제가 있으므로 향후 비연결형 공격에서도 적용 가능한 실시간 역추적 시스템에 관한 연구가 요구된다.

참고문헌

〔1〕 최양서, 서동일, 손승원, "역추적 기술 동향: TCP Connection Traceback 중심", ITFIND 주간기술동향, 1079호, pp.13-25, 2003.

〔2〕 채연주, 서진철, 임채호, 원유헌, "해킹기법을 응용한 침입자 역추적 시스템", 한국정보과학회 추계학술발표 논문집, 제27권 2호, 2000.

〔3〕 고병수, 박영신, 최용락, "컴퓨터 포렌식스를 지원하는 보안 감사/추적 모듈 설계", 한국컴퓨터정보학회 논문지, 제9권 1호, 2004.

〔4〕 김강, 전종식, "보안정책 기반 침입탐지 시스템 모델 설계", 한국컴퓨터정보학회 논문지, 제8권 4호, 2003.

〔5〕 Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, "Practical Network Support for IP Traceback", Proceedings of the 2000 ACM SIGCOMM Conference, pp.295-306, 2000.

〔6〕 Buchholz, Thomas E. Daniels, Benjamin Kuperman, Clay Shields, "Packet Tracker Final Report", CERIAS Technical Report 2000-23, Purdue University, 2000.

〔7〕 X. Wang, D. Reeves, S. F. Wu, "Tracing Based Active Intrusion Response", Journal of Information Warfare, Vol. 1, No. 1, pp.50-61, 2001.

〔8〕 K. Yoda and H. Etoh, "Finding a Connection Chain for Tracing Intruders", Computer Security - ESORICS 2000, No. 1895, pp.191-205, 2000.

〔9〕 김병룡, 김수덕, 김유성, 김기창, "마킹 알고리듬 기반

IP 역추적에서의 공격 근원지 발견 기법", 정보보호학회 논문지, 제13권 1호, 2003.
〔10〕 원승영, 한승완, 서동일, 김선영, 오창석, "패킷 마킹을 이용한 해킹경로 역추적 알고리즘", 한국콘텐츠학회 논문지, 제3권 1호, pp.21-30, 2003.
〔11〕 Dawn X. Song, Adrian Perrig, "Advanced and Authenticated Marking Schemes for IP Traceback", Proceedings IEEE INFOCOM, 2001.
〔12〕 Chun He, "Formal Specifications of Traceback Marking Protocol", Honors Thesis, 2002.
〔13〕 X. Wang, D. Reeves, S. F. Wu and J. Yuill, "Sleepy Watermark Tracing: An Active Network-Based Intrusion Response Framework", Proceedings of 16th International Conference on Information Security (IFIP/Sec '01), 2001.
〔14〕 이수형, 나중찬, 손승원, "액티브 네트워크 기반 네트워크 보안 기술동향", ITFIND 주간기술동향, 1076호, pp.1-14, 2002.
〔15〕 임채호, 원유헌, "인터넷 해킹피해 시스템자동분석에이전트(AIAA) 및 침입자 역추적 지원도구 구현", 한국정보처리학회 논문지, 제6권 11호, 1999.
〔16〕 지정훈, 남택용, 손승원, "액티브코드 기반의 실시간 역추적 시스템", 한국정보과학회 추계학술발표 논문집, 제29권 2호, 2002.
〔17〕 D. Schnackenberg, K. Djahandari, and D. Strene, Harley Holiday, Randall Smith, "Cooperative Intrusion Traceback and Response Architecture (CITRA)", Proceedings of the 2nd DARPA Information Survivability Conference and Exposition (DISCEXII), 2001.
〔18〕 Denning, D.E., "An intrusion detection model", IEEE Trans. S.E. Vol. SE-13, No.2, pp.222-232, 1987.

저 자 소 개

박 명 찬

2001년 대전대학교 컴퓨터공학과 (공학석사)
현재 대전대학교 컴퓨터공학과 (박사수료)
〈관심분야〉 역추적, 컴퓨터 포렌식스

박 영 신

2004년 대전대학교 컴퓨터공학과 (공학석사)
현재 대전대학교 컴퓨터공학과 (박사과정)
〈관심분야〉 역추적, 컴퓨터 포렌식스

최 용 락

1989년 중앙대학교 전자계산학과 (이학박사)
1982년 3월~1986년 1월 한국전자통신연구원 선임연구원
현재 대전대 컴퓨터공학부 교수
〈관심분야〉 컴퓨터통신보안, 컴퓨터 포렌식스, DRM