도메인간 보안 정보 공유를 통한 협력 대응 프레임워크 설계

이영석* · 안개일** · 김종현**

Design of Collaborative Response Framework Based on the Security Information Sharing in the Inter-domain Environments

Young-seok Lee* · Gae-il An** · Jong-hyun Kim**

요 약

국가 및 공공기관의 정보통신망에 대한 최근의 사이버공격은 날로 지능화·고도화 되어 갈 뿐 아니라 심지어 경쟁상대국이 국가기밀이나 첨단산업기술 절취를 위해 국가차원에서 조직적으로 감행하는 경우도 있어 새로운 국가안보의 위협요소로 대두되고 있다. 이러한 사이버공격에 효율적으로 대응하기 위해서는 기존의 정보보호시스템 운용만으로는 한계가 있어 사이버공격을 실시간 탐지, 분석·대응하는 협력 대응 프레임워크가 그 중요성을 더해가고 있다. 이에 본 논문에서는 사이버 위협 실태와 대응방안에 대한 기술 및 표준화 동향을 살펴보고, 도메인간 보안 정보 공유를 위한 협력 대응 프레임워크를 설계한다. 협력 대응 프레임워크에서 보안 정보 공유 기반 네트워크 위험도 산출 방식을 제안한다. 이를 기반으로 네트워크 위험 상황을 신속하게 탐지하여 보안 정책에 따라 실시간적인 행동을 수행할 수 있도록 하는 것이 가능하다.

ABSTRACT

Recently, cyber attacks against public communications networks are getting more complicated and varied. Moreover, in some cases, one country could make systematic attacks at a national level against another country to steal its confidential information and intellectual property. Therefore, the issue of cyber attacks is now regarded as a new major threat to national security. The conventional way of operating individual information security systems such as IDS and IPS may not be sufficient to cope with those attacks committed by highly-motivated attackers with significant resources. In this paper, we discuss the technologies and standard trends about actual cyber threat and response methods, design the collaborative response framework based on the security information sharing in the inter-domain environments. The computation method of network threat level based on the collaborative response framework is proposed. The network threats are be quickly detected and real-time response can be executed using the proposed computation method.

키워드

사이버 공격, 협력 대응 프레임워크, 보안 정보 공유

Key word

Cyber Attack, Collaborative Response Framework, Security Information Sharing

* 종신회원 : 군산대학교 정보통신공학과 (leeys@kunsan.ac..kr)
** 정회원 : 한국전자통신연구원

접수일자 : 2011. 01. 04
심사완료일자 : 2011. 01. 28

Ⅰ. 서 론

최근 사이버 공격의 유형이 분산 반사 서비스 거부(DRDoS : Distributed Reflected Denial of Service) 공격과 같이 지능화, 님다 바이러스와 같이 웜 바이러스 내에 악성코드를 심는 통합화, 개별 시스템에 대한 공격에서 네트워크 또는 서비스를 공격대상으로 하는 대규모화, 자동화된 공격도구를 이용한 자동화 및 대중화, 분산 서비스 거부(DDoS : Distributed Denial of Service) 공격과 같은 분산화 및 트로이목마와 같은 은닉화의 특성을 나타내고 있다.

이러한 사이버 공격은 시스템 및 네트워크의 취약점 등을 통해 급속하게 전파되는 형태를 띠고 있으며, 공격들은 상호 결합되어 그 확산 정도나 파괴력은 점점 증가하여 피해 사례와 피해규모도 커지고 있는 추세이다. 이와 같이 가까운 시일 내에 취약점에 대한 패치가 발표되기 전에 공격이 이루어지는 제로데이 공격(Zero day attack)을 포함한 수많은 사이버 공격에 대한 적극적인 대응이 필요하게 되었고, 다양한 대응 기술과 함께 사이버 공격에 대한 전 세계적인 정보공유 체계와 그 표준화의 필요성이 대두하게 되었다[1].

또한, 트래픽의 과도한 증가와 다양한 공격 유형에 보다 효율적으로 대응하기 위해서는 현재의 지역적 보안 환경을 광역망 또는 백본만 환경으로 확장 적용할 수 있는 광역 네트워크 보안 제어 프레임워크 기술이 필요하다. 지역망의 경우는 자신의 입력 트래픽의 분석에 주력하지만 광역망의 경우는 각 지역망의 출력 트래픽들을 종합 분석하고 망의 구성정보, 상태 정보, 주요 관리 요소 정보 및 트래픽 통계 정보 등과 연계한 다단계 분석을 통한 침입 예측 및 환경에 적합한 대응 정책의 결정 인가가 가능하게 될 것이다.

이를 위해서는 고속의 분석 엔진, 트래픽 측정 엔진 등의 개발이 필요하며, 이들이 제공하는 정보를 축약하기 위한 기법의 개발과 이들을 전달하기 위한 프로토콜의 표준화, 인접 영역과의 보안 제어를 위한 협력 메커니즘의 수립, 계층적인 침입분석 기법의 개발, 종합적인 침입대응 시나리오의 정의, 사용자 요구에 다른 차별화된 보안 서비스 품질을 제공하기 위한 차등 보안 서비스 개발, 효율적인 관리를 위하 공통정보 모델링 등이 필요하다.

본 논문에서는 이를 효과적으로 적용하기 위해 보안 관리 프레임워크 구조를 모델링하고 IETF(Internet Engineering Task Force)에서 추진하고 있는 표준화 동향을 참고하여 정책 프레임워크에 따라 적합한 인터도메인 협력 대응 프레임워크 구조를 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 보안 정보 공유 관련 기술동향을 살펴보고, 3장에서는 협력 대응 프레임워크 설계를 기술한다. 4장에서는 협력 대응 프레임워크에서 보안 정보 공유 기반 네트워크 위험도 산출 방식을 제안하며, 5장에서 결론을 맺는다.

Ⅱ. 관련 기술 동향

2.1 사이버 보안 정보 교환 표준화 동향

2009년 6월 말 스위스 제네바에서 열린 국제전기통신연합 연구반 17(정보보호) 연구과제 4(사이버보안) 인터림(interim) 회의에서는 글로벌 사이버보안 표준을 주도하고자 하는 국제전기통신연합의 의지와 비전이 구체화되기 시작했다.

사이버보안 연구과제 인터림 회의에서는 미국 대표가 미국 정부 사이버보안 정책의 일환으로 해석될 수 있는 새로운 글로벌 사이버보안 정보 교환 프레임워크라는 권고안을 제안했고, 일본, 미국, 한국 등의 사이버보안 전문가들이 참여하여 좀 더 구체화되었다. 이 권고안의 약어는 X.cybief(global CYBsecurity Information Exchange Framework)로 토의를 통해 확정되었고, 최종 드래프트 권고안 채택 여부는 2010년 9월 국제전기통신연합 연구반 17 회의에서 결정되었다[2].

현재까지 논의되고 있는 사이버보안 정보는 사이버보안과 관련되는 장치, 소프트웨어 등의 상태(취약성 정보 포함), 침해사고와 관련되는 디지털 포렌식(Forensic) 정보, 침해사고 경험으로부터 얻은 서명 및 학습 데이터, 정보교환 주체, 정보교환 규격, 관련 주체 및 정보 신원(Identity), 그리고 구현 요구사항 등에 대한 구조화된 정보로 정의되었다[3].

따라서, 사이버보안 정보는 각 장치가 갖는 취약성 정보, 사이버 공격 증거를 추적하기 위한 특수 침해사고 포렌식 정보, 침입차단시스템 또는 침입방지시스템 등이 수집한 일반 침해사고 포렌식 정보, 그리고 합법 감청 관련 인터페이스 및 정보 등을 포함하며, 여기에 더해 바이

러스 정보, 피싱 사이트과 악성코드를 포함하는 웹사이트 정보 등 명성 관련 정보도 포함되며, 네트워크상에 사이버 공격을 실시간으로 추적하기 위한 증거 데이터까지도 포함하고 있다.

현재 이 표준은 사이버보안 정보 교환을 위한 모든 표준화 기구와 관련 조직에 의해 만들어진 기존 표준들을 확인하고 일부 필요하다고 판단되면, 이들 중 필요한 경우 일부를 국제전기통신연합 표준으로 채택하며, 필요한 경우 기존 표준을 개선하고 새로운 표준을 개발하여 사이버보안 정보교환을 위한 글로벌 표준으로 만드는 것에 목적이 있다.

현재 그림 1은 연구과제 4(사이버보안)에서 합의한 사이버보안의 능력과 문맥을 나타내고 있다.

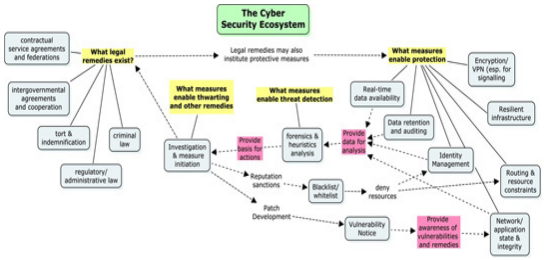

그림 1. 사이버보안 능력 및 문맥
Fig 1. Cyber Security Capability and Context
(출처: 국제전기통신연합 연구반 17 연구과제 4의 연구과제 텍스트에서 발췌)

그림 1에서 알 수 있듯이 사이버보안은 침해사고 관련 데이터의 실시간 제공 수단, 실시간 데이터를 근거로 침해사고의 발생 여부를 검출하는 수단, 검출 결과를 근거로 필요한 조치를 취하는 기술적 수단, 이를 지원하기 위한 법제도적 지원 등으로 달성된다. 이 생태계가 적절하게 동작하기 위해서는 각 수단 간에 적절한 사이버 정보가 안전하고 신뢰적으로 교환되어야 한다. 따라서 이 권고안은 이러한 사이버보안 문맥 하에서 서로 교환되어야 할 사이버 정보 교환을 위한 프레임워크를 제공할 것이다[4].

2.2 보안 정보 공유 프레임워크 표준화 동향

ITU-T의 X.1206 표준 권고안은 자동으로 보안 관련 정보를 알리고 업데이트를 전파하기 위한 벤더 중립적인 프레임워크를 규정하고 있다. 일단 자산이 등록되면 취약점, 패치 및 업데이트 정보를 사용자에 의해 또는 애플리케이션에 직접 자동적으로 업데이트 한다.

그림 2는 이 표준 권고안의 프레임워크를 적용한 취약점, 업데이트, 패치 분배 시스템의 구조를 간략하게 표현한 예이다. 각 자산, 디바이스 또는 지역 서버가 어떤 또는 모든 서버에 등록되어 있으면 취약점 정보, 업데이트 또는 패치 정보들을 요청하거나 제출할 수 있게 된다. ITU-T의 X.sisfreq 표준 초안은 시스템의 취약점, 공격, 악의적인 행위 정보 등에 관한 보안 정보들을 공유하기 위한 프레임워크의 요구사항을 규정하는 것이다.

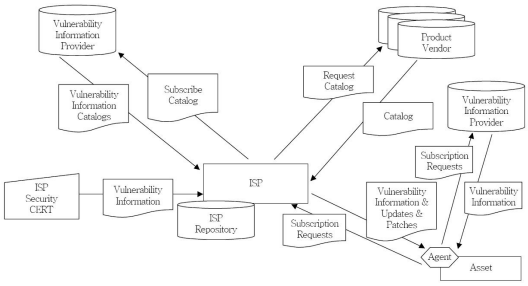

그림 2. 애플리케이션 구조의 예
Fig 2. An Example of Application Architecture

보안 정보 공유 기술을 상용화시 상호호환성을 보장하기 위한 프레임워크를 정의하기 위해 활용될 것이다. 현재 사이버보안 정보공유를 위한 보안 분야에서 논의되기 시작한 드래프트 단계의 표준 초안으로 일본과 한국이 공동 에디터로 활동하여 작성하고 있다[4].

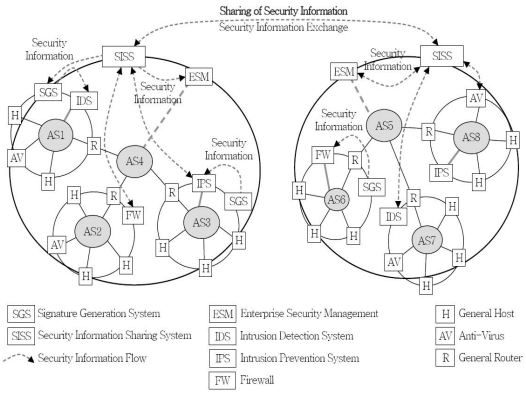

그림 3. 보안 정보 공유 프레임워크의 개념적 구조
Fig 3. Conceptional Architecture of Security Information Sharing

그림 3은 보안 정보 공유 프레임워크의 개념적 구조를 표현한 것으로, 보안 시스템들에서 생성된 보안 정보들을 수집하여 관리하거나 다른 국가, 기관, 기업 등에 분배하여 상호 공유하는 역할을 담당한다. 이 표준 초안에서는 여러 가지 연구 사례들과 프레임워크가 갖춰야 할 요구사항들을 정의해 가고 있다.

Ⅲ. 협력 대응 프레임워크 설계

사이버 침해 사고는 비대면성과 익명성의 특징이 있다. 사이버공간의 익명성으로 인하여, 공격자와 피해자의 대면이 없기 때문에 과격한 행동을 반복적으로 수행할 가능성이 많다. 또한, 최근 전문성을 갖춘 해커들의 출현과 인터넷을 통해 국가 간의 경계가 모호함으로 국제적인 광역성의 특징도 나타내고 있다. 사이버 공격의 사전 인지가 쉽지 않고 피해가 쉽게 전파되는 잠재성과 전파성도 갖고 있다. 실시간 공격이 가능하며 장소 및 시간의 제약이 없기 때문에 동시성과 함께 시간적·공간적으로 제한이 없는 특징도 내포하고 있다.

이러한 사이버 침해 사고를 방지하기 위해 사이버 보안 정보를 모델링하여 도메인 간의 침해 사고 예방을 위한 협력 대응 프레임워크 설계의 고려사항으로 제시되어야 한다.

3.1 보안 정보 모델링

네트워크에서 발생되는 위험을 시속하게 탐지하고 타 도메인과 정보를 교환하기 위해서 우선위험을 구성하는 자산과 취약점, 그리고 위협의 상관관계를 살펴본다.

취약점이란 시스템이 비정상적인 동작을 수행하도록 하는데 악용될 수 있는 소프트웨어적인 결함이라고 정의한다. 네트워크상의 각종 자산이 가질 수 있는 소프트웨어적인 취약점과 네트워크에서 운용되고 있는 자산의 종류 및 각 자산의 잔류 취약점을 다음과 같이 분류할 수 있다[5].

- V1(전체 취약점) : 모든 자산[1]이 가지고 있는 알려진 전체 취약점으로 취약점 분석시스템(VAS, Vulnerability Analysis System)의 DB로 저장
- V2(잠재 취약점) : 대상 네트워크에서 운용되고 있는 자산의 알려진 모든 소프트웨어적인 취약점
- V3(잔류 취약점) : 잠재 취약점(V2) 중 보안 패치 등을 통해 제거되지 않고 남아있는 취약점

이들 취약점간의 관계를 그림 4와 같이 나타낼 수 있다.

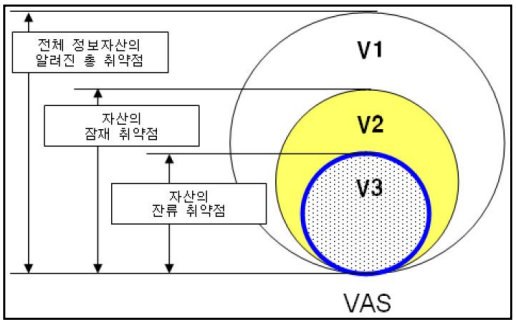

그림 4. 취약점 분류
Fig 4. Vulnerability classification

위협은 자산에 바람직하지 않은 영향을 줄 수 있는 잠재적인 요인으로 정의할 수 있으며, 이 같은 위협이 현실적으로 발생하면 공격으로 인식한다. 따라서 N-IDS (Network based Intrusion Detection System)에서 관리하는 위협 DB는 잠재적인 위협으로 볼 수 있으며, N-IDS에서 탐지한 위협은 네트워크에 대한 공격이 발생한 것으로 볼 수 있다. 위협은 네트워크에 미치는 영향에 따라 다음과 같은 속성을 갖는 요소들로 분류할 수 있다.

- 전체 위협(T1): 알려진 전체 위협으로 N-IDS의 DB로 관리된다.
- 탐지 위협(T2): 대상 네트워크의 N-IDS에서 탐지한 모든 공격 코드를 의미한다.
- 잠재 취약점 상관 위협(T3): N-IDS에서 탐지한 공격 코드 중 네트워크에 존재하는 자산의 잠재취약점과 상관성이 있는 공격코드이며, 이러한 위협이 대량 발생할 경우 자산의 가용성 저하를 일으킬 수 있다.
- 잔류 취약점 상관 위협(T4): N-IDS에서 탐지한 공격 코드 중 자산의 잔류 취약점과 직접적인 상관성 있는 공격코드이며, 보안담당자의 즉각적인 대응이 필요한 위협이다.

1) 네트워크가 제공하는 기본적인 서비스인 정보 유통 기능을 제공하는 전송 장비와 정보처리 기능을 제공하는 네트워크상의 각종 시스템으로 정의

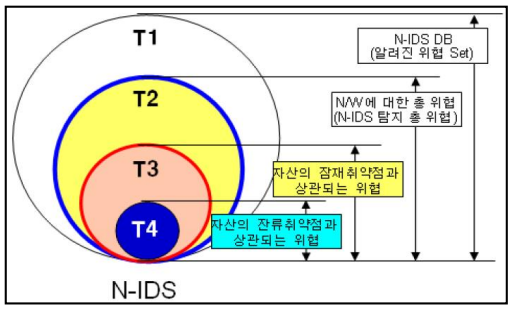

그림 5. 위협 분류 및 취약점과 상관관계
Fig 5. Threat Classification and Vulnerability Correlation

이 같은 상관관계는 그림 5와 같이 나타낼 수 있다. 잔류 취약점(V3)과 잔류 취약점 상관 위협(T4)은 자산에 직접적인 위험을 발생시킬 수 있는 원인으로 작용한다. 이들 각각의 정보를 개별적으로 산출하는 N-IDS와 VAS 시스템을 실시간 연동하면, 네트워크 취약수준의 변화를 관찰할 수 있고 N-IDS의 불필요한 경보를 대폭 줄여 탐지 정확도를 향상시킬 수 있다.

일반적으로 특정한 취약점에 대해 다수의 위협이 상관되며, 취약점과 위협의 상관관계는 그림 6과 같이 나타낼 수 있다. R1은 자산의 잔류 취약점(V3)에 대한 공격으로 실질적인 위험을 발생 시킨다. R2는 자산의 잠재 취약점(V2)에 대한 공격으로 자산에 잠재적인 위험이 된다. R3은 자산에 대한 간접 공격으로서 자산의 가용성을 저하시키는 위험으로 작용한다[6].

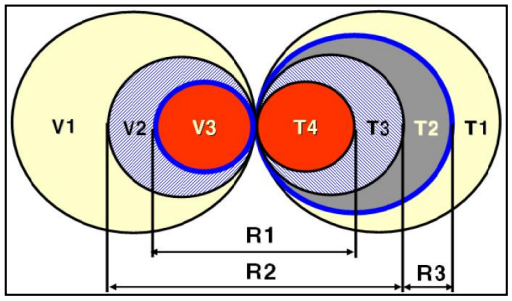

그림 6. 취약점과 위협의 상관관계
Fig 6. Correlation of Vulnerability and Threat

자산에 내재한 취약점의 존재는 잠재적인 위협을 현실화시킬 수 있는 역할을 하며, 취약점을 제거하면 취약점을 이용한 대부분의 위협은 자산에 실질적인 손실을 줄 수 없다. 이 같은 자산, 취약점 및 위협의 상관성을 이용하여 N-IDS에서 탐지한 전체 경보 중 자산 및 자산의 취약점과 직접적인 상관성에 따라 분류함으로써 불필요한 경보를 대폭 줄이고, 네트워크 보안 관리자가 직접적으로 대응할 필요가 있는 경보만 제공할 수 있다.

본 논문에서는 자산, 취약점 및 위협의 상관관계 분석을 통해 자산에 발생할 수 있는 위험을 3가지로 분류한다.

- R1(실현 위험) : 잔류 취약점에 대한 공격
- R2(잠재 위험) : 잠재 취약점에 대한 공격
- R3(가용성 잠재 위험) : 취약점과 상관성이 없는 자산에 대한 가용성 저하 공격

R1은 자산의 잔류 취약점에 대한 공격으로 실질적이고 직접적인 위험을 발생시킬 수 있는 원인으로 작용하며, R2는 잠재 취약점에 대한 공격으로 자산의 잠재적인 위험으로 작용하고, R3는 자산에 대한 간접 공격으로 자산의 가용성을 저하시키는 위험으로 작용한다.

이러한 위험의 분류를 기반으로 불필요한 보안 정보 공유를 줄이고, 직접적으로 대응할 수 있는 정보만 도메인 간에 제공하여 효율적인 협력 대응 프레임워크 설계가 가능하다.

취약점 분석 시스템(VAS)에서의 보안 정보 예는 시스템 OS, 시스템 IP, 취약점 Port, 취약점 Protocol, 취약점 ID, Common Vulnerability Exposure, 위험도 등이 있으며, 네트워크 침입탐지 시스템(N-IDS)에서의 보안 정보 예는 공격시작시간, 공격자 IP, 공격자 Port, 대상자 IP, 대상자 Port, 공격 ID, 공격 탐지/종료 시간, 프로토콜, 위험도 등을 들 수 있다.

3.2 협력 대응 프레임워크 기능

가. 경보관리 기능

도메인 내의 보안 경보를 수집, 가공하여 DB로 구축한다.

나. 보안 상황 분석 기능

도메인 내의 보안 상황을 실시간 모니터링한다. 보안 상황이란 보안 측면에서 평가된 네트워크 현재의 보안 상태를 의미하며, 보안 상황을 반영하기 위한 계량화된 단위를 보안 등급이라 한다. 도메인 내에서 발생하는 이벤트에 기반하여 보안 등급이 설정된다. 보안등급은 일반적으로 5단계로 구성되며, 보안 등급의 상태는 다음과

같다.

- 보안등급 4 - 안전 상태
- 보안등급 3 - 경계 상태
- 보안등급 2 - 준위험 상태
- 보안등급 1 - 위험 상태
- 보안등급 0 - 감시불가능 상태

다. 공격 연관성 분석 기능

도메인 내에서 발생하는 이벤트에 대해 도메인 간 정보공유를 통해 공격 연관성을 분석하여 전역적 차원의 공격을 탐지한다.

라. 대응 결정 분석 기능

발생한 이벤트에 대한 적절한 대응 규칙 및 대응 방안을 도출한다.

마. 블랙리스트 관리 기능

도메인 내 혹은 도메인 간 이벤트 분석을 기반으로 블랙리스트 및 공격 대상 리스트를 산출하여 관리를 수행한다.

바. 침해사고 발생 단계별 대응 기능

침해사고 발생 이전 단계에서는 유해 프로그램 분석, 객체 인증 등을 수행하고, 침해사고 발생 단계에서는 정상적인 트래픽은 유지하며, 유해 트래픽의 신속한 차단을 수행한다. 침해사고 발생 이후 단계에서는 시도된 공격의 핵심 특징을 추출하여 향후 동일한 공격이 발생하는 경우, 신속히 탐지 및 차단할 수 있는 시그니처(Signature)를 생성하고 배포한다.

3.3 협력 대응 프레임워크 구조

협력 대응 프레임워크는 보호해야 할 자산에 대한 위험 평가를 통해 위험도를 관리하며, 사전 정의된 외부로부터의 공격에 대해 즉각적인 인지와 빠른 전파, 정의되지 않은 공격에 대해서는 위험도 프로파일링을 기반으로 이상 징후 파악을 통하여 대응 가능하도록 해야 한다.

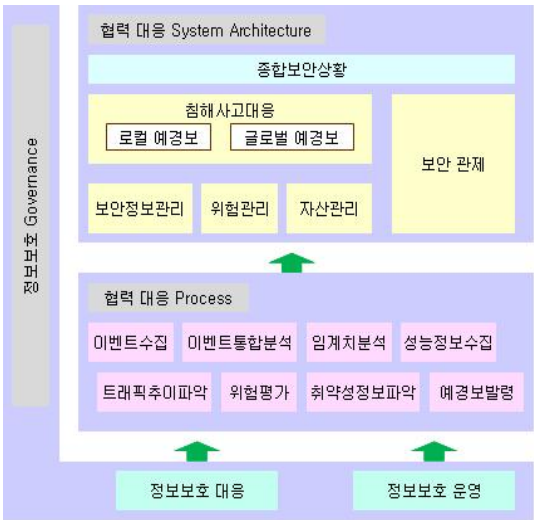

그림 7. 협력 대응 프레임워크 모델
Fig 7. Model of Collaborative Response Framework

그림 7과 같이 협력 대응 프레임워크 모델은 거버넌스 측면의 운영 기준에 따른 조직의 구성, 조직 활동의 근간이 되는 협력 대응 프로세스[2] 및 해당 프로세스를 수행하기 위한 아키텍처로 구성된다.

협력 대응 시스템 아키텍처를 정의하기 위해 국제 표준의 프레임워크를 기반으로 보안 정보 공유 및 협력 대응을 위한 단위 프로세스를 도출한다. 도출된 프로세스는 시스템 계층으로 구분하여 기능 정의를 위해 시스템 내에서 구현된다. 도출된 단위 프로세스를 통하여, 주요 단위 기능을 도출하고 그에 따른 세부 기능 정의 후 유사 기능을 그룹화하여 하나의 단위 시스템 요건으로 구분한다.

시스템 아키텍처의 구성 요소는 다음과 같다.

- 종합보안상황
  - · 보안상황 모니터링
- 자산관리/위험관리
  - · 관제대상 인프라 관리
  - · 위협/취약점 관리
  - · 위험 관리
- 침해사고 대응
  - · 로컬 실시간 예경보
  - · 글로벌 실시간 예경보

2) 보안 위협 및 협력 대응에 대한 업무 절차 관련 사항

- 보안 정보 관리
  · 트래픽 정보 관리
  · 이벤트 정보 관리
- 보안 관제

Ⅳ. 협력 대응 프레임워크에서 보안 정보 공유 기반 네트워크 위험도 산출

3.1 절에서 제안한 자산 취약점-위협 상관 분석은 개별 자산에 실질적으로 피해를 줄 수 있는 위협을 판단할 수 있지만, 전체 네트워크 대상의 위협을 탐지하기에는 적합하지 못하다. 본 논문에서는 네트워크 전체적인 위협 중에서 실제 네트워크 내부 자산에 영향을 주는 위협의 비율을 통해 위험도를 산정하고, 위험도가 특정 임계치에 도달하는 경우 경보를 생성하는 방식을 제안한다. 이 임계치는 네트워크 트래픽/위협/취약점 현황과 위험 관리 정책에 따라 결정된다[7][8].

제안하는 네트워크 위험도 산출 방식은 다음과 같다. 전체 자산의 수를 *Total_Asset*이라 하고, *i*번째 자산의 가치를 AV_i라 하며, *i*번째 자산에 대한 N-IDS 로그들 중 *j*번째 로그의 위험도를 $T_i[j]$라 한다. *i*번째 자산에 대한 N-IDS 로그 전체의 인덱스 집합을 F_i라 하고, VAS 로그와의 상관 분석을 통해 실제 취약점과 연관이 있다고 파악된 로그들의 인덱스 집합을 B_i라고 한다.

예를 들어, 2번째 자산으로 향하는 N-IDS 로그가 10개 있고, 그 중에서 8번째와 10번째 로그가 실제 취약점과 연관이 있다면 B_2={8,10}이 된다. 이 때 네트워크 위험도(R_N)을 계산하기 위한 식은 다음과 같다.

$$R_N = \frac{\sum_{i=1}^{TotalAsset}\left(\frac{\sum_{k\in B_i} T_i[k]}{\sum_{j\in F_i} T_i[j]} \times AV_i\right)}{\sum_{i=1}^{TotalAsset} AV_i}(\%) \quad (1)$$

식 (1)에서 $\sum_{j\in F_i} T_i[j]$는 i번째 자산으로 향하는 모든 위협의 위험도의 합을 의미한다. 이 값은 현재 i 번째 자산이 받고 있는 위협의 전체 크기를 정량화한 것이다.

$\sum_{k\in B_i} T_i[k]$는 *i*번째 자산으로 향하는 모든 위협 중 실제 *i*번째 자산에 영향을 줄 수 있는 위협의 위험도 합을 의미한다. 실제 위협을 줄 수 있는지의 여부를 판단하는 기준은 N-IDS 로그와 VAS 로그와의 상관관계 분석을 이용한다.

$\frac{\sum_{k\in B_i} T_i[k]}{\sum_{j\in F_i} T_i[j]}$는 *i*번째 자산으로 들어오는 전체 위협 중에서 *i*번째 자산에 영향을 줄 수 있는 위협의 비율이다.

$\frac{\sum_{k\in B_i} T_i[k]}{\sum_{j\in F_i} T_i[j]} \times AV_i$는 $\frac{\sum_{k\in B_i} T_i[k]}{\sum_{j\in F_i} T_i[j]}$에 *i*번째 자산의 가치를 곱한 값으로 자산의 가치에 따라 위험의 크기를 다르게 하는 역할을 한다.

이 값을 모든 자산에 대하여 더한 뒤, $\sum_{i=1}^{TotalAsset} AV_i$,즉 전체 자산 가치의 합으로 나누면 자산의 가치를 반영한 네트워크 위험도를 얻을 수 있다.

이러한 정량화된 네트워크 위험도를 기반으로 관리 대상 네트워크 위험 상황을 신속하게 탐지하여 보안 정책에 따라 실시간적인 행동을 수행할 수 있도록 하는 것이 가능하다.

Ⅴ. 결 론

본 논문에서는 인터넷 환경에서 복합적이고 급속도로 증가하고 있는 다양한 사이버 공격에 관한 보안 정보들을 공유하고 체계적으로 신속하게 대응하기 위한 협력 대응 프레임워크 모델을 제시하였고, 이를 기반으로 협력 대응 프레임워크에서의 보안 정보 공유를 기반으로 한 네트워크 위험도 산출 알고리즘을 제시하였다. 이를 통하여 효율적인 대응 체계를 갖추기 위한 기술 개발이 가능하며, 국가 간의 공조체계를 확고히 하고, 향후 발생하는 사이버 공격을 사전에 신속하게 대응할 수 있다. 보안 정보 공유를 기반으로 하는 협력 대응 프레임워크의 개발은 국가, 기관, 기업, 개인 등의 피해를 최소화하는 데 기여할 수 있을 것으로 기대된다.

참고문헌

[1] 정일안, 김익균, 오진태, 장종수, “Zero-day 공격 대응을 위한 네트워크 보안의 지능화 기술,” 한국통신학회지, 제24권, 제11호, 2007. 11.
[2] ITU-T X.sisfreq, Requirements for security information sharing framework, 2008.
[3] 정일옥, “확장된 증거수집 및 사건연관분석을 기반으로 한 컴퓨터 포렌식”, 2008 한국컴퓨터종합학술대회 논문집, 제35권, 제1호, 2008. 6.
[4] 정일안, 오진태. 장종수, “보안 정보 공유 기술 및 표준화 동향” 전자통신동향분석, 제23권, 제4호, 2008. 8.
[5] 호건, 최진기, 강유, 이명수, “취약점과 위협의 상관성 분석을 통한 네트워크 위험 조기경보 시스템 설계”, 정보보호학회지, 제15권, 제1호, 2005. 2.
[6] 이기혁, 이철규, “사이버 환경에서의 침해사고 대응을 위한 위험도 산정 및 실시간 경보 생성에 대한 연구”, 정보보호학회지, 제18권, 제5호, 2008. 10.
[7] 조호대, 신동일, “공공 및 민간부문의 사이버 침해사고 현황분석에 따른 대응방안”, 한국콘텐츠학회논문지, 제9권, 제1호, 2009. 1.
[8] 김영진, 이수연, 권헌영, 임종인, “국가 전산망 보안관제 업무의 효율적 수행방안에 관한 연구”, 정보보호학회논문지, 제19권, 제1호, 2009. 2.

이영석(Young-seok Lee)

1992년 충남대학교 컴퓨터공학과 공학사
1994년 충남대학교 컴퓨터공학과 공학석사
2002년 충남대학교 컴퓨터공학과 공학박사
1994년~1997년 LG전자정보통신연구소 연구원
2002년~2004년 한국전자통신연구원 선임연구원
2004년~현재 군산대학교 정보통신공학과 부교수
※관심분야 : 정보보호, 이동컴퓨팅, 컴퓨터네트워크

안개일(Gae-Il An)

1993년 충남대학교 컴퓨터공학과 공학사
1995년 충남대학교 컴퓨터공학과 공학석사
2001년 충남대학교 컴퓨터공학과 공학박사
2006년~2007년 미국 시라큐스대학교 포닥연구원
2001년~현재 한국전자통신연구원 선임연구원
※관심분야 : 정보보호, 컴퓨터네트워크, 모바일보안

김종현(Jong-Hyun Kim)

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