보안 정보 공유 기술 및 표준화 동향

Technology and Standardization Trend of Security Information Sharing

21세기를 대비하는 정보보호 특집

정일안 (I.A. Cheong) 보안게이트웨이연구팀 연구원
오진태 (J.T. Oh) 보안게이트웨이연구팀 선임연구원
장종수 (J.S. Jang) 보안게이트웨이연구팀 책임연구원

목 차

보안 정보란 알려지거나 알려지지 않은 공격, 위협, 취약성, 침입, 악성 행위 등과 관련된 정보들을 총칭하는 것으로, 정부, 금융, ISP, 기업 등 공공의 인터넷 환경에서 다양한 보안 정보들을 상호 공유하고 관리하여 사이버 보안 위협들에 대해 빠르게 대응하기 위한 체계가 필요하게 되었다. 이러한 보안 정보들을 상호 공유하기 위한 기술과 그 표준에 대한 필요성이 대두되어 국내외에서 관련 표준화 활동이 추진되고 있다. 본 고에서는 이와 같은 보안 정보를 공유하기 위한 기술과 관련 표준화 동향에 대하여 살펴본다.

I. 서론

통신 및 네트워크 기술의 발달과 함께 스팸, 바이러스, 서비스 거부 공격, 웜 등 네트워크를 통한 사이버 공격은 다양한 기법이 사용되고 있고, 전파속도가 단축되면서 더욱 치명적인 형태로 진화하고 있다. 지난 2003년에 발생한 1.25 대란으로 잘 알려진 MS-SQL 서버의 취약점을 악용한 Slammer 웜은 사고 발생 10분만에 전 세계 90%의 취약성을 가진 호스트를 감염시켰고, 약 5일간의 생산성 피해가 약 10억 달러에 이르는 경제적 손실을 초래한 것으로 추정하고 있다. 국내의 경우에는 세계적인 수준의 인터넷 인프라를 구축하고 있고, 공격에 대한 피해 역시 전체의 10% 이상을 차지하고 있다. 최근 네트워크 환경을 위협하는 사이버 공격들은 봇넷, 스팸, 메신저, 전자메일 등을 이용하는 것과 같이 그 형태가 매우 다양해지고 있으며, Bagle, MyTob, Sober, MS의 WMF, 오피스, Oracle, Adobe Flash, 웹 애플리케이션 취약점, J2ME, 모바일 디바이스용 악성코드 등 신종 및 변종 웜의 출현이 지속적으로 보고되고 있다. 이와 같은 다양한 사이버 공격 및 위협에 대해서 기존 방화벽, 침입탐지 및 대응 시스템 같은 보안 기술들이 적용되어 왔으나, 취약성을 공격하는 exploit 코드 발생 시간에 비해 해당 취약성 공격에 대한 탐지 시그니처의 생성 및 배포와 적용 시간이 길어짐에 따라 제로데이 공격 위험에 노출될 가능성이 점점 더 높아지고 있다. 이러한 기술들의 한계와 국내외 차세대 보안 대응 기술에 대한 보안 시장의 요구와 함께 Autograph, Polygraph, Earlybird, ZASMIN 등 실시간으로 시그니처를 생성하여 대응하기 위한 기술들의 개발이 진행되고 있다[1]-[3]. 또한 일반 기업을 중심으로 이종간의 보안 시스템에 대한 통합적인 관리를 통해서 효율적이고 체계적인 보안 정책을 수립하고 일관성 있게 적용하여 대응할 수 있는 대규모 전산망 보안 체계의 구축 및 관리를 위한 기술과 확장 기술에 대한 개발 노력이 진행되어 왔다[4],[5].

국내외에서는 각각 현재 발생하는 바이러스, 웜뿐만 아니라 신종 또는 변형 위협들에 관한 보안 정보를 공유하고 신속하게 대응하기 위한 체계를 갖추어 왔다. 그러나 정부 기관, 금융, 기업, ISP 등 공공의 인터넷 환경에서 다양한 보안 정보를 효율적으로 관리하는 데 절차, 소요 비용, 정책 적용, 사고 대응 및 협력의 한계 등 많은 문제를 안고 있다. 보통 보안 관리자들은 인터넷에 널리 퍼져 있는 많은 토론 포럼들을 통해 취약점, 바이러스, 웜, 악성 봇넷 등의 보안 정보들을 접하고 있지만, 이러한 사이버 공격들은 매우 빠르게 수초 내에 전 네트워크에 퍼질 수 있기 때문에 통상적인 방법으로는 악성 행위가 전파되고 엄청난 재정적 피해를 감당할 수 없게 된다. 이러한 전사적인 대응의 어려움을 극복하기 위해 국내에서는 국가사이버안전센터, 정부 보안정보 공유분석센터, 인터넷침해사고대응지원센터 등을 통해 네트워크와 시스템의 안전에 대한 근본적인 대책을 수립하게 되었고, 국외에서는 미국의 CERT/CC, MITRE, CVE/CWE, OSVDB 등의 오픈 프로젝트, 유럽 회원국들의 ENISA를 통해 사이버 공격, 취약성, 위협 등에 대한 정보를 공유하는 체계를 구축해 가고 있다. 이와 같이 네트워크 기반 기술의 발전과 함께 국내외 공공 인터넷 환경에서 다양한 보안 정보들을 상호 공유하고 관리하여 사이버 보안 위협들에 대해 빠르게 대응하기 위한 전 세계적인 공유 체계가 더욱 필요하게 되었다. 또한, 이러한 보안 정보들을 상호 공유하기 위한 기술의 표준에 대한 필요성이 대두되어 국내외에서 관련 표준화 활동이 추진되고 있다. 본 고에서는 이와 같은 보안 정보를 공유하기 위한 기술과 관련 표준화 동향에 대하여 살펴본다.

II. 보안 정보 공유 기술

최근의 보안 정보 공유는 전세계 인터넷의 오픈

● 용 어 해 설 ●

보안 정보: 알려지거나 알려지지 않은 공격, 위협, 취약성, 침입, 악성 행위 등과 관련된 정보들을 총칭한다.

프로젝트나 아시아, 미국, 유럽 등의 세계 지역별 움직임으로 진행되고 있고, 점차 지역별 상호 공조 체계를 구축해 나가고 있는 추세로 발전하고 있다. 본장에서는 이러한 보안 정보 공유의 진행 현황들과 관련 기술을 살펴본다.

1. 국내의 보안 정보 공유

지난 2003년 1.25 인터넷 침해사고는 국내 정보통신망의 보호체계를 강화하게 되는 계기가 되었다. 침해 사고의 대응에 대한 문제점과 함께 사고 발생 시 신고절차 및 관련 기관들의 공동 대응 체계 미흡, 계층별 보호 체계 미흡, 침해사고 대응 관련 전담 조직 부재, 법·제도 미흡 등 전반적으로 많은 문제점을 인식하게 되었다. 그 이후 현재는 웜·바이러스뿐만 아니라 변종 및 신종 위협 요소들에 대한 분석과 신속한 대응 기법의 개발 등 사전 예방 기술의 개발 및 활동이 강화되었다.

국가사이버안전센터(NCSC)에서는 인터넷 침해사고에 대한 사이버 공격 감시, 사이버 안전 예방 활동, 국가 사이버 위협 정보 종합 수집 및 분석, 침해사고 긴급대응, 조사 및 복구, 국내외 사이버위협 정보 공유 및 공조 대응 등의 종합보안서비스를 제공하고 있다[6]. 정부 보안정보공유분석센터(GISAC)는 주요 정보시스템과 전자정부통합망을 사이버 위협으로부터 안전하게 보호하기 위해 마련되었고, 통합망 내·외부를 감시함으로써 침해 및 유출 등의 사이버 공격에 대응한다. 그리고 국가사이버안전센터에 로그정보 제공 및 공동 대응을 지원하고, 전자정부통합망으로 연결된 정부기관들이 서로 보안관련 정보를 공유할 수 있도록 하는 활동을 하고 있다[7]. 국방정보전 대응센터에서는 국방전산망에 대한 침해정보 탐지 및 분석, 각급 부대 CERT에 대한 조정 통제, 예방 및 조사활동, 원격 및 현장의 피해복구 지원, 국내외 정보전 관련 정보분석 등을 담당하고 있고, 국가사이버안전센터와 연동하여 군 인터넷 환경을 대상으로 보안관제 업무를 지원하고 있다[8]. 인터넷침해사고대응지원센터(KISC)에서는 상시 모니터링 체계를 갖추어 주요 ISP를 비롯한 국내 관련 기업들로부터 트래픽량, 공격 정보 등 이상징후를 탐지하는 역할을 담당하고 있다. 또한, 국내외에서 발생하는 각종 취약점, 웜·바이러스 정보 등 인터넷 환경 위협에 대한 종합적인 정보를 수집하고, 국내 주요 ISP 및 보안 업체들과 협력관계를 강화하여 침해사고 예방을 위한 활동을 하고 있다. 이러한 국내 활동뿐만 아니라, 해외 유관기관과의 공조체계를 강화하기 위해 국제침해사고대응팀협의회(FIRST)의 활동과 APCERT와 함께 국제간 침해사고 대응 모의훈련을 통해 국내 인터넷 환경의 안정화에 노력하고 있다. 그리고 침해사고 대응체계를 구축하기 위한 기술적 대응뿐만 아니라 관련 법률을 정비해 사전 예방적 수단 및 사후 대응을 위한 제도적 기반을 마련하는 것도 필요하여 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 정보통신기반보호법 등 정보보호 관련 법과 제도를 강화하고 사고예방을 위한 신속한 대응과 주관부처를 명확히 하였다[9].

사이버 공격 정보를 공유하기 위해서 현재는 침입 차단 및 탐지/대응 시스템 등에 사용하는 보안 전문가의 분석정보를 대상으로 개별 시스템보다는 통합보안관제 시스템을 이용하고 있다. 그러나 복합적이고 다양한 형태의 변형, 신규 위협 및 공격들이 자동으로 전파되어 급속도로 발생하고 있는 추세에서는 보안 전문가의 분석에만 의존하여 보안 정보를 공유하고 대응하기에는 많은 어려움을 가지고 있는 실정이다. 이러한 문제점들을 극복하기 위한 노력으로 국내외에서는 보안 전문가가 신속하게 분석할 수 있도록 도움을 주거나 실시간으로 사이버 공격 정보를 자동으로 생성하는 기술의 개발과 연구가 진행되고 있다. 사례로, 최근에 발표된 한국전자통신연구원의 ZASMIN 프로젝트의 경우 제로데이 공격에 대응하기 위하여 하드웨어 기반의 고성능 시그니처 자동생성 기술을 연구·개발하고 있다. 또한, 생성된 시그니처를 기존 보안 제품 등에 자동으로 분배하거나 관리하여 상호 공유하기 위한 기술도 연구되고 있다[3].

2. 국외의 보안 정보 공유

미국은 사이버 보안 정보 공유 프로젝트(CSISP)를 추진하여 정부와 민간부문의 정보공유 모델을 연구하고 있다. 기존 CERT-CC로 침해사고 및 취약점 정보의 신고는 웹 사이트나 전화로 신고한 후, 그 결과를 회신하게 되어 긴급한 상황에서는 대응이 지연되는 단점이 있었다. 그래서 이 프로젝트 참여자들은 ArcSight의 보안사고 관리 소프트웨어를 설치하면, 보안 정보 수집원으로 활용되어 공격과 관련된 보안 정보를 수집할 수 있게 되었다. 또한, 인터넷과 분리된 사이버경보정보망(CWIN)을 구축해 정부와 민간 전문가들의 정보공유가 가능하도록 하였다. 국토안보부에서는 이와 별도로 사이버보안 모니터링 프로젝트를 계획하여 대규모 웜·바이러스 등의 사이버 공격의 돌발적 발생 및 급증을 실시간으로 분석하는 시스템을 구축하여 실시간 사이버상태 인지 시스템으로 보안사고 데이터를 즉각적으로 분석할 수 있도록 하였다[10].

미국 연방 정부가 출연해 설립한 비영리 업체인 MITRE에서는 미 국방부, 연방, 항공국, 국세청 등의 보안 관련 정보를 연구 및 개발하고 있다. 1999년 비영리 기술자모임인 MITRE와 15개의 보안 관련 기관이 주도해 운영하는 CVE 데이터베이스가 있다. CVE는 Microsoft, IBM, Computer Associates, Novell 등 200여 개 회사와 단체로부터 자료를 제공 받아 보안 위협정보를 정리해 제공한다. 정보의 안전한 유통을 위한 정보보호에 필요한 시책을 효율적으로 추진하기 위하여 만들어졌고, 정보시스템 침해사고 처리 및 대응체계 운영을 하고 정보보호에 관련된 표준을 정하고 그와 관련된 기술을 연구하고 있다. 또한, CWE는 버퍼 오버플로, 서식 지정 문자열 에러 등 소프트웨어 취약성의 정식 목록을 작성하기 위한 것으로, 현재 사용되고 있는 소프트웨어 취약성의 용어가 많은 기업이나 보안 기업마다 각각 달라 이 목록을 용어 통일에 활용하여 보안 정보를 공유하는 데 도움을 줄 수 있게 된다[11]. OSVDB는 보안 전문가들 자원 그룹이 소프트웨어에서의 보안 결함 정보를 정리한 무료 데이터베이스로서, 기업이나 개인들 간의 협력을 통해 보안 정보를 공유하고 결함에 대한 데이터베이스의 작업과 비용을 줄이는 역할을 담당한다[12].

유럽 연합의 ENISA에서는 유럽 조기경보 시스템(EWIS)을 구축하여 각 회원국가의 국가 정보보호 조직, 침해사고대응팀, 정보공유 및 분석센터, 기업의 정보보호 조직, 통신사업자, 개인 이용자 등을 연결하는 작업 등을 수행하고 있다. 조기경보체계를 구성함에 있어 수많은 정부, 기업, 민간, 공공 등에 개별적으로 CERT를 만들고, 정보보호 인력을 양성해 배치하는 데 한계가 있어서, 분야별로 대표 CERT 또는 ISAC을 구축해 많은 센터를 효율적으로 운영하고, 사이버테러에 대응하기 위해 중요 정보통신기반 구조별로 CERT 및 ISAC을 육성하였다. 향후에는 북미나 아시아의 정보보호 조직과의 연결도 추진할 계획에 있다[10],[13].

일본에서는 2007년부터 3단계의 IRISS 프로젝트를 추진하고 있다. 이는 WorldMap View 프로젝트로써 전 세계에 설치된 다중 센서들을 통해 보안 정보를 수집하고 연관성을 분석하여 사이버 공격에 관한 대규모 정보를 제공하는 것이 목적이다. 이 시스템은 조기 탐지 및 알려지지 않은 공격 분석, 지역 또는 광역 사고의 탐지, 대규모 사이버 공격의 예측, 인터넷 위험 상황의 실시간 및 시각적 인식, 악의적인 호스트 목록 작성 등의 기능을 수행하여 기관, 기업 등의 회원사들과 보안 정보를 공유한다[14].

호주는 미국의 도움으로 기존의 CERT를 중요 정보통신 기반구조와 전자정부 상위위원회를 조직하고 정부기관과 공공기관, ISAC, CERT간 정보를 공유하는 정책을 택하고 있다. 여기에 조기경보 시스템에 활용할 신뢰정보 공유 네트워크를 구축해 각 기관에 공유할 대상정보와 협력관계 그리고 기술적인 구조를 구현하고 있다[10].

국외의 시그니처 생성 기술 연구 및 개발에 관한 사례로, Autograph, Polygraph, Earlybird, First Light Signatures Service 등이 있고, 특히 First

Light Signatures Service에서 제공하고 있는 12,000개가 넘는 시그니처들은 알려진 확실한 위협들을 폭넓게 포괄하고 있다. 주요 포괄 영역은 Client-side 공격, Server-side 공격, Expolit Components, Malware, Web Application 공격, 프로토콜 및 정책 등이다[15].

3. 보안 정보 공유의 협력 및 대응

인터넷 환경의 보안위협에 대해 효과적으로 대응하기 위해서는 사이버 환경을 구성하는 요소들과 각 요소들이 주로 작용하는 계층으로 분류한다. 계층별 특성에 따라 각각 글로벌, 국가, 민간, 개인 등 계층적으로 방어체계를 구축하는 것이 바람직하다. 즉 침해사고 발생시 각각의 계층에 따라 적절한 방어체계를 구축함으로써 전체적인 안전성을 확보하는 것이다. 인터넷 환경의 특성상 사이버 공격은 국내외 사고의 분류가 명확하지 않고, 인접 국가에서 발생하는 사이버 공격은 국내에도 즉시 영향을 미치게 되므로 이러한 공격에 대한 조기대응을 위해서는 국가간 상시 정보 공유가 필요하다. 따라서, 신속한 침해사고 공동대응을 위하여 국가 CERT간 협력체계 구축은 필요하여 한국 KrCERT는 중국 CNCERT, 일본 JPCERT와 전용망을 이용하여 네트워크 공동감시 체계를 구축하고 한·중·일 3국간의 협력체계를 시범적으로 운영하고 있다[16].

2008년 4월, 제7차 APEC 정보통신장관회의에서 미국, 중국, 일본, 호주 등을 포함한 APEC 회원국들이 정보 네트워크에서의 프라이버시 및 보안에 대해 소비자의 신뢰와 확신이 선행되어야 한다는 공통된 인식에서, 향후 안전한 사이버 환경 조성을 위해 회원국 간의 국제협력 강화를 발전시킬 수 있는 계기를 마련하게 되었다. 이와 같이 인터넷 확산과 더불어 복합적이고 지능적으로 발전하고 있는 사이버 공격에 대해서 국제 사회가 효과적으로 대응할 수 있도록 정보보호 분야에 대한 회원국의 심층적인 협력을 통해 실질적인 공동 대응방안을 마련해 가고 있다[17].

Ⅲ. 보안 정보 공유 표준화 동향

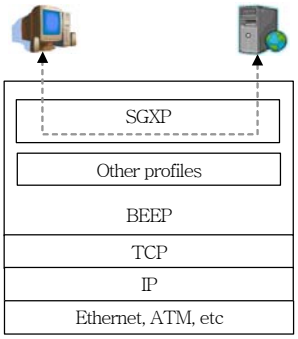
앞 절에서 살펴본 바와 같이, 최근 국내뿐만 아니라 전세계적으로 보안 정보를 공유하기 위한 활동, 기술의 연구 및 개발과 함께 관련 표준화 활동도 진행되고 있다. 본 장에서는 보안 정보 공유와 관련된 표준화 진행 현황을 살펴본다.

1. 국내 표준화 동향

가. 시그니처 교환 프로토콜

한국정보통신기술협회의 TTAS.KO-12.0061 '네트워크 공격의 시그니처 교환 프로토콜' 권고 표준에서는 네트워크 환경을 위협하는 공격에 대해 그 특징을 검출하여 생성한 시그니처 정보들을 안전하게 교환하기 위한 프로토콜(SGXP)을 규정하고 있다. 이러한 공격의 특징 패턴을 정의하고 있는 시그니처 정보는 보안 솔루션의 성능을 좌우하는 요소이며, 외부에 노출될 경우 시스템에 미치는 영향이 크기 때문에 보안이 어떤 기능보다 중요시 되어야 한다. 따라서, 이 프로토콜에서는 높은 보안성을 제공하는 BEEP 프레임워크를 기반으로 하여 시그니처 교환 프로토콜을 정의하고 있다[18].

(그림 1)은 IETF에서 표준화된 블록 확장 교환 프로토콜인 BEEP 상에서 SGXP를 이용하여 통신하는 것이다. SGXP는 시그니처 생성 시스템들과 보안 솔루션들간의 시그니처 정보를 교환하기 위한 BEEP 프레임워크 기반의 응용 계층 프로토콜이다.



(그림 1) BEEP 프레임워크 기반 SGXP

이 프로토콜은 BEEP 세션을 설정하고 그 세션상에서 데이터 교환을 위한 SGXP 채널을 설정하는 절차 및 데이터 형태를 XML 스키마로 정의한다. SGXP의 흐름은 크게 세션 연결, 상호 협상 및 인증, 시그니처 메시지 교환 과정으로 분류한다. 여기서, 시그니처 메시지 교환을 위해 공격 시그니처 정보를 표준 데이터 형식으로 정의한 SGMEF를 사용한다.

나. 시그니처 교환 프레임워크

한국정보통신기술협회의 사이버보안 프로젝트그룹(PG503)에서는 2007년부터 '네트워크 공격 시그니처의 관리 프레임워크'에 관한 표준 초안을 작성하고 있다. 주요 내용으로, 웜·바이러스 등 네트워크 환경을 위협하는 공격들에 대해 그 피해를 최소화하고 빠르게 대응하기 위해서 여러 시그니처 생성 시스템들로부터 생성된 시그니처들을 수집하고 관리하여 타 보안 솔루션으로 안전하게 전송하기 위한 운영 체계가 필요하게 되었다. 네트워크 공격 시그니처들을 수집하고 관리하여 타 보안 솔루션으로 안전하게 전송하기 위한 프레임워크를 제시하는 것이 목적이다. 또한, 이 표준 초안에서는 앞서 살펴본 시그니처 교환 프로토콜을 사용하여 생성된 시그니처 정보를 교환한다[19].

2. 국외 표준화 동향

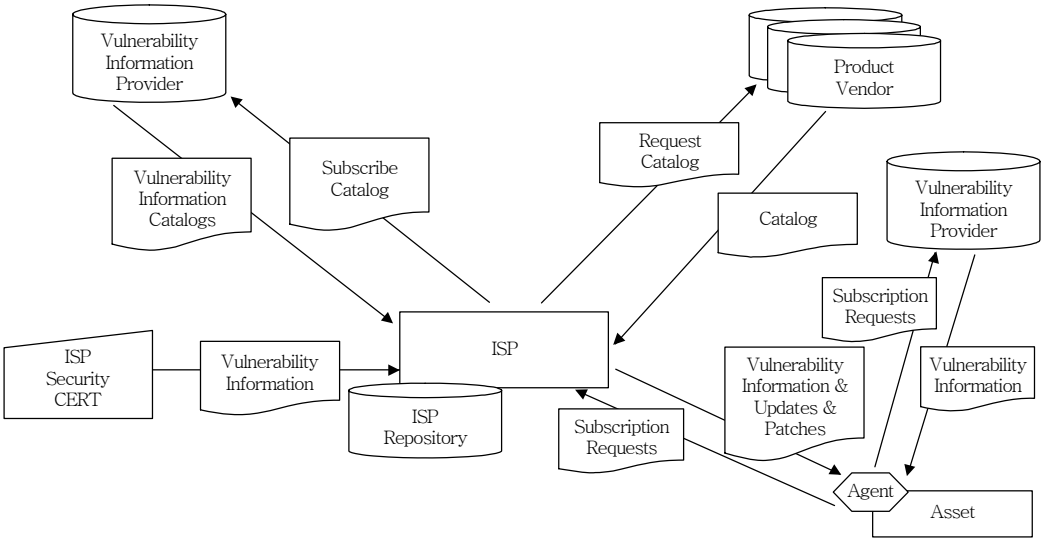
가. 취약점, 패치 정보 업데이트를 위한 벤더 중립적 프레임워크

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[20].

(그림 2)는 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.

나. 보안 정보 공유를 위한 프레임워크

ITU-T의 X.sisfreq 표준 초안은 시스템의 취약점, 공격, 악의적인 행위 정보 등에 관한 보안 정보들을 공유하기 위한 프레임워크의 요구사항을 규정하는 것이다. 보안 정보 공유 기술을 상용화시 상호 호환성을 보장하기 위한 프레임워크를 정의하기 위



(그림 2) 애플리케이션 구조의 예

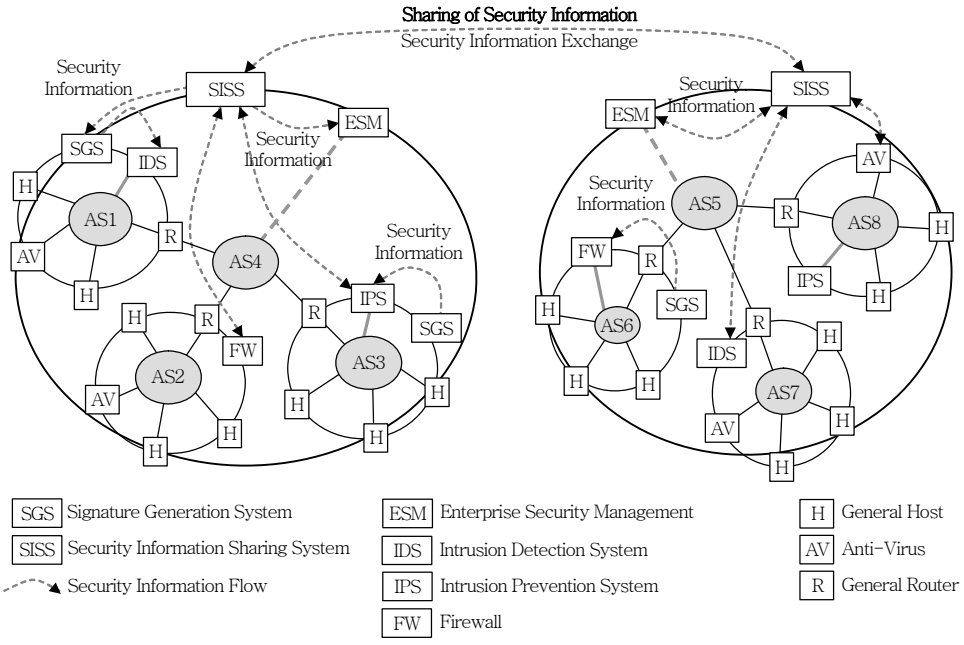
해 활용될 것이다. 현재 사이버보안 정보공유를 위한 보안분야에서 논의되기 시작한 드래프트 단계의 표준 초안으로 일본과 한국이 공동 에디터로 활동하여 작성하고 있다[21].

(그림 3)은 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. 다음은 이 프레임워크를 활용하기 위한 여러 가지 연구 사례를 설명한 것이다.

- 사례1: ISP A와 ISP B는 서로 다른 네트워크로의 공격을 막기 위해 보안 사고와 사건 관련정보를 공유하기로 동의한다.
- 사례2: ISP A, ISP B, ISP C는 보안 정보를 공유하지만, 각 ISP는 그 정보를 전파하거나 접근할 수 있는 고유하고 합법적인 요구사항이 있다.
- 사례3: ISP A와 ISP B는 각각 다른 나라에서 잠재적인 프라이버시와 관련한 데이터를 전파하고 접근하는 고유하고 합법적인 요구사항이 있다.
- 사례4: CERT는 네트워크를 통한 새로운 위협을 발견하고 그 위협을 알리거나 분석한다.
- 사례5: 보안 자문 기업은 서비스 제공에 따라 다른 수준의 정보를 제공한다.
- 사례6: ISP A는 보안 관련 정보 패킷을 받고 협동자인 ISP B에게 그 패킷을 알려줄 필요가 있다.
- 사례7: 기업내 CERT는 다른 기관과 비즈니스 모델을 통해 보안 정보와 경보를 생성하고, 그 정보는 무료로 다운로드 할 수 있도록 전자메일 등 서비스 수준에 따라 제공한다.
- 사례8: ISP는 사용자 인터페이스를 통해 분류에 기반한 보안 관련 정보를 접근한다.
- 사례9: ISP A는 의심스러운 트래픽과 관련된 포트 또는 포트 범위 등의 정보를 ISP B에게 전달하여 특정 공격을 식별하도록 한다.
- 사례10: ISP A와 ISP B는 민감한 보안 관련 정보를 교환하기 위해서 안전한 채널을 사용한다.

이 표준 초안에서는 보안 정보 공유 프레임워크



(그림 3) 보안 정보 공유 프레임워크의 개념적 구조

를 구성하기 위한 요구사항들을 규정하고 있다. 크게 일반 요구사항과 기능 요구사항으로 나누고, 기능 요구사항은 각 구성 요소별 역할에 따라 수집, 관리, 분석, 교환, 저장, 인터페이스 요구사항으로 나눈다.

- 일반 요구사항: 벤더 중립적인 프레임워크로 구성되어야 하고, 보안 정보를 교환하는 데 가능한 위협 시도를 막아야 한다. 통신 신뢰도와 보안 연결, 접근 제어, 상호 협상 및 인증을 지원해야 한다. 또한, 보안 정보를 공유하기 위한 엔티티들간에는 다중 연결을 지원해야 하고, 안정적으로 운영되어야 한다. 모든 기능 모듈들간에는 유연하게 설계되어야 하고, 효율적으로 통합 관리되어야 한다.
- 기능 요구사항: 보안 정보의 수집, 분석, 관리, 저장, 교환 기능을 지원해야 한다. 시스템 및 감사 로그를 주기적으로 저장하고 그 정보는 관리자가 파악할 수 있도록 제공해야 한다. 기존 보안 엔티티들과 연동이 가능해야 하고, 보안 정보를 공유하는 데 모든 기능적 태스크를 지원해야 한다.
- 수집 기능 요구사항: 엔티티들 간에는 안전한 연결, 상호 협상 및 인증을 지원해야 하고 보안 정보 메시지를 공유하기 위한 교환 프로토콜을 지원해야 한다. 수집은 실시간적으로 이루어져야 하고, 관리자의 정책에 따라 수집될 수 있도록 해야 한다.
- 관리 기능 요구사항: 관리자에 의한 정책 수정, 관리, 접근제어를 지원해야 하고, 보안 상황을 시각적으로 쉽게 볼 수 있도록 하는 사용자 친화적 인터페이스를 지원해야 한다. 동작 및 보안 상태 등 시스템과 기능 모듈의 활동을 감시 및 기록하고 보고할 수 있어야 한다. 또한, 운영 시간, 기능 모듈명, 사건 메시지 등의 상태 정보를 기록하고 유지할 수 있어야 한다.
- 분석 기능 요구사항: 각 엔티티들로부터 수집된 보안 정보를 분석하는 방법과 정보를 제공해야 한다. 의심 트래픽이나 패킷의 특징에 대한 연관 및 분석 정보를 포함해야 한다. 이 분석은 정책에 의해 자동 또는 수동으로 동작되어야 하고, 분석 결과를 분류해야 한다.
- 교환 기능 요구사항: 이기종의 보안 엔티티들 간에 호환성을 제공하는 표준화된 보안 정보 메시지여야 한다. 메시지 교환 포맷은 다양한 보안 정보를 대표하는 표준화된 데이터 포맷이어야 하고, 포괄적인 표준이어야 한다. 데이터 모델링 언어와 구현은 확장성과 유연성을 고려하여 UML과 XML 스키마를 지원해야 한다. 교환 프로토콜은 안전한 프로토콜이나 널리 활용되는 응용계층 프로토콜이어야 한다.
- 저장 기능 요구사항: 저장 정보에는 위협, 공격, 취약점 같은 보안 정보를 포함하고 엔티티의 관리와 감시 정보도 포함해야 한다. 저장되어 있는 공유 보안 정보는 생성된 엔티티들을 구별할 수 있어야 하고, 관리를 위해 중복성을 검사해야 한다. 또한, 관리자에 의해 접근제어와 데이터 보안을 지원해야 하고, 보안 정책으로 데이터베이스를 관리해야 한다.
- 인터페이스 기능 요구사항: 신뢰성과 보안을 지원해야 하고, 내·외부 인터페이스와의 효율성과 가용성을 위해 발전되고 안전한 기술을 사용해야 한다. 다른 엔티티들과의 확장성을 지원해야 하고, 예외나 오류가 발생 시에도 자동적으로 복구가 가능해야 한다. 내부 인터페이스는 기능 모듈들 간의 인터페이스를 정의한 것으로, 주로 명령어와 데이터 정보를 전달하기 위해 내부 기능 모듈들간의 정보를 교환하는 데 사용된다. 반면, 외부 인터페이스는 이 프레임워크와 다른 시스템 간의 인터페이스를 정의한 것으로, 주로 시스템들 간의 정보를 교환하는 데 사용된다.

향후에 이 표준 초안이 승인되면 다음 단계로 정보 공유 프레임워크에 관한 표준화를 진행할 계획이고, 완성된 표준 권고안들은 사이버 공격에 대해 세계적 공조 체계를 갖추는 데 활용될 것이다.

Ⅳ. 결론

최근의 사이버 공격은 시스템 및 네트워크의 취약점 등을 통해 급속하게 전파되는 형태를 띠고 있다. 또한, 이러한 공격들은 상호 결합되어 그 확산 정도나 파괴력은 점점 증가하여 피해 사례와 피해 규모도 커지고 있는 추세이다. 이와 같이 가까운 시일 내에 취약점에 대한 패치가 발표되기 전에 공격이 이루어지는 제로데이 공격을 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.

본 고에서는 전세계 인터넷 환경에서 복합적이고 급속도로 증가하고 있는 다양한 사이버 공격에 관한 보안 정보들을 공유하고 체계적으로 신속하게 대응하기 위한 기술 개발 및 연구 동향과 관련 표준화 활동에 대해 살펴보았다. 이와 같이 전 세계적인 대응 체계를 갖추기 위한 기술 개발 및 표준화를 통해서 국가 간의 공조체계를 확고히 하고, 향후 발생하는 사이버 공격을 사전에 신속하게 대응하면 국가, 기관, 기업, 개인 등의 피해를 최소화하는 데 기여할 수 있을 것으로 기대된다.

약 어 정 리

APCERT	Asia-Pacific Computer Emergency Response Team
BEEP	Block Extensible Exchange Protocol
CERT	Computer Emergency Response Team
CSISP	Cyber Security Information Sharing Project
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
CWIN	Cyber Warning Information Network
ENISA	European Network and Information Security Agency
ESM	Enterprise Security Management
EWIS	European Warning and Information System
FIRST	Forum of Incident Response and Security Teams
GISAC	Government Information Sharing and Analysis Center
IRISS	Internet Risk Information Sharing System
ISAC	Information Sharing and Analysis Center
ISP	Information Service Provider
ITU-T	International Telecommunication Union - Telecommunication
KISC	Korea Internet Security Center
NCSC	National Cyber Security Center
OSVDB	Open Source Vulnerability Database
SGMEF	Signature Generation Message Exchange Format
SGXP	Signature Generation eXchange Protocol
ZASMIN	Zero-day Attack Signature Management INfrastructure

참 고 문 헌

[1] 정일안, 김익균, 오진태, 장종수, “Zero-day 공격 대응을 위한 네트워크 보안의 지능화 기술,” 한국통신학회, 2007. 9.
[2] 한국정보보호진흥원, “인터넷 침해사고 동향 분석,” 2008. 5.
[3] ZASMIN, http://www.etri.re.kr
[4] 한국소프트웨어개발연구조합, “다중보안기술을 수용하는 지능형 통합보안 관리도구,” 1999. 9.
[5] 김석훈, 손우용, 송정길, “통합보안 관리 시스템 표준에 관한 연구,” 한국인터넷정보학회, 2004. 3.
[6] 국가사이버안전센터, http://www.ncsc.go.kr
[7] 디지털타임즈, http://www.dt.co.kr
[8] 국군기무사령부, http://www.dsc.mil.kr
[9] 한국정보보호진흥원, 정보보호뉴스, 2008. 2.
[10] 보안뉴스, http://www.boannews.com
[11] MITRE, http://www.mitre.org
[12] OSVDB, http://osvdb.org
[13] ENISA, http://www.enisa.europa.eu
[14] IRISS, http://wmv-project.nicter.jp
[15] Endeavor, http://www.endeavorsecurity.com
[16] 이홍섭, “IT839 3대 인프라 보호를 위한 사이버공격 예방 및 대응체계 고도화,” 한국정보보호진흥원, 2004. 9.
[17] 한국정보보호진흥원, 정보보호뉴스, 2008. 2.
[18] TTAS.KO-12.0061, 네트워크 공격에 대한 시그니처 교환 프로토콜, 2007. 12.
[19] 한국정보통신기술협회, http://www.tta.or.kr
[20] ITU-T X.1206, A vendor-neutral framework for automatic notification of security related information and dissemination of updates, Mar. 2008.
[21] ITU-T X.sisfreq, Requirements for security information sharing framework, 2008.