제로데이 공격 대응력 향상을 위한 시그니처 자동 공유 방안

(Automated Signature Sharing to Enhance the Coverage of Zero-day Attacks)

김 성 기 † 장 종 수 †† 민 병 준 †††
(Sung Ki Kim) (Jong Soo Jang) (Byoung Joon Min)

요 약 공표되지 않은 취약성을 이용하는 악성코드에 의한 제로데이 공격에 대응하기 위한 목적으로 최근 시그니처 자동생성 시스템이 개발되었다. 자동 생성된 시그니처의 효용성을 높이기 위해서는 탐지 정확도가 우수한 고품질 시그니처를 식별하여 보안시스템에 적시에 공급할 수 있어야 한다. 이러한 자동화된 시그니처 교환 및 분배, 갱신 작업은 네트워크의 관리 경계를 넘어 보안상 안전한 방법으로 범용성 있게 이루어져야 하며, 보안시스템의 성능저하를 초래하는 시그니처 집합의 노이즈를 제거할 수 있어야 한다. 본 논문은 시그니처 재평가를 통해 고품질 시그니처의 식별과 공유를 지원하는 시스템 구조를 제시하고 시그니처의 교환 및 분배, 갱신을 다루는 알고리즘을 제시한다. 제시한 시스템과 알고리즘을 테스트베드로 구현 실험한 결과, 보안시스템에서 시그니처 집합의 노이즈를 줄이면서 제로데이 공격 대응력을 향상시키는 시그니처의 축적이 자동화됨을 확인하였다. 본 논문에서 제안한 시스템 구조와 알고리즘은 제로데이 공격 대응력을 향상시키는 시그니처 자동 공유 프레임워크로 활용할 수 있으리라 기대한다.

키워드 : 침입탐지, 시그니처, 데이터분배

Abstract Recently, automated signature generation systems(ASGSs) have been developed in order to cope with zero-day attacks with malicious codes exploiting vulnerabilities which are not yet publically noticed. To enhance the usefulness of the signatures generated by ASGSs it is essential to identify signatures only with the high accuracy of intrusion detection among a number of generated signatures and to provide them to target security systems in a timely manner. This automated signature exchange, distribution, and update operations have to be performed in a secure and universal manner beyond the border of network administrations, and also should be able to eliminate the noise in a signature set which causes performance degradation of the security systems. In this paper, we present a system architecture to support the identification of high quality signatures and to share them among security systems through a scheme which can evaluate the detection accuracy of individual signatures, and also propose a set of algorithms dealing with exchanging, distributing and updating signatures. Though the experiment on a test-bed, we have confirmed that the high quality signatures are automatically saved at the level that the noise rate of a signature set is reduced. The system architecture and the algorithm proposed in the paper can be adopted to a automated signature sharing framework.

Key words : Intrusion Detection, Signature, Data Distribution

· 본 연구는 인천대학교 자체연구비 지원에 의한 것임

† 정 회 원 : 선문대학교 IT교육학부 교수
skkim@sunmoon.ac.kr
†† 정 회 원 : 한국전자통신연구원 책임연구원
jsjang@etri.re.kr
††† 종신회원 : 인천대학교 컴퓨터공학과 교수
bjmin@incheon.ac.kr

논문접수 : 2010년 1월 12일
심사완료 : 2010년 3월 23일

정보과학회논문지: 정보통신 제37권 제4호(2010.8)

1. 서 론

인터넷에 만연하고 있는 악성코드와 사이버 위협에 대응하기 위해서 대부분의 네트워크 관리자들은 침입탐지시스템 (IDS) 또는 침입방지시스템(IPS)과 같은 보안시스템에 설치된 침입탐지용 시그니처에 의존하고 있다. 이 시그니처들은 주로 보안전문가들이 만들어 데이터베이스로 축적되는데, 아직 알려지지 않은 제로데이(zero-day) 공격에 대한 대응력을 결정짓는 시그니처의 품질과 갱신의 적시성이 지금까지는 모두 보안 전문가의 손에 달려 있다. 과거 수년간 Honeycomb[1], Autograph[2], EarlyBird[3] 와 같은 시그니처 자동생성시스템(ASGS: Automated Signature Generation Systems) 연구가 진행되었고, 최근에 한국전자통신연구원에서는 제로데이 웜 공격에 대응 할 수 있는 ZASMIN(Zero-day Attack Signature Manufacture INfrastructure)[4]을 개발하였다. 이 시스템은 Snort와 유사한 시맨틱을 갖는 탐지 시그니처를 자동 생성하고 검증한 다음, 원격 시스템으로 분배하기 위한 프로토콜을 제공한다.

ZASMIN과 같은 시그니처 자동생성 시스템이 생성한 시그니처를 적시성과 범용성 있게 다양한 보안시스템에 분배하고 갱신하려면 네 가지 문제점에 봉착하게 된다.

첫 번째 문제점은 시그니처 집합의 노이즈이다. 이것은 전체 보유한 시그니처 집합에서 효용성이 없는 시그니처들을 말한다. 일반적으로 시그니처들은 잘 대항할 수 있는 침입의 패턴이 제한되어 있다. 따라서 보안 시스템이 다수의 시그니처로 무장하고 있어도 해당 시그니처가 효력을 보이는 공격이 없거나 취약점이 제거되면 보안시스템에 해당 시그니처를 보유하고 있어야 할지의 여부를 자동적으로 결정하기 어렵다. 즉 공격이 없어서 "미탐지" 인지 공격이 있음에도 불구하고 "미탐지" 인지 단정하기 어렵다. 더욱이 취약점이 제거되어 실제 공격이 있어도 아무런 영향을 끼치지 않는다면 시그니처의 탐지정보는 보안시스템의 과탐지율을 높이는데 기여할 것이다. 결국 이러한 시그니처의 증가는 IDS/IPS의 성능을 저하시키는 노이즈로 작용하여 [5]에서 지적하고 있는 오탐지율을 높이는 요인이 될 수 있다. 침입탐지 이벤트 로그에서 의미 있는 침입탐지 정보를 추출하기 위한 [6]의 연구도 바로 이 문제를 해결하기 위한 노력이다.

두 번째 문제점은 "관리"의 문제이다. 시그니처 집합의 노이즈를 줄이는데 분산 보안시스템 간에 시그니처 교환이 도움을 줄 수 있다. 즉 시그니처 품질 비교와 재평가의 피드백을 이용하여 유효하지 않는 시그니처를 분리시킬 수 있다. 그러나 문제는 이러한 협업이 관리할 수 있는 도메인의 경계를 넘어 이루어지기 때문에 어떻게 안전하게 협업을 관리하고 지원하는지 시스템 구조와 방안이 필요하다.

세 번째 문제점은 시그니처 식별의 문제이다. 시그니처 교환을 위해서 개별 시그니처를 고유한 값으로 식별할 수 있는 방안이 필요하다. 그리고 해당 시그니처가 어느 정도 탐지 정확도를 보여주었는지 품질 속성을 포함하는 시그니처 표현 방안이 필요하다.

네 번째 문제점은 "범용성"의 지원이다. 교환되는 시그니처가 응용레벨과 독립적으로 어떤 IDS/IPS에도 범용적으로 적용 가능하도록 해야 한다.

본 논문에서는 이러한 네 가지 문제점을 해결하기 위한 프레임워크로서 탐지 정확도가 높은 시그니처의 교환 및 분배, 갱신을 지원하는 시스템 구조와 알고리즘을 제안하고 실험한 결과를 논한다.

본 논문의 2장에서는 관련연구에 대하여 논한다. 그리고 3장에서는 시그니처를 고유하게 식별하기 위한 방안을 논하고, 개별 시그니처의 품질이력을 관리하기 위한 시그니처 데이터 구조를 설계한다. 4장에서 시그니처 자동 공유를 위한 분산시스템 구조를 제시하고, 시그니처 교환 및 분배, 갱신을 위한 알고리즘을 설명한다. 5장에서는 구현 실험한 결과를 논하고 6장에서 결론을 맺는다.

2. 관련 연구

2.1 침입탐지 정보공유를 위한 시스템 구조

탐지 적중률이 높은 시그니처를 교환, 분배, 갱신하기 위해서는 침입탐지 정보를 교환하고 공유할 수 있는 시스템 구조 연구가 필요하다. 이와 관련한 연구로는 AAFID(Auto-nomous Agents for Intrustion Detecton)[7], GrIDS(Graph based IDS)[8], EMERALD (Event Monitoring Enabling Response Anomalous Live Disturbance)[9], SHOMAR[10]가 있다. 이 연구들은 공통적으로 [11]에서 지적하고 있는 지역 네트워크에서 하나의 IDS가 단독으로 운용될 때의 문제점을 해결하기 위한 노력들을 포함하고 있다.

2.2 침입탐지 시그니처 표현을 위한 포맷 연구

현재의 침입탐지 시그니처의 포맷은 보안 관련 단체나 보안시스템 벤더에서 개별적으로 관리되고 있고, 이 점은 이종 보안시스템 간에 네트워크를 통한 시그니처의 공유가 어렵다는 것을 말해준다. 이러한 문제를 해결하기 위해서 시그니처 표현을 통일하기 위한 포맷 연구가 진행되고 있다. 대표적인 연구로 AISF(ACME Intrustion Signature Format)[12], CIDSS(Common Intrustion Detection Singature Standard)[13]가 표준화를 위해서 제안되었다. 이 두 가지 포맷은 모두 이종의 IDS 시그니처를 저장하기 위한 공통의 데이터 포맷을 정의하고 있다. 따라서 그 포맷의 표현이 적응성과

응용을 고려한 XML에 기반을 두고 있다.

AISF는 시그니처 활용도를 높이기 위한 모듈 단위의 속성 집합을 지원한다. 시그니처 식별 모듈은 개별 시그니처들을 고유하게 식별하기 위한 속성 값들을 포함하고, 시그니처 정보 모듈은 침입이벤트의 위험도나 침입 유형의 범주, CVE(Common Vulnerability Exposure) [14] 및 BugTraq[15] ID와 같은 속성 값들을 포함한다. 시그니처 특성 모듈은 과탐지율 및 미탐지율과 같은 개별 시그니처의 품질속성 값들을 포함한다. 그리고 프로토콜 세부 사항에 대한 속성 값들을 담는 모듈들이 추가될 수 있다.

CIDSS는 아직 구체적인 시그니처 기능속성에 대한 정의가 불충분한 상태이다.

3. 시그니처의 식별방안과 시그니처 데이터 구조

3.1 시그니처의 식별과 바인딩

대규모 네트워크에서 시그니처를 교환하거나 분배, 갱신하려면 개별 시그니처를 고유하게 식별할 수 있어야 한다. 중복을 피하기 위한 단순한 식별을 넘어 개별 시그니처가 어떤 속성 값을 가지고 있는지 예를 들어, 탐지 적중도와 같은 품질 지수가 얼마인지를 확인할 수 있어야 고품질 시그니처를 선별할 수 있다. 본 논문에서 개별 시그니처를 고유하게 식별할 수 있는 속성 집합을 다음과 같이 표현한다.

$$S_{vid,sid,rev} \quad (1)$$

*vid*는 ASGS ID. 또는 시그니처를 제공하는 시스템(즉, IDS)을 고유하게 식별하는 값을 의미한다. *sid*는 특정 공격유형을 탐지하는 개별 시그니처를 식별하는 값이고, *rev*은 *sid*에 해당하는 시그니처 패턴의 변종이다. 만약 *vid, sid, rev* 값 모두가 일치한다면 해당 시그니처들은 동일한 시그니처로 간주된다. 이렇게 3 개의 값으로 시그니처를 식별하는 이유는 시그니처 교환과 분배에 따른 시그니처 제공처를 식별하고 수입한 시그니처에 대한 지역 품질 평가를 효과적으로 수행하기 위함이다.

IDS와 같은 보안시스템은 각각 시그니처의 표현이 달라 *sid* 값이 다르다. 그러나 공통의 취약점을 노리는 시그니처라는 점에서 CVE ID, BID(Bugtraq ID) 값을 참조하여 각 보안시스템의 시그니처를 연결할 수 있다[16].

3.2 시그니처 품질 속성 변수

본 논문에서는 개별 시그니처의 품질등급을 식별하기 위하여 다음과 같은 품질 속성 변수들을 새로이 정의한다. 모든 변수의 값들은 일정시간동안 탐지수행을 통해서 얻는 값들이다.

- *OAE*(Occurrence of Alert Events) : Alert 이벤트의 발생횟수
- *Hit* : 탐지 적중횟수
- *Hit Rate* : 탐지 적중률
- *FPR*(False Positive Rate) : 과탐지율
- N_s : IDS가 보유한 시그니처의 수
- N_{ts} : 임계값 이상의 Hit Rate를 갖는 시그니처의 수
- *Noise Rate* : 보유한 시그니처 중에서 임계값 이상의 Hit Rate를 갖는 시그니처 수의 비율

여기서 개별 시그니처의 Hit Rate, FPR, 하나의 IDS가 갖는 시그니처 집합의 Noise Rate는 다음과 같은 알고리즘으로 구한다.

- $HitRate = \frac{Hit}{OAE}$,

  $(OAE \geq Hit \geq 1,\ 0 \leq Hit\ Rate \leq 1)$ (2)
- $FPR = 1 - Hit\,Rate,\ (0 \leq FPR \leq 1)$ (3)
- $NoiseRate = 1 - \frac{N_{ts}}{N_s}$,

  $(N_s \geq N_{ts} \geq 1,\ 0 \leq Noise\ Rate \leq 1)$ (4)

3.3 시그니처 표현을 위한 데이터구조

본 논문에서 제안하는 프레임워크에서는 하나의 시그니처 표현을 위해 다음 그림 1과 같은 시그니처 변수들을 포함하는 데이터구조를 사용한다. 시그니처 표현을 위한 데이터구조는 시그니처 식별을 위한 변수들과 품질이력을 관리하기 위한 변수, 시그니처가 탐지한 패킷의 정보를 담고 있는 변수들로 구성된다.

- ASGS ID (또는 IDS ID)
- Signature ID
- Revision
- Hash value of Captured Packet Data
- Reference ID : CVE ID 또는 BID
- OAE
- Hit
- Hit Rate
- FPR
- Packet Payload Details
- Captured Packet Data

그림 1 시그니처 표현을 위한 데이터 구조

4. 시그니처 자동 공유를 위한 프레임워크

4.1 시그니처 자동공유 시스템 구조

시그니처의 자동공유는 세 가지 태스크 즉, 시그니처를 안전하고 적시성 있게 교환, 분배, 갱신하는 일을 포함한다. 본 논문에서는 분산된 IDS 간에 이러한 시그니처자동 공유 태스크를 수행하는 시스템 구조를 제안한다.

본 논문에서 제안하는 시스템 구조의 특징은 역할이 다른 이중화된 IDS를 통해서 시그니처 갱신에 따른 노

이즈를 최소화한다. 두 IDS 중 하나는 탐지 정확도가 높다는 것이 검증된 시그니처를 보유하고 있고 다른 하나는 품질이 검증되지 않은, 새로이 생성된 시그니처나 교환을 통해 수입한 시그니처, 탐지 정확도가 낮은 시그니처를 보유한다. 이렇게 IDS를 이중화하는 이유는 운용중인 IDS에 대해 시그니처 갱신을 수행했을 때 발생할 수 있는 부작용을 최소화하기 위함이다. 가장 큰 부작용으로는 다량의 시그니처 갱신 태스크에 따른 미탐지와, 시그니처 노이즈에 의한 오탐지 이벤트의 증가를 둘 수 있다. 아래 그림 2는 본 논문에서 제안하는 시스템 구조를 나타낸다.

제안하는 시스템은 관리 도메인 단위로 시그니처 자동생성시스템(ASGS), 시그니처 교환관리자(XM : eXchange Manger), 에이전트 소프트웨어로 구성된다. 에이전트 소프트웨어는 각 IDS로 분산되며 각 도메인의 교환관리자(XM)는 하나의 연합체를 이루도록 상호 신뢰관계를 유지하는 인프라스트럭처를 가지고 있다. 관리 도메인 내에서 에이전트와 XM, ASGS는 안전한 통신 채널로 보호된다.

ASGS가 시그니처를 생성할 때 마다 해당 시그니처와 패킷 바이트열이 XM이 관리하는 시그니처 DB에 저장된다. 주기적으로 XM은 XM 연합 내 타 XM의 고품질 시그니처를 *pull* 함으로서 갱신할 시그니처를 수집한다. XM은 이를 위해 그림 1과 같은 구조화된 데이터를 유지한다. 수집된 시그니처를 대상으로 Reference ID를 참조하여 시그니처 바인딩을 수행한다.

XM의 시그니처 DB에 저장된 시그니처들은 도메인 내 모든 IDS로 분산된다. IDS의 에이전트 소프트웨어들은 자신의 IDS 역할에 따라 XM의 시그니처 DB에서 시그니처 품질 속성 값을 참조하여 시그니처를 가져온다.

침입탐지는 Primary IDS와 Secondary IDS 모두가 동시에 수행하고 탐지수행에 관한 정보를 로깅한다. 로그에 대한 분석은 각 에이전트가 수행한다. 분석결과는 각 IDS의 시그니처 DB에 저장된 시그니처들에 대해서 품질속성 값의 변경으로 나타난다. 각 에이전트는 시그니처 품질속성 값을 참고하여 시그니처들을 재평가한다. 이때 탐지 적중률이 높은 고품질 시그니처들은 Primary IDS 의 시그니처 DB로 모이도록 교환이 이루어진다. 즉 일정 주기로 시그니처 재평가 후에 탐지 적중률이 기준치 이하인 시그니처들은 Secondary IDS의 시그니처 DB로 모이고 기준치 이상의 고품질 시그니처들은 Primary IDS의 시그니처 DB에 모이도록 Primary IDS와 Secondary IDS 간에 시그니처 수입과 수출이 이루어진다. 한편 XM이 특정 시그니처의 품질이 높은 정확도를 가졌다는 것을 XM 연합을 통해 발견하게 되면 해당 시그니처들은 Primary IDS의 시그니처 DB로 옮겨지고 시그니처 재평가과정을 밟는다.

4.2 시스템 엔티티간의 보안

본 논문에서 제안하는 시스템은 다음 그림 3과 같이 시스템 구성 엔티티간의 보안성을 제공한다.

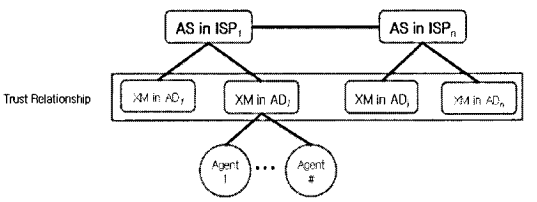


그림 3 시스템 엔티티간의 신뢰관계

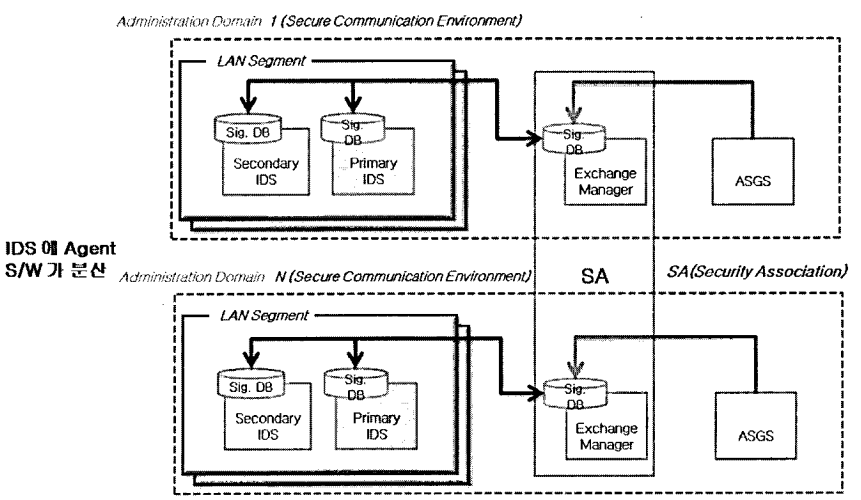


그림 2 시스템 구조

그림 3에서 각 관리 도메인의 XM은 복수의 에이전트와 연결을 맺는다. 이 연결은 상호 인증과 메시지 교환을 신뢰할 수 있음을 뜻한다. 마찬가지로 XM과 ISP의 인증서버(AS)의 연결도 동일한 보안성을 제공한다. 그러나 각 XM 간의 연결의 보안성은 ISP 인증서버에 의존한다. 동일한 ISP 인증서버를 이용하지 않는 XM간에는 인증서버간의 신뢰를 확인할 수 있는 메커니즘을 사용하여 신뢰관계를 맺을 수 있다.

4.3 XM에서 시그니처의 변환과 교환 메시지 형식

본 논문에서 제안하는 시스템에서는 XM에서 ASGS가 생성한 snort 기반 원시 시그니처를 XML 형식의 시그니처로 변환하는 과정을 수행한다. 이것은 시그니처를 그림 1에서 제시한 데이터 구조를 갖도록 표현함으로써 개별 시그니처를 식별하고 품질이력을 관리하기 위함이다. 아래 그림 4는 이러한 과정을 보여준다.

XM의 시그니처 DB에는 두 개의 테이블을 갖는다. 본 논문에서는 하나는 루키(rookie) 시그니처 테이블, 다른 하나는 에이스(ace) 시그니처 테이블이라고 부른다. 루키 시그니처들은 그림 4의 과정을 통해 XML 형식으로 표현된 품질 표시 시그니처들이거나 XM 간의 상호작용을 통해 수입된 시그니처들이다. 루키 시그니처들은 해당 도메인에서 침입탐지 수행에 투입된 적이 없어 장차 시그니처 품질 재평가가 이루어져야할 시그니처들이다. 에이스 시그니처들은 도메인 내 품질 재평가 과정에서 고품질 시그니처로 등급 판정된 시그니처들이다. 축적된 에이스 시그니처들은 XM간의 시그니처 교환 대상이 된다. XM 간의 시그니처를 교환하기 위해 SOAP(XML over HTTP) 프로토콜을 사용한다. 교환되는 메시지 형식은 그림 1의 데이터 구조를 준용한다.

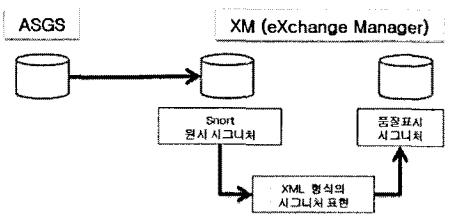


그림 4 XM에서의 시그니처 변환과정

4.4 시그니처 교환 및 품질 평가 알고리즘

가. Intra-domain 시그니처 교환 알고리즘

도메인 내에서 시그니처들은 각 IDS의 에이전트 소프트웨어에 의해서 주기적으로 다음 그림 5에 표현된 알고리즘에 따라 교환된다.

이 알고리즘 수행에 따라, Primary IDS는 Secondary IDS의 시그니처 DB로부터 FPR이 우수하다고 볼 수 있는 시그니처를 수입하게 된다. 이들 시그니처들은 침입탐지 수행 과정에서 실제로 탐지 적중률이 좋은지 평가 받게 된다. FPR이 우수하다고 봤지만 실제로 탐지 적중률이 저조했던 시그니처들은 재평가되어 Secondary IDS로 수출된다. 반대로 새로 생성된 시그니처들이 Secondary IDS에서 높은 탐지 적중률을 보였다면 Primary IDS의 시그니처 DB로 수출된다. 궁극적으로 Primary IDS의 시그니처 DB에는 탐지 적중률이 우수한 시그니처들만 남게 된다.

Step 1	XM의 루키시그니처를 Secondary IDS DB 로 수입
	Secondary IDS Agent 가 수행하며, XM의 루키 시그니처들을 자신의 DB로 가져온다
Step 2	Primary IDS Agent 가 수행, Secondary IDS DB 에서 루키 시그니처의 선별 수입
	for(looking up each sig. in Secondary IDS DB) { if(FPR of each sig. != null) && (FPR of each sig. <= threshold) 해당 시그니처들을 Primary IDS DB 로 수입; }
Step 3	Primary IDS Agent가 수행, Secondary IDS DB로 탐지 적중률이 임계값 보다 낮은 시그니처를 선별 수출
	for(looking up each sig. in Primary IDS DB) { if(Hit Rate of each sig. <= threshold) 해당 시그니처들을 Secondary IDS DB 로 수출; }
Step 4	Secondary IDS Agent가 수행, Primary IDS DB로 탐지 적중률이 임계값 보다 높은 시그니처를 선별 수출
	for(looking up each sig. in Secondary IDS DB) { if(Hit Rate of each sig. >= threshold) 해당 시그니처들을 Primary IDS DB 로 수출; }

그림 5 도메인 내에서 시그니처 교환 알고리즘

나. Inter-domain 시그니처 교환 알고리즘

대규모 네트워크에서 시그니처의 교환은 그림 6의 교환 알고리즘에 따라 이루어진다. 각 도메인의 XM에서

Step 1	*Primary IDS Agent* 가 수행, 자신의 Sig. DB에서 고품질 시그니처를 XM의 에이스 시그니처 테이블로 수출
	시그니처 품질 평가주기 마다 Primary IDS DB 에 남아있는 시그니처를 XM의 에이스 시그니처 테이블로 수출
Step 2	이웃 도메인의 XM_j 가 lookup 수행, XM_i 의 에이스 시그니처 테이블의 시그니처들에 대해서 선별적으로 *pulling* 수행
	for(looking up each sig. in Ace sig. table of XM_i) { if(Ace $S_{vid,sid,rev}$ in XM_i != Ace $S_{vid,sid,rev}$ in XM_j) { 해당 시그니처들을 XM_j 의 Ace Sig. 테이블로 *pulling* 수행; } }

그림 6 도메인 간에 시그니처 교환 알고리즘

주기적으로 타 XM의 에이스 시그니처 테이블을 참조하여 자신이 보유하지 않은 고품질 시그니처를 가져온다.

다. 시그니처 이력 갱신 알고리즘

시그니처가 침입탐지에 사용된 이력을 갱신한다. 관리 도메인 내부에서 Primary IDS와 Secondary IDS가 보유한 시그니처들은 동시에 침입탐지 수행에 적용된다. 각 시그니처들의 품질 속성 값들은 IDS에 유입되는 모든 패킷에 대하여 시그니처의 패턴을 비교한 후 재설정된다. 유입되는 패킷에서 시그니처에 대한 패턴이 존재한다면 경보 이벤트가 발생하여 품질 속성 변수 $\alpha\alpha e$ 값을 증가시키고 해당 패킷을 수집하게 된다.

라. 시그니처 품질 평가 알고리즘

시그니처 품질 평가 알고리즘은 개별 시그니처가 일정 시간동안 어느 정도의 탐지 정확도를 보여주었는지를 평가하는 것이다. 경보이벤트가 발생한 패킷이 실제 침입이면, Hit 수가 증가하고 식 (2)와 (3)에 의해서 FPR과 Hit Rate 값이 갱신된다. 경보 이벤트에 대한 실제 침입발생여부를 판정하는 것은 본 논문에서는 전문가나 별도의 도구를 이용하는 것으로 가정한다.

4.5 시그니처 분배 및 갱신 방안

탐지 시그니처의 분배는 그림 5와 그림 6의 알고리즘에 따라 XM과 각 IDS의 에이전트 소프트웨어에 의해서 자동적으로 이루어진다.

문제는 IDS가 의존하는 시그니처의 갱신이 모든 IDS 구현에 독립적으로 이루어질 수 있는 방안이 필요하다. 즉, 실제 IDS 구현이 그림 4에 설명한 품질표시 시그니처를 인식하도록 구현되어 있지 않다는 것이다. 본 논문에서는 이 문제를 해결하기 위해서, 원시 시그니처와 품질표시 시그니처를 연결하여 두 개의 로컬 시그니처 파일을 유지하고, 갱신 할 때 식 (1)을 매개로 원시 시그니처에서 품질표시 시그니처에 해당하는 시그니처만 유효하도록 갱신한다.

5. 실험 및 논의

5.1 실험 환경과 소프트웨어 도구

본 논문에서 제안하는 시그니처 자동 공유 프레임워크가 제로데이 공격 대응력 향상에 어떻게 기여하는지 알아보기 위해서 그림 2에서 제시한 시스템의 일부를 구현하였다. 실험 환경은 아래 그림 7과 같이 구성하였다.

IDS 소프트웨어는 공개 IDS 소프트웨어인 Snort를 이용하였고, ASGS는 임의의 시그니처들을 선정하여 XM에게 제공하는 일종의 서버로 가정하고 실험에서는 준비된 시그니처 집합을 사용하는 것으로 대신하였다. 침입실험은 알려진 취약점을 실제로 공격할 수 있는 도구를 제공하여 시스템 침입시험용으로 널리 알려져 있는 Metasploit 프레임워크[17]와 300 가지의 다양한 보안

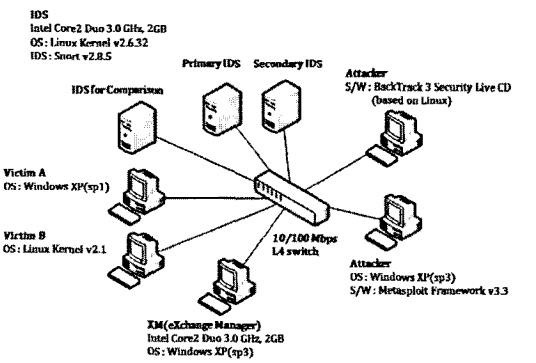


그림 7 실험환경

관련 도구들을 제공하는 BackTrack[18]을 이용하였다.

Metasploit은 다양한 공격 페이로드를 추가할 수 있는 스크립트 언어기반의 개발 환경을 제공하여 취약점을 찾아내는 도구로도 활용가능하며, Snort는 이러한 도구를 통해 발견한 공격패턴을 잡아내는 시그니처의 작성과 추가를 지원한다. [19]에서는 공개소스기반의 시그니처 집합을 제공한다. 제공되는 시그니처 집합에는 명백히 침입을 판정할 수 있는 시그니처와 그렇지 않는 시그니처 집합을 구분하고 있다.

이들 도구를 이용하여 공격대상 호스트에 대해 명백히 침입이라고 판정할 수 있는 공격과 대응 시그니처 집합을 사전에 식별하여 구분하였다. 표적 호스트는 공격도구를 참조하여 Windows 용과 Linux(또는 BSD Unix)용으로 구분하고 알려진 취약점이 상대적으로 많은 버전의 OS와 응용들을 설치하였다.

트래픽 발생을 위해 사용한 도구로는 Colasoft Packet Builder[20]를 이용하였다. 이 소프트웨어는 기존에 수집된 패킷파일을 읽어 올 수 있으며 패킷의 수정과 생성, 삽입, 정렬을 지원한다. 아울러 완성된 패킷집합에 대하여 네트워크 트래픽 재연을 지원한다.

5.2 실험내용 및 방법

실험은 시그니처를 교환, 갱신하였을 때, IDS가 보유한 시그니처 집합의 Noise Rate와 연산비용을 측정하였다. 실험에 사용되는 모든 탐지 시그니처들은 XM에서 XML 형식의 품질표시 시그니처로 변환될 때, 각 시그니처들의 FPR 초기값이 임의로 설정된다. 시그니처의 교환 및 갱신의 효과를 비교하기 위해 비교용 IDS에는 기능이 수정된 에이전트 소프트웨어를 설치하였다. 단순히 XM에서 시그니처를 가져와 시그니처 이력 갱신과 품질평가를 위한 알고리즘만을 수행한다.

실험은 XM에서 주기적으로 루키 시그니처를 가져오는 것을 가정하여 임의로 선택된 n 개의 시그니처를 비교용 IDS와 Secondary IDS에게 제공한다. 실험에 사용

한 시그니처의 수는 8,184 개이며, 본 논문의 실험에서 명백히 침입이라 판정한 시그니처의 수는 366개(공격의 수)이다.

정상 트래픽과 공격 트래픽의 혼합을 위해 Colasoft Packet Builder를 이용하였다. 수집된 정상 트래픽 패킷 파일과 앞 절에서 소개한 공격 소프트웨어 도구를 통해 수집한 공격패킷파일을 병합하였다. 모든 패킷에 대해서 발신지 및 수진지 IP 주소, 서비스 포트를 그림 7의 실험환경에 맞도록 수정한 후, 트래픽을 재연하였다. 실험은 시그니처 n개(n=1,000)를 단위로 반복된다.

5.3 실험결과 및 분석

실험결과는 그림 8과 그림 9와 같다. 이 결과는 그림 5의 시그니처 교환 알고리즘에서 임계치가 Hit Rate > 0.8, FPR < 0.2 인 조건이었을 경우의 결과이다.

그림 8의 결과는 제공된 시그니처를 단순히 보유한 경우와 시그니처 품질의 재평가 과정을 통해 유효하지 않는 시그니처를 분리한 결과이다. 실험을 통해서 Primary IDS에서는 개별 시그니처에 대해 Hit Rate 의 임계치를 높이고, Secondary IDS에서는 FPR의 임계치를 낮출수록 탐지 정확도가 높은 시그니처의 식별이 가능함과 동시에 시그니처의 수입과 수출을 위한 교환 횟수가 감소함을 발견하였다.

그림 9의 결과는 각 IDS 의 시그니처 집합의 노이즈를 보여줌과 동시에 침입탐지 수행에 소용되는 연산자원의 사용량을 보여주고 있다. Snort IDS는 패킷의 수집과 분류, 패턴 매칭, 기타 연산 등을 수행하기 때문에 침입탐지 수행에 따른 부하가 네트워크 트래픽량과 보유중인 시그니처의 수에 큰 영향을 받는다. 따라서 본 논문의 실험에서는 일정한 트래픽량(≒22.3Kpkts/sec)의 조건하에서 IDS의 시그니처 집합의 노이즈가 끼치는 영향을 분석하였다.

그림 9에서 시그니처 집합의 노이즈 비와 IDS의 부하부담률이 반드시 비례하지 않다는 것을 주목해야 한다. 노이즈비가 낮더라도 시그니처 보유수가 많은 경우, 제로데이 공격에 대한 보안시스템의 대응력이 높아진다는 것을 의미한다. IDS가 보유한 고품질 시그니처 수가 많아서 성능상의 문제가 된다면, 고품질 시그니처의 분할운용이 가능하다.

결론적으로 본 논문에서 제시한 실험 결과는 시그니처 분배가 이루어지더라도 시그니처가 효용성을 갖는 고품질 시그니처의 수는 제한된다는 사실을 보여준다. 즉 발생 가능한 모든 공격에 대한 준비로 모든 대응 시그니처를 보유하는 것이 중요한 것이 아니라 네트워크 환경과 응용에 따라 효용성 있는 시그니처의 선별을 위한 실시간 관리가 중요함을 뜻한다.

6. 결 론

본 논문에서는 제로데이 공격에 대한 대응력 향상을 위해 시그니처의 공유를 자동화 할 수 있는 프레임워크를 제시하였다.

제로데이 공격에 대응하기 위해서 고유의 대응력을 지닌 다수의 시그니처를 보안시스템이 보유하는 것이 능사는 아니다. 시그니처 자동생성 시스템이나 여타 다양한 수단의 지원으로 시그니처 교환과 분배와 같은 시그니처의 공유가 이루어지더라도 시그니처의 탐지 효용성을 사용처에서 보장 할 수 없다면, 제공된 시그니처는 보안시스템의 성능을 저하시키고 오탐지율을 증가시킨다.

본 논문에서는 이 문제를 해결하기 위해서 탐지 정확도를 신뢰할 수 있는 고품질 시그니처의 식별방안을 제시하였고, 범용성과 적시성을 고려하여 보안시스템에 자동적인 시그니처 공유를 지원할 수 있는 알고리즘과 시스템 구조를 제시하였다.

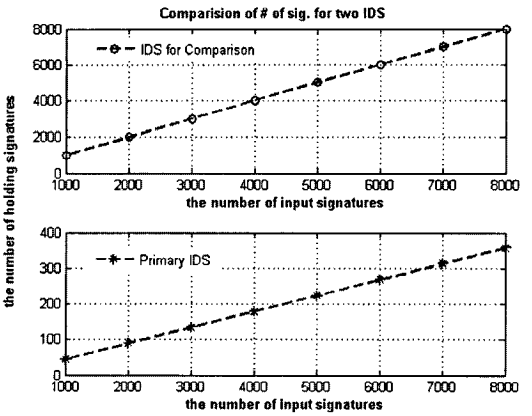


그림 8 시그니처 보유 수의 비교

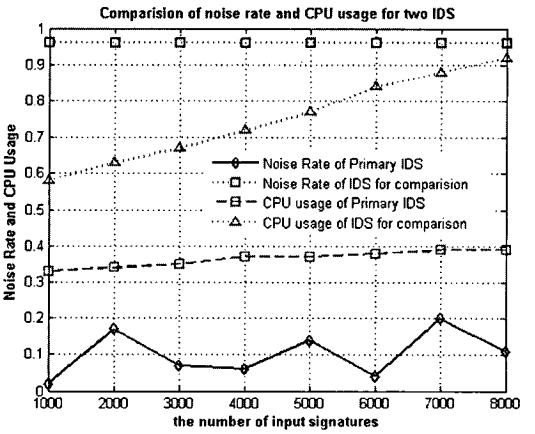


그림 9 Noise Rate와 CPU 사용량의 비교

참 고 문 헌

[1] C. Kreibich and J Crowcroft, "Honeycomb - Creating Intresion Detection Signatures Using Honeypots," Workshop on Hot Topics in Networks, 2003.

[2] H.A. Kim and B. Karp, "Autograph: Toward Automated, Distributed, Worm Signature Detection," 13th Usenix Security Symposium, 2004.

[3] S. Sinh, et. al., "Automated Worm Fingerprinting," 6th Symposium on Operating System Design and Implementation, 2004.

[4] 오진태, 김익균, 장종수, 전용희, "제로데이 웜 공격 대응을 위한 ZASMIN 시스템 구조", *한국정보보호학회*, 제18권 제1호, 2008. 2.

[5] Eric Frimpong, M.H.MacGregor, "A Performance Study of the Snort IDS," TR08-04, Department of Computing Science, University of Alberta, Feb, 2008.

[6] L. Perrochon. Using context-based correlation in network operations management. Technical report, Stanford University Department of Computer Science, 1999. http://pavg.stanford.edu/cep/ cidf.ps.gz.

[7] Eugene H. Spafford and Diego Zamboni, Intrusion detection using autonomous agents, Elsevier, Computer Networks, 34(4):547-570, October 2000.

[8] Eugene H. Spafford and Diego Zamboni, Intrusion detection using autonomous agents, Elsevier, Computer Networks, 34(4):547-570, October 2000.

[9] Philip A Porras and Peter G Neumann. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In Proceedings of the 20th National Information SystXMs Security Conference, pages 353.365, Baltimore, Maryland, USA, 7.10 October 1997. NIST, National Institute of Standards and Technology/National Computer Security Center.

[10] Undercoer, J.L., Perich, F., Nicholas, C.: SHOMAR: An Open Architecture for Distributed Intrusion Detection Services. Technical report, University of Maryland, Baltimore County (2002).

[11] Julia Allen, Alan Christie,William Fithen, John McHugh, Jed Pickel, and Ed Stoner. State of the Practice of Intrusion Detection Technologies. Technical Report 99tr028, Carnegie Mellon - Software Engineering Institute, 2000.

[12] Adriano M. Cansian, Artur R. A. da Silva, Marcelo de Souza : An Attack Signature Model To Computer Security Intrusion Detection. IEEE 2002.

[13] Internet Engineering Task Force - Common Intrusion Detection Signature Standard. http://tools.ietf.org /html/draft-wierzbicki-cidss-05. SeptXMber 4, 2008.

[14] Common Vulnerability Exposure, http://cve.mitre.org/

[15] BugtraqID, http://www.securityfocus.com

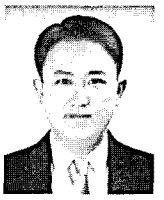
[16] http://xforce.iss.net/xforce/xfdb/2019

[17] http://www.metasploit.com

[18] http://www.remote-exploit.org

[19] http://www.emergingthreats.net

[20] http://www.colasoft.com



김 성 기

1996년 인천대학교 전자계산학과(학사) 1998년 인천대학교 컴퓨터공학과(석사) 2006년 인천대학교 컴퓨터공학과(박사) 2006년~2009년 인천대학교 초빙교수 2009년~현재 선문대학교 IT교육학부 전임강사. 관심분야는 컴퓨터 및 네트워크 보안, 분산시스템, 유비쿼터스 컴퓨팅

장 종 수

1984년 경북대학교 전자공학과(학사). 1986년 경북대학교 전자공학과(석사). 2000년 충북대학교 컴퓨터공학과(박사). 1989년~현재 한국전자통신연구원 책임연구원. 2004년~2008년 한국전자통신 연구원 네트워크보안그룹장. 2000년~ 2003년 한국전자통신연구원 네트워크 보안구조팀장. 2004년~현재 한국정보보호학회 이사(부회장). 2006년~현재 대검찰청 디지털수사자문위원회 위원. 2006년~2008년 행정안전부 전자정부서비스보안위원회 실무위원. 2008년~현재 방송통신위원회 인터넷정보보호협의회 안전인터넷분과 위원. 관심분야는 네트워크 보안

민 병 준

1983년 연세대학교 전자공학과(학사). 1985년 연세대학교 전자공학과(석사). 1991년 미국캘리포니아대학교(UC Irvine) 전기및컴퓨터공학과(박사). 1984년~1986년 삼성전자 연구원. 1992년~1994년 KT 선임연구원. 1994년 감사원 사무관. 1995년~현재 인천대학교 컴퓨터공학과 교수 관심분야는 컴퓨터 및 네트워크 보안, 분산시스템, 유비쿼터스 컴퓨팅