침입 탐지 도구에서 능동 대응 정책 생성 방안

The Scheme for Generate to Active Response Policy in Intrusion Detection System

김봉한*, 이재광**, 백승헌***, 오형근***, 박응기***
청주대학교 컴퓨터정보공학과*, 한남대학교 컴퓨터공학과**, 국가보안기술연구소***

Bong-Han Kim(bhkim@cju.ac.kr)*, Jaw-Kwang Lee(Jklee@netwk.hannam.ac.kr)**,
Seung-Hyun Paek(shpaek@etri.re.kr)***, Hyung-Geun Oh(hgoh@etri.re.kr)***,
Eung-Ki Park(ekpark@etri.re.kr)***

요약

본 논문은 침입탐지 도구에서의 능동 대응 정책 생성 방안에 대하여 연구하였다. 능동 대응형 침입탐지 시스템을 설계·구현하기 위한 선행 연구로서 능동 대응을 위한 침입탐지 도구의 요구사항을 7가지 구성요소로 고려하였고, 공격에 대한 능동 대응 방안으로 NIDS와 ADS를 통합한 모델을 기반으로 상호 유기적으로 시그니쳐를 생성할 수 있는 방안을 제시하였다. Unknown Attack의 탐지를 위하여 트래픽 비정상행위 탐지와 프로토콜 비정상행위 탐지로 나누어 연구하였고 자동적인 시그니쳐 생성 엔진을 위해 헤더영역과 페이로드영역으로 나누어 연구하였다.

■ 중심어 : | 침입탐지 | 능동대응 | 시그니쳐 생성 |

Abstract

This paper studied active respense policy generation scheme in intrusion detection system. We considered seven requirements of intrusion detection system for active response with components as the preceding study. We presented the scheme which I can generate signature with a base with integrate one model with NIDS and ADS. We studied detection of the Unknown Attack which was active, and studied scheme for generated to be able to do signature automatically through Unknown Attack detection .

■ keyword : | Intrusion Detection | Active Response | Signature Generation |

I. 서 론

침입탐지 시스템은 침입을 시도하였을 때 의심스러운 행위를 감시하여 조기에 침입을 발견하여 처리하는 시스템을 말한다. 현재의 침입탐지 시스템은 트래픽이 과중한 네트워크, 스위치드 네트워크, 비대칭 네트워크, 탐지 후 대응의 불가능, 대응까지 오랜 시간 소요, 과도한 분석 데이터의 축적, 판정 오류 등 많은 문제점을 가지고 있다.

위와 같은 문제를 해결하기 위해서 연구되고 있는 침입탐지 시스템이 능동 대응 침입탐지 시스템이다. 기존의 정보보호 방식이 시스템 설계 단계부터 반영된 것이

접수번호 : #051026-001
접수일자 : 2005년 10월 26일
심사완료일 : 2005년 11월 09일
교신저자 : 김봉한, e-mail : bhkim@cju.ac.kr

아니기 때문에 서비스 제공 이후에 발생 가능한 다양한 공격에 대해서 탐지하고, 이에 대한 효과적인 대응책을 제시하기에는 태생적 한계를 지니고 있다. 이에, 능동 대응 침입탐지 시스템에서는 네트워크 인프라 차원에서 실시간 침입에 대한 탐지 및 역추적, 복구 등의 기능을 효과적으로 수행할 수 있다[1][2][7].

현재 능동 대응 침입탐지 시스템에 대한 국내 연구는 초기 연구개발 단계로, 시범적인 침입탐지 시스템과 이와 연계한 능동대응정책에 관한 연구가 진행되었지만, 아직까지는 기존의 침입탐지 시스템에 대한 정부의 표준안 및 권고 사항만 마련되었으며, 이에 대한 기술은 국가기술지도에 간략하게 언급하고 있을 뿐이다.

따라서 본 논문에서는 침입탐지 도구에서 요구되는 능동 대응 접근을 위한 고려사항을 연구하였고, 이러한 기초 연구를 통해 능동적으로 Unknown Attack을 탐지할 수 있는 방안과 Unknown Attack 탐지를 통해 자동적으로 시그니쳐를 생성할 수 있는 방안에 대하여 연구하였다.

II. 능동 대응을 위한 요구사항

침입탐지 도구에서 능동 대응 정책 생성을 위한 7가지의 요구 사항을 고려하였다[5].

1. 시그니쳐 품질

시그니쳐 기반 탐지 시스템은 침입과 일치하는 시그니쳐를 생성해야만 한다. 필터링 트래픽에서 침입 시그니쳐의 유효성을 위해 민감도와 특이성을 요구한다.

• 민감도(Sensitivity)

민감도는 시그니쳐에 의해 생성되는 탐지(true positive)와 관련이 있다. 침입과 침입이 아닌 흐름의 혼합된 트래픽에서, 침입 흐름의 단편이 일치한다., 따라서 시그니쳐에 의해 성공적으로 식별된다.

• 특이성

특이성은 시그니쳐에 의해 생성되는 오탐지(false positive)와 관련이 있다. 혼합된 트래픽에서, 침입이 아닌 흐름의 단편은 시그니쳐에 의해 일치된다. 따라서 침입으로 틀리게 식별된다.

2. 시그니쳐 양과 길이

시그니쳐에 대응하여 흐름 페이로드를 일치하는 시스템은 흐름을 IP 프로토콜과 포트로 알려져 있는 모든 시그니쳐와 비교해야만 한다. 따라서, 소수의 시그니쳐는 매칭 속도를 증가시킨다. 또한, 매칭하고 있는 시그니쳐의 비용은 시그니쳐의 길이에 비례한다. 따라서 짧은 시그니쳐는 긴 시그니쳐보다 효율적이다. 시그니쳐 길이는 특이성에 깊은 영향을 미친다.

3. 다형성 웜에 대응하는 견고성

다형성 웜은 연속적인 침입 시도에서 그 페이로드를 변경한다. 웜은 하나의 웜 페이로드의 부분에 민감한 시그니쳐가 또 다른 웜 페이로드의 부분에는 민감하지 않을 수도 있기 때문에, 시그니쳐와 매치하기 위해 배치한다. 만일 웜이 다형성이라면, 각각의 페이로드는 다른 것과 같이 어떤 바이트 열도 포함하지 않을 것이다. 단일 바이트 열은 모든 페이로드에 의해 공유된다. 다형성은 웜과 매칭하기 위해 요구되는 시그니쳐의 수를 늘리는 원인이 된다. 따라서 모든 웜의 변이와 매칭하기 위해 요구되는 시그니쳐의 수를 최소화한다.

4. 탐지의 적시성

패치, 트래픽 필터링 등과 같은 방법을 사용하여 패킷을 검사를 하지 않는다면, 감염된 호스트가 포화상태가 될 때까지, 기하급수적으로 포트 스캐닝 웜의 공격은 취약한 호스트를 공격시킨다. 그러므로 감염시키게 되는 호스트를 패칭하는 것이 상당히 중요하다. 그것은 실제 공격 시나리오에서 공격이 일어나기 전에 패칭이 이루어져야 한다. 공격 시작될 때 공격 트래픽의 시그니쳐 기반 필터링은 웜의 전파를 가장 효과적으로 방지한다.

5. 자동화

시그니쳐 기반 침입탐지 시스템은 최소한의 실시간

관리자 개입을 요구해야 한다. 예를 들어 관리자의 눈으로 특이성을 위해 시그니쳐를 면밀하게 조사하는 것은 신규 공격에 대한 탐지에 유용하나 관리자의 부재시에는 대응 방법이 없다. 이것은 시그니쳐 탐지의 적시성과 함께 고려해야 한다.

6. 어플리케이션 독립성

TCP 계층(예를 들어, HTTP, NF RPC 등)보다 위의 응용 프로토콜에 관한 지식은 웜과 무해한 트래픽을 구별할 때에 그리고 민감하고 특정한 시그니쳐를 생산할 때에 유용하다. 그러나 그런 응용 프로토콜 지식을 반드시 학습할 필요는 없다. 현재는 TCP 보다 상위 층의 모든 프로토콜로 시그니쳐 탐지 시스템의 적용 가능성을 넓이고 있기 때문이다.

7. 대역폭 효율성

시그니쳐 탐지 시스템이 분산된 형태로 배치된다면, 이 같은 트래픽 모니터는 검사에 대해 다른 탐지 시스템과 상호 협력을 하고 심지어 공격이 상당한 네트워크 활동을 생성하더라도, 통신은 확장성을 가져야 할 것이다. 즉 공격 활동이 증가함에 따라 모니터-대-모니터 상호 협력통신도 증가해야 한다.

III. Unknown Attacks 탐지

Unknown Attacks는 시그니쳐 기반의 침입탐지시스템에서 탐지하지 못하는 공격에 대해서 비정상행위 탐지 기법으로 탐지 가능하다. 현재 Unknown Attacks를 탐지하기 위해서 많은 연구가 진행되고 있지만, 실시간 탐지에 적용하기에는 많은 무리가 있다. 실시간 탐지를 위해 가장 많이 사용되는 탐지기법으로는 트래픽의 폭주여부를 판단하는 트래픽 비정상행위 탐지 기법과 프로토콜의 적법성 및 비정상적 사용 여부를 판단하는 프로토콜 비정상행위 기법이 많이 사용되고 있다. 따라서 본 논문에서도 Unknown Attacks 탐지를 위해서 트래픽 비정상행위 탐지와 프로토콜 비정상행위 탐지 기법을 이용하였다[2].

1. 트래픽 비정상행위 탐지

트래픽 폭주(Network Consumption) 공격을 탐지하기 위해서는 다음과 같은 엔진이 필요하다.

트래픽 측정 엔진(Traffic Measuring Engine)

트래픽 비정상행위 탐지 분석 기능(Traffic Anomaly Detection Engine)

Worm/DDoS 공격의 특징을 기초로 트래픽 측정 엔진을 통해 얻어지는 가공된 흐름 정보를 이용하여 Worm/DDoS 공격에 대한 탐지가 가능하다. 트래픽 측정을 위해서 Libpcap 라이브러리를 이용해 S/W모듈로 제공할 수 있지만 Gigabit 이더넷 환경에서는 현재 평균 패킷 사이즈가 256bytes이다. 따라서 452,898 패킷에 대한 수집이 가능해야 하지만 알려진 바로는 Libpcap은 초당 10,000~16,000 패킷만을 수집 가능하다.

따라서 Libpcap을 이용한 트래픽 측정 엔진은 패킷 수집 기능에 한계가 있다. 현재 Hardwired된 트래픽 측정 도구로는 Cisco의 Netflow가 가장 많이 이용되어지고 있다. Netflow의 기능은 정보를 자체에서 분석하거나 다른 분석시스템으로 UDP를 통하여 내보내 주며 5-Tuple 정보(근원지 IP 주소, 목적지 IP 주소, 근원지 포트번호, 목적지 포트번호, 프로토콜 유형 등)를 기준으로 트래픽 추이 분석을 함으로써 최근에 발생하는 웜 바이러스 및 분산서비스거부 공격을 탐지할 수 있다는 것이다.

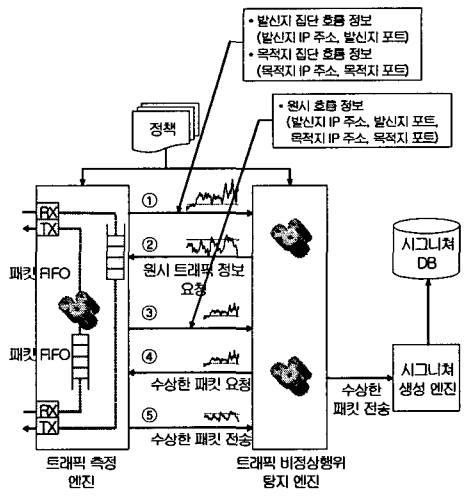

그림 1. 트래픽 측정 엔진과 트래픽 비정상행위탐지 엔진의 상호 작용

Netflow 정보를 이용하여 네트워크 트래픽에 대한 집합 흐름 단위의 트래픽 측정 정보를 나타내는 집단 흐름(Aggregation Flow)과 세부흐름 단위의 트래픽 측정 정보를 나타내는 원시 흐름(Primitive Flow)을 얻을 수 있다. 따라서 비정상적으로 집단 흐름이나 원시 흐름이 증가하게 되면 Worm/DDoS 공격으로 판단이 가능하다. Netflow는 비정상행위 탐지를 위한 매우 유용한 트래픽 측정 도구이지만, 대응에 필요한 Raw 패킷 제공 및 트래픽 비정상행위 탐지를 위한 비정상행위 탐지 엔진(트래픽 비정상행위 탐지 엔진)과의 인터페이스 제공이 불가능하기 때문에 트래픽 폭주 공격 대응 및 새로운 시그니쳐 생성을 위한 트래픽 측정 도구로 이용에 한계가 있다. 따라서 비정상행위 탐지 엔진과 인터페이스가 가능한 Hardwired된 트래픽 측정 도구가 필요하다. [그림 1]은 Worm/DDoS공격을 탐지 및 대응에 필요한 정보를 제공하기 위해 트래픽 측정 엔진과 트래픽 비정상행위탐지 엔진의 상호 작용을 보이고 있다.

트래픽 측정 엔진과 트래픽 비정상행위탐지 엔진과의 구체적인 상호 작용은 다음과 같다.

① 트래픽 측정 엔진을 이용한 집단 흐름 정보 제공

집단 흐름은 발신지 집단 흐름과 목적지 집단 흐름 정보를 제공하며, 발신지 집단 흐름은 발신지 IP 주소와 발신지 포트를 키로 하여 트래픽 수집 정보를 트래픽 비정상행위 탐지 엔진에 제공한다. 목적지 집단 흐름은 목적지 IP 주소와 목적지 포트를 키로 하여 트래픽 수집 정보를 트래픽 비정상행위 탐지 엔진에 제공한다.

② 트래픽 비정상행위 탐지 엔진에서의 비정상행위 탐지 측정 및 원시 트래픽 정보 요구

트래픽 비정상행위 탐지 엔진에서는 집단 흐름 정보를 이용하여 비정상행위 트래픽 여부를 판단한다. 판단기준은 다수의 발신지 IP 주소와 발신지 포트 쌍과 다수의 목적지 IP 주소와 목적지 포트 쌍에 대한 BPS(Bits Per Second)와 PPS(Packets Per Second)의 임계치 초과여부로 판단하며, 임계치를 정책을 통해서 전달 받게 된다. 만약 임계치를 초과하는 흐름이 존재하면 해당 흐름에 대한 보다 구체적인 정보를 얻기 위해 원시 트래픽 정보를 트래픽 측정 엔진에 요구하게 된다.

③ 트래픽 측정 엔진을 이용한 원시 트래픽 정보 제공

트래픽 비정상행위 탐지 엔진에서 요구받은 원시 트래픽 정보는 해당 발신지 IP 주소와 발신지 포트 쌍에 대한 목적지 주소, 목적지 포트의 트래픽 정보나 목적지 주소와 목적지 포트 쌍에 대한 발신지 IP 주소와 발신지 포트의 트래픽 정보를 제공한다.

④ 트래픽 비정상행위 탐지 엔진에서 비정상행위탐지 및 의심 패킷 전송 요구

트래픽 비정상행위 탐지 엔진에서는 해당 집단 흐름의 구체적인 원시 트래픽 정보를 전달받아 비정상행위 트래픽 여부를 판단한다. 판단근거는 해당 발신지 IP 주소와 발신지 포트 쌍에 다수의 목적지 IP 주소와 목적지 포트 트래픽 정보 중 BPS와 PPS의 임계치 초과여부 트래픽이 있는지 여부를 판단하다. 해당 목적지 IP 주소와 목적지 포트 쌍에 다수의 발신지 IP 주소와 발신지 포트 트래픽 정보 중 BPS와 PPS의 임계치 초과여부 트래픽이 있는지 여부를 판단하다. 만약 임계치 초과 트래픽이 존재하면 해당 흐름에 대한 Raw 패킷 정보를 트래픽 측정 엔진에 요구한다.

⑤ 트래픽 측정 엔진에서 의심스러운 패킷 전송

해당 흐름에 대한 패킷 전송을 요구 받은 트래픽 측정 엔진은 패킷 버퍼에 있는 해당 패킷을 트래픽 비정상행위 탐지 엔진에 전달한다.

2. 프로토콜 비정상행위 탐지

프로토콜 비정상행위 탐지는 인터넷과 표준 사용 방식과 관련해 예외적인 프로토콜 포맷과 프로토콜 동작 현상을 의미한다. 또한 3~4 계층의 네트워크와 전송 계층 프로토콜 비정상행위 현상과 6~7 계층의 애플리케이션 계층 프로토콜 비정상행위 현상도 포함한다. 이 경우 기본 TCP/IP 스택 동작을 여러 측면에서 모니터링해야 한다. 이는 전체 IP 패킷 조립과 TCP 재조합의 수행, 그리고 프로세스의 모든 비정상인 조건을 확인하는 것으로 실현할 수 있다. 그리고 인라인 IPS인 경우, 엔

드 호스트에서 해석이 제대로 되지 않을 가능성을 없애주는데, 이를 트래픽 정규화(Traffic normalization)라고 한다. 3~4 계층에서 일어나는 프로토콜 비정상행위 탐지 현상은 IP Fragmentation Overlap, 수상한 IP 옵션, 비정상 TCP Segmentation Overlap, 부적합한 TCP 옵션의 사용 등을 들 수 있다.

프로토콜 비정상행위 탐지 엔진을 이용한 버퍼 오버플로우 공격 탐지 방법은 공격자가 공격 대상이 되는 시스템에 전달하는 패킷의 데이터 중 응용계층 프로토콜의 필드 값에 대한 길이 및 필드 값의 문자열 구성도를 분석하여 탐지할 수 있다.

정상적인 패킷의 필드 값의 크기는 버퍼 오버플로우 공격을 유발하기 위해서 필드 값에 Non-Operation 코드를 삽입해야 하는 비정상 패킷의 필드값 크기보다 매우 작다는 특징을 이용하여 버퍼 오버플로우 공격을 탐지할 수 있다. 따라서 [그림 2]와 같이, 필드 값의 비정상 여부를 확인하기 위해서는 필드 값의 길이를 계산하는 필드 길이 계산(Field Length Calculation) 엔진과 필드 값을 구성하는 문자열 분포도를 계산하는 문자열 분포도 분석(Character Distribution Analysis) 엔진이 필요하다.

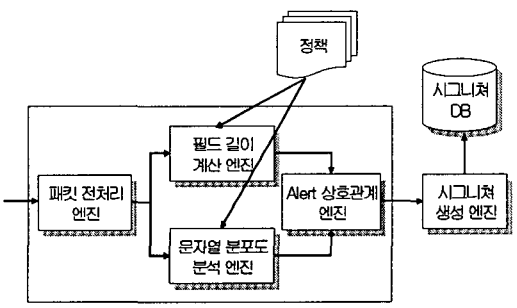

그림 2. 프로토콜 비정상행위 엔진

1) 패킷 전처리(Packet Preprocessing) 엔진

패킷 전처리 엔진의 기능은 진입 패킷이 어떤 프로토콜인지 확인하고, 분석이 필요한 필드의 필드 값을 추출하여 필드 길이 계산 엔진과 문자열 분포도 분석 엔진에 전달하는 역할을 담당한다.

2) 필드 길이 계산(Field Length Calculation) 엔진

필드 길이 계산 엔진은 전달받은 필드 값의 크기를 계산하여 해당 필드 값의 임계치를 넘으면 수상한 패킷으로 간주하여 Alert 상호관계에 전달한다.

3) 문자열 분포도 분석(Character Distribution Analysis) 엔진

문자열 분포도 분석 엔진은 전달받은 필드 값의 문자 분포도와 특정 문자의 연속성을 분석하여 임계치를 넘으면 수상한 패킷으로 간주하여 Alert 상호관계에 전달한다.

4) Alert 상호관계(Alert Correlation) 엔진

Alert 상호관계 엔진에서는 필드 길이 계산 엔진과 문자열 분포도 분석 엔진에서 전달받은 정보를 이용하여 최종적으로 해당 패킷의 적법성을 판단하고, 해당 패킷이 적법하다고 판단되면 시그니쳐 생성 엔진에 Raw 패킷을 전달한다.

Ⅳ. 시그니쳐 자동 생성 엔진

시그니쳐 자동 생성 엔진은 트래픽 비정상행위 탐지 엔진과 프로토콜 비정상행위 탐지 엔진에서 전달받은 공격 패킷을 시그니쳐 규칙으로 생성하는 기능을 담당한다. 시그니쳐 규칙은 IDS와 정의되는 필드영역, 패킷 헤더, 페이로드 영역으로 구성된다.

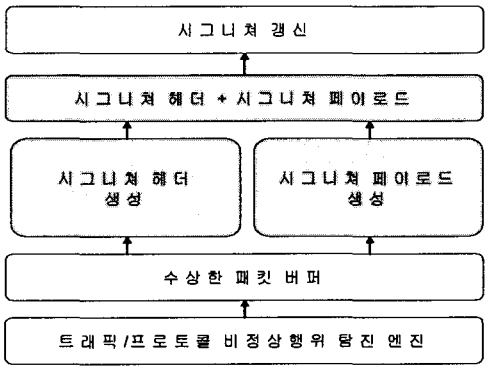

그림 3. 시그니쳐 규칙

[그림 3]과 같이 트래픽 비정상행위 탐지 엔진과 프로토콜 비정상행위 엔진에서 탐지한 Unknown Attack 패킷에 대해서 새로운 시그니쳐 규칙으로 생성하기 위해서는 헤더 영역에 대한 규칙 생성과 페이로드에 대한 규칙 생성으로 구분된다. ID, Level, Name은 시스템에 의해 정의되는 필드로 규칙을 생성할 때 시스템의 정책에 맞게 정의된다.

1. 헤더 영역에 대한 규칙 생성

헤더 영역에 대한 규칙 생성 시 전달받은 Unknown Attack 패킷의 헤더 중에서 참조할 필드는 [그림 4]와 같이 정의 할 수 있다.

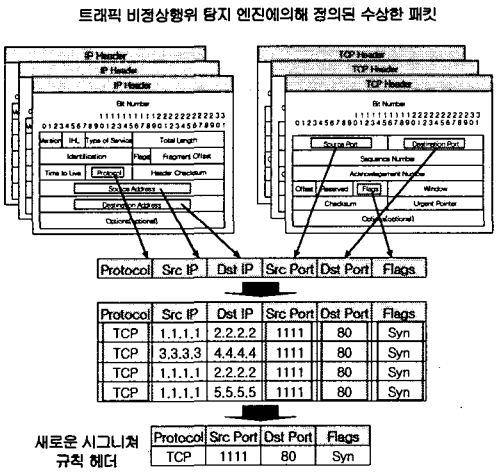

그림 4. 트래픽 비정상행위 패킷 헤더 규칙 생성

트래픽 비정상행위 탐지 엔진에서 전달받은 의심스러운 패킷은 1개의 이상의 패킷으로 구성되기 때문에 규칙의 헤더 영역 중에서 동일한 값을 가지는 필드를 조사하여 새로운 시그니쳐 규칙의 헤더 값으로 정의할 수 있다. [그림 4]는 그 과정을 보여준다.

프로토콜 비정상행위 탐지 엔진은 Packet-By-Packet으로 검사를 수행하기 때문에 시그니쳐 자동 생성 엔진에 전달되는 패킷은 단일 패킷이다. 따라서 시그니쳐 생성 엔진은 시그니쳐 규칙 생성할 때, 규칙 필드에 해당 되는 패킷의 헤더 값을 이용하면 된다. [그림 5]는 그 과정을 보여준다.

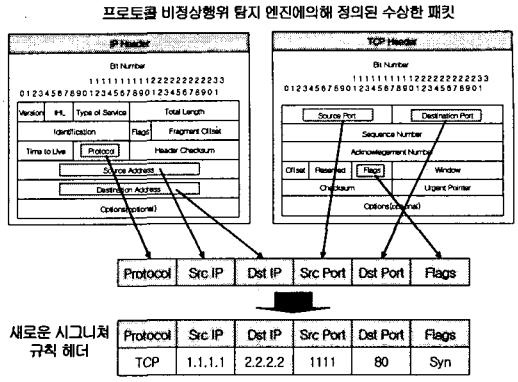

그림 5. 프로토콜 비정상행위 패킷 헤더 규칙 생성

2. 페이로드 영역에 대한 규칙 생성

트래픽 비정상행위 탐지 엔진에서 전달받은 여러 개의 패킷에 대한 페이로드 중에서 특정 문자열을 시그니쳐 규칙의 시그니쳐 필드에 저장하기 위해서는 여러 개의 패킷 중에서 일치하는 문자열을 추출해야 한다. 동일 문자열 추출을 위해서 문자열을 전 처리한 후, 결과를 자료 구조로 만들어 두는 인덱스 데이터 구조 중에서 Suffix Tree를 이용한다.

Suffix Tree는 m 길이를 가지는 스트링 S는 1~m으로 기록된 m개의 노드가 직접적으로 루트에 연결된 트리 형태를 의미한다. 하나의 노드로부터 생성된 자식 중에서 동일한 문자로 시작된 Edge label은 존재하지 않는다. Suffix Tree를 이용하여 스트링에 대한 전처리 결과를 이용하여 두 문자열 간에 동일 스트링을 추출하는 접근 방법에는 3가지로 정의할 수 있다. 이들 접근 방법을 통해서 패턴을 우회하려는 시도 즉, 단편화(Fragmentation) 및 변경(Mutation)된 패킷에 대해서도 동일 시그니쳐를 생성할 수 있도록 고안하였고, 오탐지를 최소화하기 위한 접근 방법을 고려하였다[3][6].

2.1 String equality(SE)

SE는 가장 직관적인 접근방법이다. 의심스러운 패킷들에서 연속된 동일한 문자열만을 추출하는 방법이다. 이 방법은 매우 정확한 동일 문자열을 추출할 수 있고, 오탐지를 줄일 수 있다는 점에서 매우 유용하게 사용 가능하다.

그러나 패킷을 미세하게 변경시키기만 해도, 동일 문자열을 찾을 수 없다. 웜이 전파하면서 미세하게 자신의 페이로드를 변경시키거나, 단편화를 발생시키면 이 접근 방법으로 시그니쳐를 추출할 수 없게 된다. [그림 6]은 두 문자열에 대해서 SE를 적용한 예를 보이고 있다.

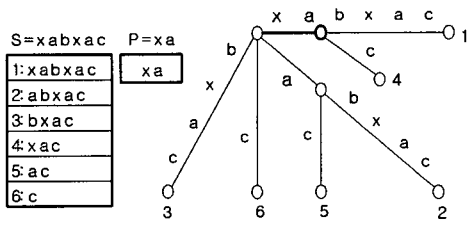

그림 6. String Equality

2.2 Longest Common Substring(LCS)

LCS는 SE처럼 정확하게 동일문자열을 추출한다는 점에서 동일하다. 하지만, SE는 동일한 문자열이 다수개 일 경우 SE는 동일한 문자열은 나열하는데 그치지만, LCS는 다수개의 동일 문자열 중 가장 긴 문자열을 추출해 준다는 데 그 차이점이 있다.

가장 긴 문자열은 추출해 주면 일부 패킷이 단편화되거나 미세하게 변경되어도 시그니쳐를 추출 할 수 있다. LCS로 연속된 동일 문자열을 찾는 과정을 suffix tree로 나타내면 [그림 7]과 같다.

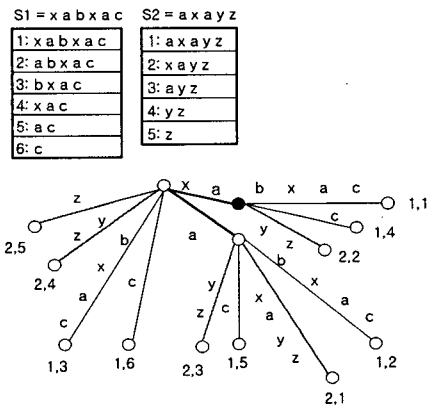

그림 7. Longest Common Substring

2.3 Longest Common Subsequence(LCSeq)

LCSeq는 LCS와 유사하다. 하지만, LCS는 동일 스트링의 순서에 상관없이 CS를 찾는 Order-insensitive 방법이지만, LCSeq는 동일 스트링의 순서를 고려하는 Order-sensitive 방법이다. 또한, LCS는 동일한 연속된 값을 찾아주지만, LCSeq는 연속되지 않은 동일한 스트링을 찾아 준다.

따라서 스스로 복제하면 변형된 형태를 지니는 다형성(Polymorphic) 웜의 시그니쳐를 찾는데 유용하다. 그러나 LCS보다 오탐지가 높은 단점이 있다. 다음은 LCS로 연속된 동일 문자열을 찾는 과정의 예이다. 두 개의 주어진 문자열 S1= 'ABCDEFCBGH', S2= 'FECBGAGFHE'에서 동일한 문자열을 추출한다. [그림 8]과 같이 LCSeq를 이용하여 시그니쳐를 추출하면 동일한 문자 'FCBGH'가 추출된다.

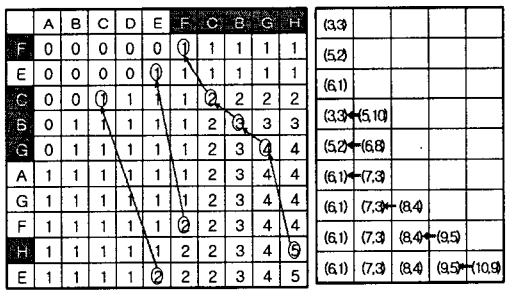

그림 8. LCSeq를 이용한 시그니쳐 추출

예를 들어, 다음과 같이 패킷 A, B의 페이로드가 구성되어 있다면,

```
A={GET/    default.ida?NN...NN%u9090%ucbd3%u7801=a
HTTP/1.0}
B={GET/default.ida?NN...NN%u9090%ucbd3%u9090%909
0%u7801=a HTTP/1.
```

그림 9. LCSeq를 이용한 시그니쳐의 결과

패킷 A는 원본 웜의 페이로드이고, B는 A가 전파되면서 NOP(Non-Operation) 코드가 삽입되어 변형된 형태의 웜이라고 가정할 때, 얻고자 하는 시그니쳐는 'GET/default.ida?NN..N%u9090%ucbd3%u7801=a HTTP/1.0' 형태가 될 것이다. [그림 9]는 LCSeq를 이용하여 얻을 수 있는 시그니쳐의 결과를 보이고 있다.

본 절에서는 수상한 패킷을 입력으로 3가지 스트링 알고리즘을 적용하여 시그니쳐 생성에 대해서 연구하였다. 이들 알고리즘을 적용할 경우 공통적으로 사용되는 정상적 문자열도 시그니쳐에 포함된다. 예를 들어 HTTP의 경우 'GET', 'HTTP/1.1', 'HOST' 등과 같은 필드가 그 예에 해당된다. 만약 이러한 문자열이 시그니쳐로 생성된다면 상당히 많은 오탐지가 발생될 것이다.

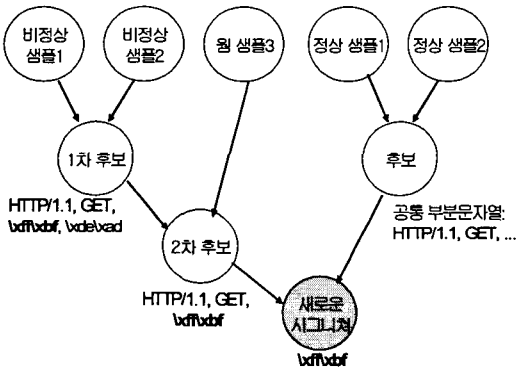

그림 10. 새로운 시그니쳐 생성

따라서 [그림 10]과 같이 오탐지를 줄이기 위해서는 정상 패킷과 수상한 패킷을 동시에 적용하여 비정상 패킷에서 생성된 시그니쳐 중에서 정상 패킷에서 생성된 시그니쳐를 제외한다면 오탐지를 상당히 줄일 수 있을 것이다.

V. 결 론

본 논문은 침입탐지 도구에서의 능동 대응정책 생성 방안에 대하여 연구하였다. 능동 대응형 침입탐지 시스템을 설계·구현하기 위한 선행 연구로서 능동 대응을 위한 침입탐지 도구의 요구사항을 7가지 구성요소로 고려하였고, 공격에 대한 능동 대응 방안으로 NIDS와 ADS를 통합한 모델을 기반으로 상호 유기적으로 시그니쳐를 생성할 수 있는 방안을 제시하였다.

능동적으로 Unknown Attack을 탐지할 수 있는 방법과 Unknown Attack 탐지를 통해 자동적으로 시그니쳐를 생성할 수 있는 방안을 연구하였다. 특히 Unknown Attack의 탐지를 위하여 트래픽 비정상행위 탐지와 프로토콜 비정상행위 탐지로 나누어 연구하였고 자동적인 시그니쳐 생성 엔진을 위해 헤더영역과 페이로드영역으로 나누어 연구하였다. 특히 페이로드 영역에서는 Suffix Tree를 이용하여 제시될 수 있는 시그니쳐 생성 방안들을 제안하였다.

참 고 문 헌

[1] http://csrc.nist.gov/publications/nistir/nistir-7007.pdf

[2] J. Zhang, J. Gong, and Y. Ding, "Research on automated rollbackability of intrusion response," Journal of Computer Security, Vol.12, No.5, pp.737-751, 2004.

[3] J. Newsome, B. Karp, and D. Song, "Polygraph: automatically generating signatures for polymorphic worms," Security and Privacy, IEEE Symposium, pp.226-241, May., 2005.

[4] J. Yu, Y. V. Ramana Reddy, S. Selliah, S. Kankanahalli, S. Reddy, and V. Bharadwaj, "TRINETR: An Intrusion Detection Alert Management System," 13th IEEE (WETICE'04), pp.235-240, 2004.

[5] http://www-2.cs.cmu.edu/~bkarp/autograp-husenixsec2004.pdf

[6] http://worminator.cs.columbia.edu/papers/2005/r-aidcut4.pdf

[7] K. Hwang, Y. Chen, and H. Liu. "Defending Distributed Systems Against Malicious

Intrusions and Network Anomalies," 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05), p.286a, 2005.

저 자 소 개

김 봉 한(Bong-Han Kim) 정회원

- 1994년 2월 : 청주대학교 전자계산학과(공학사)
- 1996년 2월 : 한남대학교 전자계산공학과(공학석사)
- 2000년 2월 : 한남대학교 컴퓨터공학과(공학박사)
- 2001년 3월~현재 : 청주대학교 컴퓨터정보공학과 교수

<관심분야> : 멀티캐스트, P2P, 정보보호

이 재 광(Jae-Kwang Lee) 정회원

- 1984년 2월 : 광운대학교 전자계산학과(공학사)
- 1986년 2월 : 광운대학교 전자계산학과(공학석사)
- 1993년 2월 : 광운대학교 전자계산학과(공학박사)
- 1986년 3월~1993년 8월 : 군산전문대학 전자계산학과 부교수
- 1993년 8월~현재 : 한남대학교 컴퓨터공학과 교수

<관심분야> : 컴퓨터네트워크, 정보통신, 정보보호

백 승 현(Seung-Hyun Paek) 정회원

- 현재 : 국가보안기술연구소(연구원)

오 형 근(Hyung-Geun Oh) 정회원

- 현재 : 국가보안기술연구소(선임연구원)

박 응 기(Eung-Ki Park) 정회원

- 현재 : 국가보안기술연구소(책임연구원)