독립적인 보안관리 도메인간 효과적인 사이버보안정보 교환 방법의 설계 및 구현

정회원 안 개 일*°, 서 대 희*, 임 선 희*, 김 종 현*, 서 동 일*, 종신회원 조 현 숙*

Design and Implementation of Mechanism for Effectively Exchanging Cybersecurity Information between Independent Security Management Domains

Gae-il An*°, Dae-hee Seo*, Sun-hee Lim*, Jong-hyun Kim*, Dong-il Seo* ***Regular Members***,
Hyun-sook Cho* ***Lifelong Member***

요 약

현재 사이버보안 위협을 방어하기 위한 하나의 방편으로서 보안 관리 도메인간 사이버보안 정보 공유를 통하여 전체 네트워크에 대한 보안 성능을 높이려는 연구가 활발히 진행되고 있다. 사이버보안 정보를 교환할 때 큰 이슈가 되는 것 중의 하나는 각 도메인이 서로 독립적이기 때문에 정보공유에 관련된 각 도메인의 요구사항이 서로 다르다는 것이다. 본 논문에서는 공유정책과 공유정책제어 프로토콜을 통하여 보안관리 도메인의 정보공유에 관한 요구사항을 반영함으로써 사이버보안정보의 교환을 효과적으로 제공할 수 있는 사이버보안정보 교환 방법을 제안한다. 아울러 본 논문에서는 제안하는 방법을 제공하는 통합보안제어 시스템을 개발하고 그 시스템상에서 제안하는 방법의 성능을 평가한다.

Key Words : Cybersecurity Information, Information exchange, Sharing policy, 정보공유

ABSTRACT

As a way for defending against cyber security threats, there has been a research on cybersecurity information exchange between security management domains in order to raise security performance of the whole network. One of the hottest issues in exchanging cybersecurity information between security management domains is that the requirements of those domains on information sharing are different with each other because each is autonomous domain. This paper proposes a mechanism for effective cybersecurity Information exchange between independent security management domains, which can satisfy their requirements on information sharing through sharing policy and sharing policy control protocol, proposed in this paper. In this paper we have developed an integrated security control system that supports the proposed mechanism. Through the system the performance of the proposed mechanism is measured and evaluated.

Ⅰ. 서 론

최근 컴퓨터 하드웨어 및 IT 기술의 발달과 모바일 환경의 활성화에 따른 반대급부로서 보안위협이 크게 증가하고 있다. 스팸, 바이러스, 서비스 거부 공격 등 사이버 공격 기법이 더욱 더 다양화될 뿐만 아니라 공

※ 본 연구(2011/10914-06002, 전역적 협력기반의 통합보안제어 시스템 개발)는 방송통신위원회 정보보호 원천기술개발 사업의 일환으로 수행됨.

* 한국전자통신연구원 지식정보보안연구부({fogone, dhseo, capsunny, jhk, bluesea, hscho}@etri.re.kr), (° : 교신저자)

논문번호 : KICS2011-05-225, 접수일자 : 2011년 5월 22일, 최종논문접수일자 : 2011년 11월 28일

격전파속도도 크게 단축되면서 단일 컴퓨팅 자원에 대한 공격 형태에서 인프라 자체를 공격하여 통신 네트워크 자체를 마비시킬 수 있는 치명적인 공격 형태로 진화되고 있다. 실 예로 2009년도 및 2010도의 웜/바이러스 건수는 전년도에 비해 각각 22.7%, 72.5%로 계속 증가하는 추세[1]이며, 2010년도에 발생한 7.7 DDoS 공격의 피해 규모가 큰 이유는 공격 대상이 개별시스템 공격이 아니라 네트워크 전체를 대상으로 했기 때문이라고 분석되고 있다.

사이버 공격을 탐지하고 방어하기 위한 가장 전통적인 연구는 IDS(Intrusion Detection System), IPS(Intrusion Prevention System), 방화벽과 같은 보안 시스템의 공격 탐지/차단 성능 및 정확도를 높이려는 연구이다. 그러나 지금처럼 복합적이고 다양한 형태로 변형되거나 새로이 등장하는 위협 및 공격들이 자동으로 전파되어 정보통신 인프라를 공격하는 추세에서는 보안 시스템의 성능 향상만으로는 지능화되고 고도화된 사이버 공격위협을 효과적으로 차단하기에는 역부족인 상황이다. 이러한 문제를 해결하기 위하여 최근에는 ISP (Internet Service Provider)와 같이 서로 다른 보안 관리 도메인간에 공격탐지 정보, 침해사고 정보, 공격대응정보 등의 사이버보안 정보를 서로 공유함으로써 협력을 통하여 전체 네트워크에 대한 보안을 제공하려는 연구가 진행되고 있다[2-5]. 여기서 사이버보안 정보란 사이버환경과 조직 그리고 사용자 자산을 보호하기 위해 사용될 수 있는 정보(예, 침해사고, 유해사이트, 유해콘텐츠, 보안분석, 사이버공격에 관한 정보)이다[2].

보안관리 도메인간 사이버보안정보 교환을 위해 제안된 프레임으로서 ITU-T (ITU-T, International Telecommunications Union - Telecommunication)에서 표준으로 제안하는 CYBEX (CYBersecurity information Exchange) 모델[2]이 있다. 사이버보안 정보를 교환하기 위한 표준 프로토콜로서는 IETF (Internet Engineering Task Force) 표준화 단체에서 개발한 IDMEF(Intrusion Detection Message Exchange Format)[6,7], IODEF (Incident Object Description and Exchange Format)[8,9], 그리고 RID(Real-time Inter-network Defense)[10] 프로토콜이 있다.

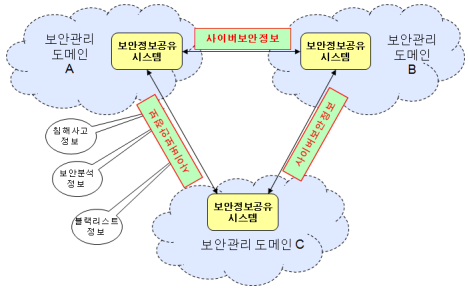

그림 1. 사이버보안정보 공유의 개념도

기존의 사이버보안 정보 교환방식은 정보 제공 도메인이 정보 요청 도메인에게 일방적으로 정보를 전송하는 정적인 형태의 정보교환방식이다. 이 방식은 정보 제공 도메인과 정보 요청 도메인이 정보공유에 관한 상대의 요구사항을 모르기 때문에 정보공유 요구사항이 변경되었을 때 대처할 수 없다는 문제가 있다. 즉, 정보 제공 도메인은 정보 요청 도메인의 요구사항을 고려하지 않기 때문에 정보 요청 도메인이 필요하지 않는 정보가 전송되어 정보공유 효율성이 떨어지며, 또한 정보 요청 도메인은 정보 제공 도메인의 사이버정보공유에 관련된 요구사항을 모르기 때문에 수신한 사이버보안정보를 분석할 때 어려움을 겪을 수 있다.

이러한 문제를 해결하기 위하여 본 논문에서는 사이버보안정보를 교환하는 보안관리 도메인의 정보공유에 관한 요구사항을 동적으로 반영함으로써 사이버보안정보 교환을 효과적으로 제공할 수 있는 방법을 제안한다. 제안하는 방법은 크게 공유할 사이버보안 정보를 제어하기 위해 정의된 공유정책과 그 공유정책을 원격으로 제어하는 정책제어 프로토콜로 구성된다. 사이버보안정보 공유에 관한 각 도메인의 요구사항은 공유정책에 명세되고, 그 요구사항의 변경은 공유정책을 수정하는 정책제어 프로토콜을 통하여 수행된다.

본 논문에서 제안하는 동적형태의 보안정보 공유방식이 동작하기 위해서는 보안정보를 공유하는 해당 도메인들간의 협상이 먼저 선결되어야 한다.

상대 도메인의 승인없이 정보공유에 관한 요구사항을 반영할 수 없기 때문이다. 본 논문에서는 보안정보 공유협상에 대해서는 다루지 않으며, 보안정보를 공유하는 도메인들은 이미 협상이 완료되어 상대 도메인의 요구사항을 허락한다고 가정한다.

본 논문의 구성은 다음과 같다. 2장에서는 사이버보안 정보 교환에 관한 기존 연구를 살펴보고, 3장에서는 독립적인 보안관리 도메인의 요구사항을 고려하여 사이버보안정보를 효과적으로 교환할 수 있는 사이버보안정보 교환 방법을 제안한다. 4장에서는 프로토타입 시스템 개발을 통하여 제안하는 방법의 성능을 측정하고 평가한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련 연구

사이버정보공유 교환기술은 주로 ITU-T와 IETF에서 개발하고 있는데, ITU-T에서는 사이버정보공유 교환 프레임워크에 중점을 두고 있으며, IETF에서는 사

이버보안 정보공유 프로토콜 등의 핵심 요소기술 개발에 초점을 맞추고 있다.

그림 2는 ITU-T에서 사이버보안 엔터티(Entity)간 사이버보안정보 교환 프레임워크로 제안하고 있는 CYBEX 모델[2]이다. 사이버보안 엔터티란 사이버보안 정보를 제공하거나 제공받는 조직 또는 사람을 말한다. 사이버보안 정보는 사이버 환경과 조직 그리고 사용자 자산을 보호하기 위해 사용될 수 있는 툴, 정책, 가이드라인, 액션, 훈련, 기술 등의 정보를 의미한다. CYBEX 모델은 사이버보안 정보교환을 위한 정보 구조화, 사이버보안 정보 및 엔터티의 식별과 검색, 사이버보안 엔터티간 신뢰와 정책 합의 설정, 사이버보안 정보의 요청과 응답, 그리고 사아버보안 정보 교환시 무결성 보장을 위한 기술을 개발하고 있다. CYBEX 모델에서는 사이버보안 정보의 전송 포맷 및 프로토콜은 IETF 등 다른 표준단체에서 제정한 프로토콜을 그대로 수용하고 있다.

사이버보안정보를 교환하기 위한 표준 프로토콜로서는 IETF 표준화 단체에서 개발한 IDMEF[6,7], IODEF[8,9], 그리고 RID[10] 프로토콜이 있다. IDMEF는 IDS 및 IPS와 같은 공격 탐지 시스템이 탐지한 공격 이벤트에 대한 경보(alert)를 보안관리 시스템에게 보고하기 위한 데이터 포맷 및 데이터 교환 절차를 정의하고 있다. IDMEF는 경보를 생성한 분석기(analyzer) 식별정보, 경보가 생성된 시간, 경보가 탐지된 시간, 분석기의 현재 시간, 공격 시스템과 타켓(목적지) 시스템에 대한 정보, 공격정보, 공격 위험도와 경보에 대응하기 위해 실행된 액션 등의 정보를 표현할 수 있다.

IODEF 프로토콜은 보안침해사고 대응팀(CSIRT: Computer Security Incident Response Team) 상호간에 컴퓨터 보안 사고에 대한 정보를 공유하기 위한 데이터 표현을 정의하는 것을 목적으로 한다. IODEF 프로토콜은 보안사고가 언제, 어디서 발생했고, 누가 어떤 공격 수법을 사용했는지, 그리고 사고 피해는 어떠한지 등 컴퓨터 보안 사고에 대한 전반적인 정보를 전달하기 위하여, 침해사고 식별 번호, 침해사고가 탐지/시작/종료/보고된 시간, 침해사고에 대한 설명, 침해사고와 관련된 단체의 연락처, 피해상황, 사용된 공격기술, 침해사고 처리동안 일어났던 이벤트 및 액션, 그리고 침해사고를 구성하는 이벤트들에 대한 정보를 표현할 수 있다.

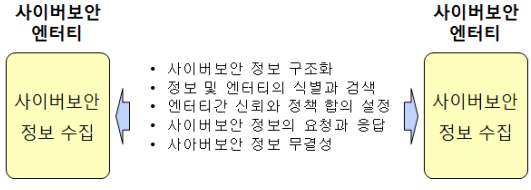

그림 2. CYBEX 모델

RID 프로토콜은 IDMEF 및 IODEF 프로토콜을 수용하며, 침해사고 처리를 위한 모든 일련의 과정들을 용이하게 지원하기 위해 제안되었다. RID 프로토콜은 사이버보안 정보 공유 시스템간의 공격 탐지 정보, 공격 시스템 추적 및 식별, 그리고 공격 대응 메커니즘 등 침해사고 처리와 관련된 데이터의 공유를 목적으로 한다.

Ⅲ. 사이버보안 정보 제어 방법

3.1 사이버보안정보 교환 구조

보안관리 도메인간 사이버보안 정보를 교환할 때 가장 큰 이슈중 하나는 각 도메인들마다 사이버보안 정보를 요청하거나 제공할 때의 요구사항이 서로 다르다는 것이다. 예를 들어, 사이버공격탐지 데이터를 제공하는 어떤 도메인은 사용자 프라이버시(Privacy) 문제 때문에 교환할 정보에 포함된 IP 주소를 외부에 공개하지 말아야 하는 요구사항을 가질 수 있으며, 사이버보안 정보를 수신하는 도메인도 내부 보안요구사항에 따라서, 모든 원시 데이터를 원할 수도 있고, 또는 보안 심각도가 높은 데이터나 아니면 단순히 사이버공격 통계정보만을 필요로 하는 등 사이버보안정보 공유에 관해 다양한 요구사항을 가질 수 있다.

CYBEX 프레임워크 등 기존의 연구는 사이버보안 정보 제공자가 요청자에게 교환할 보안정보를 일방적으로 제공하는 구조이기 때문에 각 도메인의 다양한 요구사항을 반영할 수 없는 정적인 형태의 보안정보공유 방식이다. 이러한 방식에서는 정보 수신 도메인이 정보 제공 도메인의 요구사항을 모르기 때문에 사이버보안 정보를 활용할 때 부정확한 결과가 도출될 수 있다. 또한 정보 수신 도메인은 정보공유에 관한 자신의 요구사항이 정보 제공 도메인에게 제공하지 않기 때문에 불필요한 사이버보안 정보가 교환될 수 있다. 예를 들어, 공격탐지로그 정보를 공유하는 경우에 사이버 공격의 강도와 크기에 비례하여 공유되는 정보의 양이 결정되는데, 만약 엄청난 규모의 보안정보를 수신하는 경우에 이를 적절히 제어할 수 없다면 정보를 수신하는 도메인에서는 혼잡 문제를 겪을 수 있다.

본 논문에서는 정보요청 도메인이 정보제공 도메인의 사이버보안 정보를 제어하게 함으로써 사이버보안 정보를 효과적으로 교환할 수 있는 방법을 제안한다. 그림 3은 본 논문에서 제안하는 방법의 구조이다. 그림

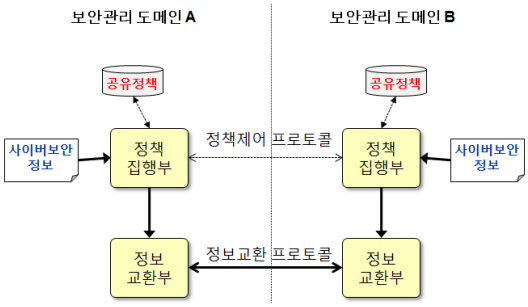

그림 3. 제안하는 사이버보안정보 교환 구조

3에서, 기존의 보안정보교환 방식은 사이버보안 정보, 정보 교환부, 그리고 정보교환 프로토콜로 구성된다. 이에 반하여 본 논문에서 제안하는 동적 교환방식은 기존의 정적 교환방식의 구성요소에 공유정책과 정책 집행부, 그리고 정책제어 프로토콜이 추가로 정의된다. 공유정책은 공유할 사이버보안 정보를 제어하기위해 정의된 정책이다. 공유정책은 사이버보안정보에 대한 전송 요구사항(예, 암호화 유무 등), 데이터 요구사항(예, 통계 데이터 또는 원시 데이터), 프라이버시 요구사항(예, IP 주소 마스킹) 등의 정보를 포함한다. 정책 집행부는 도메인 내부에서 수집된 사이버보안 정보를 입력 받으면 공유정책을 적용하여 외부의 다른 도메인에게 제공할 사이버보안정보를 생성한다. 정책제어 프로토콜은 사이버보안 정보를 공유하는 도메인의 요구사항에 해당하는 공유정책을 제어(삽입/삭제/수정/검색)하는 프로토콜이다. 마지막으로 정보교환부는 다른 도메인과 사이버보안 정보를 직접 공유(제공/수신)하는 역할을 한다. 정보교환 프로토콜로는 IDMEF, IODEF, RID 등이 사용될 수 있다.

본 논문에서 제안하는 사이버보안 정보 교환 방법은 사이버보안 정보 공유에 관한 각 도메인의 요구사항은 공유정책에 명세되고, 그 요구사항의 변경은 정책제어 프로토콜을 통하여 수행된다. 그림 3의 보안관리 도메인 A가 B에게 사이버보안정보로서 공격탐지정보를 제공하는 경우를 가정할 때, 본 논문에서 제안하는 방법의 사이버보안 정보 공유 시나리오는 다음과 같다. 먼저, 보안관리도메인 A에서는 IDS 및 IPS 등의 보안 시스템에 의해 탐지된 공격탐지 정보를 수집하여 정책집행부에게 전달한다. 정책집행부는 전달받은 공격탐지 정보를 수신할 보안관리 도메인 B에 대한 공유정책을 검색한다. 정책집행부는 검색된 공유정책에 따라서 공격탐지 정보를 가공한 후에 그 결과를 정보 교환부에 넘겨준다. 마지막으로 정보 교환부는 넘겨받은 정보를 정보교환 프로토콜을 통해 보안관리도메인 B에게 전송한다. 만약 정보공유중에 보안관리 도메인 B의 정보공유에 관한 요구사항이 바뀌면, 정책제어 프로토콜을 통하여 보안관리 도메인 A에게 공유정책변경을 요청한다.

3.2 사이버보안 정보 공유정책

사이버보안 정보 공유정책은 도메인간에 공유할 사이버보안 정보를 제어하는 규칙들의 집합으로서, 내부의 원시 사이버보안정보를 입력 받아서 외부로 제공할 가공된 사이버보안정보를 생성하는 방법이라 할 수 있다. 정보를 공유하는 도메인의 요구사항에 따라서 다양한 종류의 공유정책을 정의할 수 있는데, 본 논문에서는 사이버보안정보 전송에 관한 가장 기본적인 정책으로서 필터링, 요약, 그리고 마스킹 등 세 종류의 규칙을 정의한다.

CSSP, R, S, P를 공유정책, 원시 사이버보안정보, 원시 사이버보안정보의 집합, 그리고 가공된 사이버보안정보라고 다음과 같이 정의할 때,

- CSSP: CyberSecurity information Sharing Policy
- R: a Raw cybersecurity information
- S: a Set of R, $S \supset R$
- P: a Processed cybersecurity information

필터링 규칙 $CSSP^F$, 요약 규칙 $CSSP^S$, 마스킹 규칙 $CSSP^M$의 정의는 다음과 같다.

- $CSSP^F$: $S_x \rightarrow S_y$, $S_x = \{R_a .. R_b\}$, $S_y = \{R_c .. R_d\}$, $a \leq c \ \& \ b \geq d$
- $CSSP^S$: $S \rightarrow P$
- $CSSP^M$: $R_x \rightarrow R_y$, $R_x \supseteq R_y$, $R_y \neq \varnothing$

보안정보 필터링 규칙은 정보제공자가 보유한 사이버보안 정보 리스트들 중에서 공유할 정보를 뽑을 때 사용되는 규칙이며, 보안정보 요약 규칙은 사이버보안 정보에서 요약/통계 정보를 추출하는 규칙이다. 마지막으로 보안정보 마스킹 규칙은 정보제공자가 보유한 사이버보안 정보중에서 공개하지 말아야 할 정보를 명세한 규칙이다.

그림 4는 사이버보안 공유정책의 일 예이다. 공유정책은 조건과 그 조건이 만족될 때 실행될 액션으로 구성된다. 사이버보안 공유정책에서 조건은 "수신도메인", "수집정보", "전송주기" 등의 필드로 구성되며, 액션은 "검색필드명", "최소순위", "랭킹방법", "출력정보", "비공개필드명", "마스킹값"으로 구성된다. 그림 4에서 명세된 필터링 규칙은 "수집정보가 보안로그이고 수신할 도메인이 ISP A 또는 ISP B" 이고 이 규칙이 최

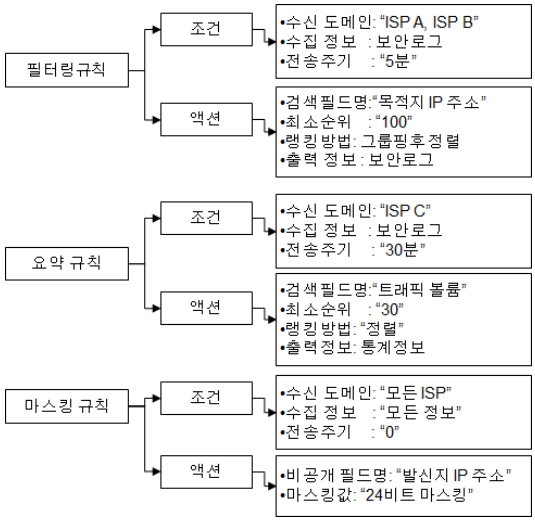

그림 4. 사이버보안 공유정책의 예

근에 실행된 후 5분이 지났으면, 목적지 IP 주소로 그룹핑하고 정렬한 후 순위 100위 안에 드는 보안로그를 출력하라" 라는 의미이다. 그림 4에서 요약 규칙은 "수집정보가 보안로그이고 수신할 도메인이 ISP C" 이고 이 규칙이 최근에 실행된 후 30분이 지났으면, "트래픽 볼륨값으로 보안로그를 정렬한 후 순위 30위 안에 드는 보안로그에 대한 통계정보를 출력하라" 라는 의미이다. 마지막으로 그림 4의 마스킹 규칙은 "수집정보와 수신할 도메인에 상관없이 발신지 IP 주소를 24비트 마스킹하라" 라는 의미이다.

그림 5는 보안정보 공유정책 적용 알고리즘으로서 사이버보안 정보를 제공하는 시스템에서 실행된다. 보안정보 제공 시스템은 보안정보 요청 도메인/시스템에게 기 설정된 보안정보 공유정책을 기반으로 하여 공유할 사이버보안 정보를 생성하고 전송한다. 즉, 보안정보 제공 시스템은 보안정보 요청 도메인을 결정하면, 먼저 그 요청 도메인에 해당하는 보안정보 공유정책을 검색한다. 만약 공유정책에 요약 규칙이 존재하면 그 요약 규칙에 따라서 원시보안정보를 입력으로 받아서 요약통계정보를 출력으로 생성한다. 만약 필터링 규칙이 존재하면 그 필터링 규칙에 따라서 원시보안정보를 필터링하여 남겨진 보안정보를 출력으로 생성한다. 만약 요약 규칙이나 필터링 규칙이 존재하지 않으면 원시보안정보는 그대로 출력된다. 출력된 보안정보(또는 요약통계정보)는 마스킹 규칙이 존재하면 출력된 보안정보내에 포함된 개인정보(예, IP주소)를 마스킹 규칙에 따라 마스킹하여 최종 보안정보를 생성한다. 마지막으로, 최종 보안정보에 대한 프로토콜 메시지가 생성하

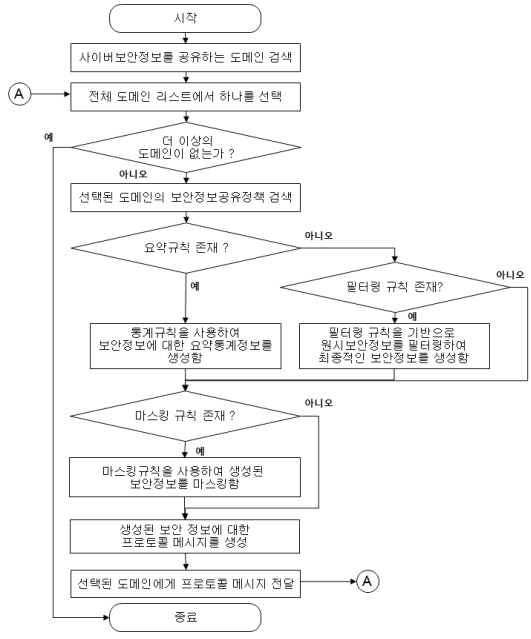

그림 5. 보안정보 공유정책 적용 알고리즘

여 선택된 보안정보 요청 도메인에게 전달한다.

Ⅳ. 구현 및 성능평가

4.1 프로토타입 구현

본 논문에서는 제안하는 독립적인 보안관리 도메인간 사이버보안정보 교환 방법을 제공하는 COSMOS (CO-operative Security Motoring System)라고 명명한 통합 보안 제어 시스템을 개발하였다. COSMOS 시스템은 에이전트와 서버로 구성된다. COSMOS 에이전트는 각 독립적인 보안관리 도메인에서 운용되며 사이버보안 공격 정보(예, DOS, 봇넷 등 공격탐지정보)와 블랙리스트 정보를 수집하여 COSMOS 서버에게 제공하는 역할을 한다. COSMOS 서버는 전역관점에서 전체 보안관리 도메인의 보안상황을 모니터링하는 것을 목적으로 하며 에이전트로부터 전달된 보안정보 분석을 통하여 대응/차단할 공격지 주소를 결정한 후 해당 COSMOS 에이전트에게 알려준다. COSMOS 시스템은 Apche Tomcat 6.0에서 Adobe Flex Air 2.0과 Java SE 1.6 프로그램 언어를 사용하여 구현하였다.

COSMOS 에이전트는 EMS(Enterprise Management Security), TMS(Threat Management Security), IPS 와 같은 보안 시스템으로부터 사이버 보안정보를 수집하기 위하여 syslog 프로토콜을 사용한다. COSMOS 에이전트와 COSMOS 서버간 사이버보안정보 교환을 위한 프

로토콜은 IETF에서 제안한 IODEF를 사용한다. COSMOS 에이전트와 COSMOS 서버간 공유정책 제어 프로토콜로는 요구-응답형 프로토콜형태로 자체 정의하여 개발하였다. 공유정책 제어 프로토콜의 메시지 포맷 및 데이터 모델링은 그림 6에 도시되어 있다. Msg_Type, Peer_ID, length, SecuritySharing-PIB는 각각 메시지의 타입, 공유정책을 적용할 에이전트 ID, SecuritySharing-PIB 길이, 보안공유정책 PIB(Policy Information Base)를 의미한다. 메시지 타입으로는 Get, Set, 그리고 Result가 있다. Get은 Peer_ID에 대한 공유정책을 문의할 때, Set은 Peer_ID에 대한 공유정책을 설정할 때, 그리고 Result는 Get과 Set에 대한 응답 메시지로서 Peer_ID에 설정된 공유정책을 담고 있다. Set과 Result 메시지는 Get 타입의 메시지와 달리 Length와 SecuritySharing-PIB 필드를 포함한다. IODEF와 공유정책 제어프로토콜은 Python과 XML 언어를 사용하여 개발하였다.

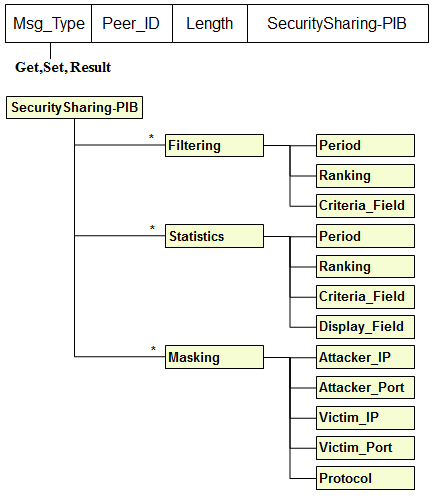

그림 6. 공유정책 제어 프로토콜의 메시지 포맷 및 데이터 모델링

4.2 성능 평가

본 논문에서는 제안하는 방법의 성능을 분석하고 평가하기 위하여 그림 7과 같은 환경을 구축하였다.

각 COSMOS 에이전트에 저장된 COSMOS 서버에 대한 공유 정책의 값을 수정하면서 두 가지 실험을 진행하였다. 첫 번째 실험은 사이버보안 정보를 제공하는 보안관리 도메인의 요구사항을 본 논문에서는 제안하는 방법이 지원하는지에 관한 실험이다. 실험 결과, 다른 도메인에게 공격탐지 정보를 제공하는 각 COSMOS 에이전트의 관리자는 사용자 프라이버시에 관한 요구

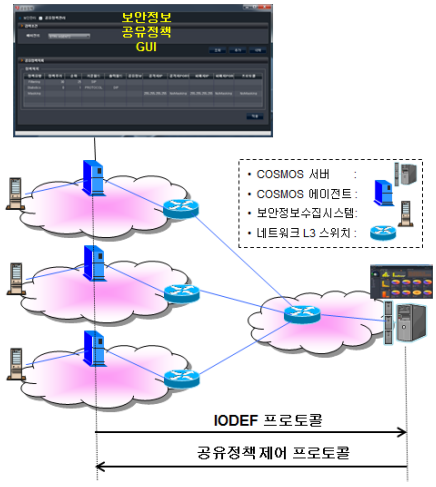

그림 7. 시험 환경

사항을 GUI를 통해 쉽게 입력할 수 있었으며, 입력된 요구사항은 마스킹 정책으로 변환되고 COSMOS 에이전트에 적용되어 다른 도메인에게 IP 주소가 마스킹된 공격탐지정보를 제공하였다. 따라서 본 논문에서 제안하는 방법은 보안정보 제공자의 요구사항을 만족시키는 것을 실험을 통하여 확인하였다.

두 번째 실험은 사이버보안정보를 수신하는 보안관리 도메인의 요구사항을 본 논문에서는 제안하는 방법이 만족시키는지에 관한 실험이다. 그림 8은 COSMOS 에이전트와 COSMOS 서버간 보안로그 전송 성능에 대한 실험 결과이다. 그림 8에 도시된 바와 같이 전송할 보안로그가 증가할수록 전송시간도 그와 비례하여 증가하는 것을 볼 수 있다. 본 실험을 통하여 교환할 사이버보안 정보의 규모가 클수록 또는 동시에 정보공유를 위해 통신하는 도메인의 수가 늘어날수록 사이버보안 정보 교환시 혼잡이 발생할 가능성이 높기 때문에 사이버보안 정보 공유 성능이 떨어질 수 있는 문제를 확인하였다. 정보공유 성능문제 때문에 사이버보안 정보를 수신하는 도메인은 모든 원시 보안정보 데이터가

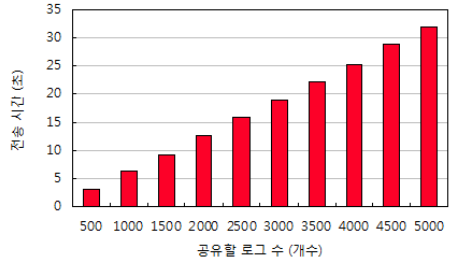

그림 8. 공유하는 보안로그 수에 따른 전송시간

아닌 일부 유용한 정보만을 원하는 요구사항을 가질 수 있다. 본 논문에서 제안하는 방법은 공유정책을 제어함으로써 사이버보안정보를 수신하는 독립적인 보안관리 도메인의 정보공유에 관한 다양한 요구사항을 만족시킬 수 있음을 실험을 통하여 확인하였다. 그림 9와 그림 10은 보안정보 공유정책의 성능을 측정한 실험이다.

그림 9는 COSMOS 에이전트가 서버에게 보안로그를 1000개 보냈을 때의 보안정보 공유정책별 보안로그 전송시간을 비교한 실험결과이다. 그림 9에서 X, Y축은 각각 "최소순위" (그림 4와 그림 6 참조)와 전송 시간이다. 실험결과, 보안정보공유 성능은 공유정책을 적용했을 때가 더 뛰어나며, 공유 정책중에서 통계 규칙이 필터링 규칙보다 더 우수하였다. 즉, 공유정책이 적용되지 않았을 때는 약 6초정도가 소요되었지만, 필터링 정책이 적용되었을 때는 최소순위 값에 따라서 0.6초에서 3.5초 걸리며, 통계 정책이 적용되었을 때는 0.05초에서 0.17초 정도 소요되었다.

그림 10은 전송메시지 수에서 필터링과 통계정책을 비교한 실험 결과이다. 그림 10에 도시된 바와 같이 통계정책이 필터링 정책보다 전송메시지 처리 수에서 성능이 우수하며, 랭킹이 증가하면 할수록 성능차이는 더 커지고 있다. 필터링 정책과 통계정책은 랭킹이 같음에도 불구하고 전송메시지 수가 크게 차이 나는 이유는 필터링 정책은 조건을 만족시키는 보안 로그가 하나 이상일 수 있기 때문이다. 예를 들어, "검색필드명"이 공격지 IP 주소이고 "최소순위"가 1라고 설정되었을 때, 순위가 1위인 1.1.1.1인 공격지 IP를 포함하는 보안로그가 100개라고 가정하면 필터링 규칙에서는 전송할 보안로그의 수는 100개지만, 요약 규칙에서는 단 1개이다.

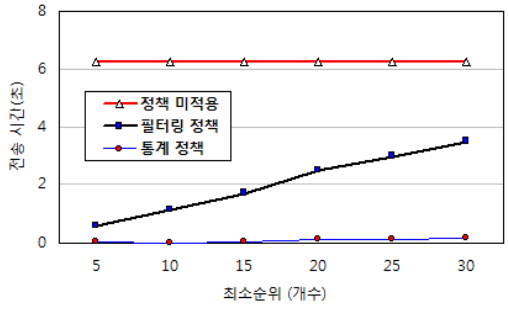

그림 9. 공유정책 규칙별 보안정보공유 성능

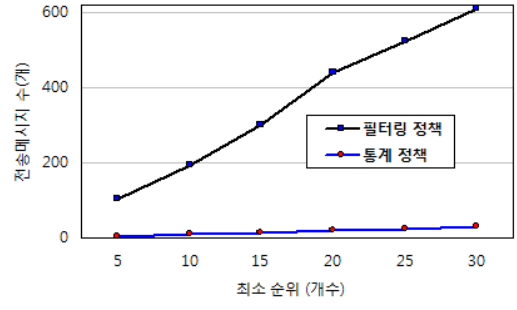

그림 10. 필터링 정책과 통계 정책 비교

V. 결 론 및 향후 연구과제

사이버보안 정보 교환은 정부, 금융, ISP, 기업 등 공공의 인터넷 환경에서 다양한 사이버보안 정보들을 상호 공유하고 관리하여 사이버 보안 위협들에 대해 빠르게 대응하기 위한 체계를 제공할 수 있기 때문에 도메인간 보안정보공유는 점점 더 활성화 될 것으로 기대된다.

본 논문에서는 독립적인 보안관리 도메인들이 자신의 요구사항을 만족시키면서 사이버보안정보를 교환할 수 있는 방법을 제안하였다. 제안하는 방법은 사이버보안정보 공유에 관한 각 도메인의 요구사항은 공유정책으로 명세하고, 그 요구사항이 변경되면 정책제어 프로토콜을 사용하여 공유정책을 수정하기 때문에 서로 다른 다양한 요구사항을 갖는 보안관리 도메인상에서 효과적인 보안정보 공유를 제공할 수 있다.

본 논문에서는 필터링, 마스킹, 요약 등 세 종류의 정보공유 규칙만을 정의하였지만 보안정보를 교환하는 도메인은 전송방법, 정보이용요금 등 다양한 요구사항을 가질 수 있기 때문에 정보 공유정책에 대한 연구가 더 필요할 것이다. 또한 본 논문에서는 사이버보안정보를 공유하는 도메인들은 상대방의 요구사항을 모두 따른다고 가정하였지만, 실제로는 그렇지 않을 것이다. 즉, 보안정보를 제공하는 도메인과 수신하는 도메인의 요구사항이 서로 부합되는 지 확인하는 과정이 필요하다. 이에 대한 연구는 향후연구과제로 남긴다.

참 고 문 헌

〔1〕 통계청, "웜/바이러스 피해 현황," http://www.index.go.kr/egams/stts/jsp/potal/stts/PO_STTS_IdxMain.jsp?idx_cd=1364

〔2〕 Anthony Rutkowski, Youki Kadobayashi, Inette Furey, Damir Rajnovic, Robert Martin, Takeshi Takahashi, "CYBEX - The Cybersecurity Information Exchange Framework (X.1500)," *ACM SIGCOMM Computer Communication Review*, Vol.

40 Num. 5, pp. 59-64, Oct. 2010
〔3〕 E. Kenneally and K. Claffy, "An Internet Data Sharing Framework For Balancing Privacy and Utility," *First International Forum on the Application and Management of Personal Electronic Information*, pp. 1-6, Oct. 2009.
〔4〕 Messaging Standard for Sharing Security Information (MS3i) Project, "Messaging standards for computer network defence warnings and alerts," *JLS/2007/EPCIP/007 - Project Report*, June 2009
〔5〕 정일안, 오진태, 장종수, "보안 정보 공유 기술 및 표준화 동향," *전자통신동향분석*, 제23권 제4호, pp. 30-38, 8월, 2008.
〔6〕 M. Wood and M. Erlinger, "Intrusion Detection Message Exchange Requirements", *IETF*, RFC 4766, March 2007
〔7〕 H. Debar, D. Curry and B. Feinstein, "The Intrusion Detection Message Exchange Format (IDMEF)", *IETF*, RFC 4765, March 2007
〔8〕 J. Arvidsson, A. Cormack, Y.Demchenko, J. Meijer, "TERENA's Incident Object Description and Exchange Format Requirements," *IETF*, RFC3067, Feb. 2001
〔9〕 R. Danyliw, J. Meijer, Y. Demchenko, "The Incident Object Description Exchange Format," *IETF*, RFC 5070, Dec. 2007
〔10〕 K. M. Moriarty, "Real-time Inter-network Defense," *IETF*, RFC 6045, Nov. 2010

안 개 일 (Gae-il An) 정회원

1993년 2월 충남대학교 컴퓨터공학과 졸업
1995년 2월 충남대학교 컴퓨터공학과 석사
2001년 8월 충남대학교 컴퓨터공학과 박사
2006년 7월~2007년 6월 미국 Security University 포닥연구원
2001년 8월~현재 한국전자통신연구원 선임연구원
<관심분야> 네트워크 보안, 네트워크 시뮬레이션, 개인정보보호, 사이버보안 정보공유

서 대 희 (Dae-hee Seo) 정회원

2003년 2월 순천향대학교 전산학과 석사
2006년 2월 순천향대학교 전산학과 박사
2006년 4월~2007년 4월 Howard University post-doc
2008년 7월~2009년 9월 이화여자대학교 컴퓨터 정보통신공학부 연구교수
2009년 10월~현재 한국전자통신연구원 선임연구원
<관심분야> 정보보호, 네트워크 보안, 보안성 평가

임 선 희 (Sun-hee Lim) 정회원

1999년 2월 고려대학교 컴퓨터학과 학사
2005년 2월 고려대학교 정보보호대학원 석사
2010년 8월 고려대학교 정보보호대학원 박사
2010년 9월~현재 한국전자통신연구원 선임연구원
<관심분야> 무선이동통신보안, 통합보안제어

김 종 현 (Jong-Hyun Kim) 정회원

2000년 오클라호마주립대 컴퓨터과학과 공학석사
2005년 오클라호마주립대 컴퓨터과학과 공학박사
2005년~현재 한국전자통신연구원 선임연구원
2000년~2001년 삼성SDS 시스템컨설턴트
1995년~1997년 삼성전자 연구원
<관심분야> 정보보호, 사이버보안, 역추적기술

서 동 일 (Dong-il Seo) 정회원

1989년 2월 경북대학교 전자전자공학과 졸업
1994년 2월 포항공대 정보통신과 석사
2004년 8월 충북대학교 전산학과 박사
1994년 3월~현재 한국전자통신연구원 팀장(책임연구원)
2010년 3월~현재 충남대학교 겸임교수
<관심분야> 인터넷정보보호, 미래인터넷 보안 등

조 현 숙 (Hyun-sook Cho) 정회원

1979년 2월 전남대학교 수학교육과 졸업
1989년 2월 충북대학교 컴퓨터학과 석사
2001년 2월 충북대학교 컴퓨터학과
1982년 3월~현재 한국전자통신연구원 부장(책임연구원)
<관심분야> 정보보호, 지식정보보안 및 융합