KISM Smart Media Journal
Vol. 4, No. 4 pp. 80~85 ISSN:2287-1322

통합 사이버 보안 상황분석을 통한 관제 상황인지 기술

Context cognition technology through integrated cyber security context analysis

남승수*, 서창호*, 이주영**, 김종현**, 김익균**
Seung-Soo Nam*, Chang-Ho Seo*, Joo-Young Lee**, Jong-Hyun Kim**, Ik-Kyun Kim**

요 약

인터넷을 이용하는 응용의 수가 급격히 증가함에 따라 인터넷 상에서 이루어지는 사이버 공격의 발생 빈도는 점점 증가하고 있다. 전 세계적으로 L3 DDoS 공격 탐지 중비의 장비에서 응용계층 기반의 지능형 DDoS 공격에 대한 탐지가 미비하다. 차세대 네트워크 보안솔루션의 다양한 요구사항을 충족할 수 있는 고성능 유무선 네트워크 위협대응 기술에 있어서 국내제품은 외국제품에 비해 기능면에서는 근접하나 성능은 미비한 상황에 있으며, 악성코드 탐지 및 시그니쳐 생성연구 관련하여 주로 Window OS에서 동작하는 악성코드 탐지 및 분석 연구 중심으로 진행하고 있다. 본 논문에서는 최신 사이버 보안 상황 침해 공격 분석을 통한 최신 다양한 신종 공격 기법 및 분석 기술의 현황 조사, 분석등을 기술한다.

■ 중심어 : DDos, 네트워크 보안, 사이버 보호, 침입방지시스템, 데이터 중복제거 기술

Abstract

As the number of applications using the internet the rapidly increasing incidence of cyber attacks made on the internet has been increasing. In the equipment of L3 DDoS attack detection equipment in the world and incomplete detection of application layer based intelligent. Next-generation networks domestic product in high-performance wired and wireless network threat response techniques to meet the diverse requirements of the security solution is to close one performance is insufficient compared to the situation in terms of functionality foreign products, malicious code detection and signature generation research primarily related to has progressed malware detection and analysis of the research center operating in Window OS. In this paper, we describe the current status survey and analysis of the latest variety of new attack techniques and analytical skills with the latest cyber-attack analysis prejudice the security situation.

■ keywords : DDos, Network Security, Cyber Security, Intrusion Prevention System, SIR

Ⅰ. 서 론

인터넷의 급격한 확산과 인터넷을 이용하는 응용의 수가 급격히 증가함에 따라 인터넷 상에서 이루어지는 사이버 공격의 발생 빈도는 점점 증가하고 있으며, 이로 인해 입게 되는 시간적, 경제적 피해 규모는 이전과는 비교할 수 없을 정도로 커지고 있다 [1]. 미국 마이크로소프트사에서 악성 URL 자동 수집 시스템을 구축하였으나, 최근 사회 공학적 방법을 통해 유포되는 악성코드 수집에는 어려움이 있으며, 국외 대학 및 비영리 단체에서 지능화된 악성코드의 행위 분석 관련 연구를 진행하고 있다 [2, 3]. 전 세계적으로 L3 DDoS 공격 탐지 중비의 장비에서 응용계층 기반의 지능형 DDoS 공격에 대한 탐지 미비하며, 시스코, 아버네트웍스, 라드웨어 등

* 공주대학교 융합과학과 ** 한국전자통신연구원
본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신 · 방송 연구개발사업의 일환으로 수행하였음. [14-824-06-001, 사이버 공격의 사전 사후 대응을 위한 사이버 블랙박스 및 통합 사이버보안 상황분석 기술 개발]

접수일자 : 2014년 12월 31일
수정일자 : 2015년 12월 24일
게재확정일 : 2015년 12월 30일
교신저자 : 서창호 e-mail : chseo@kongju.ac.kr

에서 DDoS 전용 보안장비를 출시하고 있으며, 아웃오브 패스 방식과 인라인 방식을 적용하여 일부 국제연구에서 학습기반 탐지/대응에 대한 연구가 진행되고 있으나, 연구초기 단계로 상용화하기에는 어려운 상황에 있다. ESM 장비가 NMS/SMS의 주요기능을 흡수합과 더불어 TMS 및 UTM 등과 같은 보안 솔루션과의 결합이 진행중에 있으며, 지속적인 사이버 위협의 증가로 기존 관제장비의 공격대응 한계를 인식하고 각 망별로 산발적 도입 적용된 단위망 보안장비들을 전역적 보안관리 측면에서 해결하려는 동향이다. 차세대 네트워크 보안솔루션의 다양한 요구사항을 충족할 수 있는 고성능 유무선 네트워크 위협대응 기술에 있어서 국내제품은 외국제품에 비해 기능면에서는 근접하나 성능은 미비한 상황에 있으며, 악성코드 탐지 및 시그니처 생성연구 관련하여 주로 Window OS에서 동작하는 악성코드 탐지 및 분석 연구 중심으로 진행하고 있다.

국내에서 시그니처 기반의 악성코드 경유/유포지 탐지기술이 일부 개발되었으나 대량의 신종 악성코드 탐지 어려움에 있으나, 최근 악성코드는 분석도구 회피, 실행정보 은닉등 다양한 지능화된 기능이 적용됨에 따라, 행위기반 동적 분석기술 필요하며, 융·복합 단말에서 개인정보 유출 방지 등 일부 보안 기술이 개발되었다. 그러나 최근 등장한 FMC 서비스에서의 보안기술 개발 필요하다. 현재 DDoS 대응 기술은 L3 계층의 네트워크 대역폭 고갈형 공격대응 및 대용량 트래픽처리 성능 강화 위주로 개발되고 있으며, 최근 지능화된 웹기반 DDoS 공격에 대한 대응 능력은 미비한 상황이며, 기존 L3기반의 무작위적인 패킷차단은 불특정 다수가 이용하는 응용서비스 적용은 어렵기 때문에 L7기반의 대응 솔루션 필요하며, 통합보안 제어 분야에 있어서, 단순한 보안장비의 통합관리에서 점차 네트워크 장비까지 연계 제어해주는 시스템으로 진화 발전하고 지속적이고 안정적인 사이버 보안관리와 사이버위기 적시 대응을 위한 전역적 통합보안제어 및 연동기술 개발의 필요성 대두되고 있다.

보안 이벤트 시각화 기술은 유선망에서 직관적인 인지를 위해 공격 이벤트를 시각화하는 기술이 연구되었으나, 무선망에 대한 공격 이벤트 수집 기술과 유무선망에 대한 N차원 속성간 시각화 기술 개발이 필요하다. 본 논문에서는 국내외 관련된 시스템 개발연구와 최신 사이버 보안 상황 침해 공격 분석을 통한 최신 다양한 신종 공격 기법 및 분석 기술의 현황 조사, 분석등을 기술한다.

그림 1. SPiDER TM of Architecture

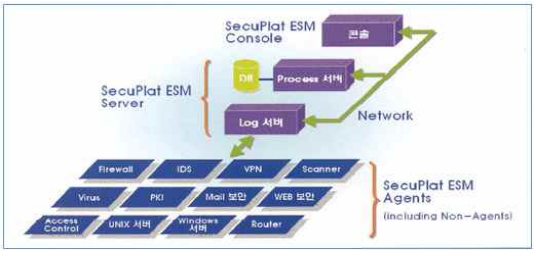

그림 2. Secuplat@ESM of Architecture

Ⅱ. 국내외 관련 연구

1. 국내 통합 관제 시스템

국내 보안 업체 중 한 곳인 이글루시큐리티에서 개발한 개방형, 멀티 밴더 기반의 전사적 통합보안관리 플렛폼으로서, IT 환경에서 발생 가능한 각종 위험들을 지속적으로 최소화하고 예방 할 수 있도록 개발된 일종의 Frame work이다[4]. SPiDER의 구조는 대상 시스템의 부화를 최소화하면서 효율적인 중앙 처리 및 운영이 가능하도록 그림 1과 같이 Data 수집 및 판단하는 Agent, Agent로부터 발생되는 정보를 저장, 분석하는 Manager, 시스템 리소스 상태 및 각 보안제품의 로그를 실시간으로 모니터링하고 수집된 각종 정보로부터 리포트를 출력 하며, 정책을 설정할 수 있는 Console 등 3-Tier Architecture로 구성 되어 있다.

인젠시큐리티 서비스(www.inzenss.com)에서 개발한 통합보안관리시스템으로 유연한 확장성을 제공함과 동시에 가용성을 높여주는 구조로, Agent, Server, Console로 구성되어있다 [5]. Server는 Process Server와 Log Server로 분리되어 있으며, 관리대상의 증가시 Log Server를 병렬로 추가 확장하여 관리대상에 대해 지속적으로 보안업무를 할 수 있도록 확장형 3-Tier-Architecture로 그림 2와 같이 설계되었다. 특징 및 장점으로 자사의 보안 제품을 통합한 제품으로 보안 기능을 제공 할뿐 아니라, 미 연동된 보안 제품이 있는 경우 추가 연동 위

한 커스터마이징 작업도 제공하고 있다.

2. 국외 통합 관제 시스템

최근 국내 ESM 시장에서는 2가지 기술 이슈가 부각되어와 왔다 [6]. 상호 연관성 분석과 능동인데 멀티 밴더 솔루션이 즐비해 있는 국내 전산 환경상 새로운 기술을 추가하는 것보다는 현재 시스템을 보다 효율적으로 관리 하도록 분석하는 것이 시급했다고 판단해 연관성 분석을 택한 국내시장과 달리 국외에는 능동이라는 요소 기술을 선택하였다. 국외 기업들의 경우 보안 솔루션의 종류가 국내처럼 많지가 않기 때문에 멀티 밴더형 ESM보다는 자사 중심적인 ESM 도입만으로도 충분한 관리가 가능하기 때문이다. 그렇기 때문에 국외에선 다양한 보안 솔루션을 분석 관리하는 것보다는 능동적으로 동작하는 솔루션이 필요한 셈이다. 국외에서는 미국, 영국 등 소수의 국가를 제외하고는 대부분의 국가에서 현재까지 국가/공공기관을 대상으로 보안 관제를 수행하지 않고 있는 것으로 확인되고 있다.

미 연방정부기관 전산망에 대한 사이버위협 징후 모니터링 등 관제 업무는 국토안보부 (DHS: Department of Homeland Security)내의 국가사이버보안처(NCSD : National Cyber Security Division)산하 US-CERT에서 수행하고 있다.

NCSD는「국토안보대통령명령(HSPD-7)」에 의거 2003. 6월에 설립되었으며 산하에 미국 사이버침해사고대응팀(US-CERT)을 운영하고 있다. 최근 들어 국토안보부는 중국 등 해외 스파이로 추정되는 해커의 공격으로 인해 주요 정부기 관의 컴퓨터시스템 정보가 노출되는 사고가 빈발하자 장관 직속의 '국가사이버안보센터(NCSC)'를신설(2008. 3월), FBI · NSA · 국방부 공조 하에 연방정부기관의 컴퓨터시스템에 대한 사이버테러를 감시하고 해킹 취약정보를 관리하는 등 모든연방정부기관의 컴퓨터시스템과 인터넷보안을 총괄하는 범 부처기구로 운영하고 있다.

국가안전부(NSA: National Security Agency) 정보보증국(IA)에서 국방망 일부 및 정보기관들이사용하는 정보망 등 주요 국가기밀을 보관, 소통하는 정보시스템 보호를 목적으로 테러상황실(TOC: Threat Operation Center)를 설치, 24시간보안관제 활동을 수행하고 있다.

국방부(DoD: Department of Defense)는 전략사령관 직속에 연합컴퓨터센터(JTF-CNO: JointTask Force - Computer Network Operation)를 설치하여 국방 CERT(DISA: Defense InformationSystem Agency)를 중심으로 전 세계에 주둔하고 있는 미군과 정보, 작전 수행 및 사이버공격을 상시 감시 중에 있다. DISA는 15-20명 규모의 상황실을 24시간 운영하면서 바이러스·해킹공격 등의 유무를 모니터링 하여 사이버공격 정보수집 및 대응활동을 수행 중에 있다.

Ⅲ. 사이버 보안 이벤트 분석

1. 보안이벤트 연관성

보안 이벤트 연관성 분석을 통해 관리 네트워크에 실제 위협이 되는 공격 징후를 선별하고 이들의 심각성을 계산하여 대응에 필요한 우선순위를 결정하는 위협 관리(threat management) 기능을 제공하는 분야이다. 주로 이기종의 보안이벤트간의 연관성을 분석함으로써 단일 정보로는 판단하기 어려운 위협을 발전하는데 이용된다. 가장 대표적인 방법으로는 IDS 정보와 관리 자산의 취약점을 연관 분석하여 실제 위협을 찾아내는 취약점 연관성 분석이 있다.

NIDS와 같이 네트워크를 모니터링 하여 이상 상태를 감지해 내는 메커니즘은 정의된 룰에 조금만 위배되더라도 이에 대한 경보를 발생시킨다. 따라서 이러한 경보 속에는 실제 관리 네트워크의 위협과는 상관없는 무의미한 정보가 다수 존재 할 수 있다. 예를 들면 해킹 툴에 의한 포트스캐닝을 탐지한 IDS에 의해 발생된 다수의 경보에는 이미 패치 되었거나 존재하지 않는 자산에 대한 공격을 탐지한 오경보가 대량으로 포함되어 있을 확률이 크다. 대부분의 해킹 툴은 근원지 주소 또는 목적지 주소를 무작위로 발생시키기 때문이다. 이와 같이 대량의 오탐지 이벤트 가운데 실제 위협을 선별하고 그 위협들에 대해서 우선 순위를 부여한 후 적절한 대응을 수행하는 threat refining 기술에 보안이벤트 연관성 분석 기술이 이용되고 있다.

2. 위협인지 영역

네트워크의 규모와 보안 서비스의 규모가 커짐에 따라 보완이벤트는 기하급수적으로 증가하기 때문에 보안관리자는 이들 데이터를 분석하여 현재의 네트워크 보안 상황을 즉각적으로 판단하기가 어려워졌다. 위협 인지(threat awareness) 방법은 사용자 인지 관점에서의 분석 방법으로써 관련있는 이벤트 정보를 하나의 view

에 가시적으로 표시함으로써 상호간의 관련성을 사용자가 직관적으로 인지할 수 있도록 하는 방법이다. 즉, 대량의 보안이벤트 정보를 구조화하여 상호간의 관계를 시각화(visualization)함으로써 관리자가 현재의 보안 상황을 쉽게 인지하도록 하기 위한 연관성 분석 방법이다. 위협 인지 방법으로는 사전에 공격 유형별로 발생하는 각 이벤트 정보간의 연관성을 도출하고 시퀀스를 규정하여 분석한 후 상호간의 상관성을 도출하고 시퀀스를 규정하여 분석한 후 상호간의 상관성을 이해하기 쉬운 형태로 가시화하는 View-based 방식과 다량의 이벤트 정보와 다수의 속성들을 의미 있는 정보로 표현하기 위하여 하나의 view에 다차원적으로 표현하는 event visualization 방법이 있다. View-based 방식은 사전에 분석된 방법을 토대로 시각화를 수행하기 때문에 그려진 결과물에 대한 분석도 어느 정도까지 자동화 할 수 있어 대량의 데이터를 처리하는데 매우 효과적이다 [7]. zation은 그려질 대상 이벤트 정보와 속성들을 주기적으로 수집하여 하나의 화면에 축약하여 나타내며 그 결과는 운영자가 판단하도록 하기 때문에 프로세스 부하가 적고 구현이 용이하나 매뉴얼적인 인지를 강조하는 방법이기도 하다. 이처럼 시각화를 이용한 방법들은 분석에 대한 계산 오버헤드가 타 방법에 비하여 비교적 작으며 구현 알고리즘이 단순하여 대량의 데이터를 실시간으로 나타낼 수 있는 장점이 있어 대규모 네트워크의 분석방법으로 유효하다. 하지만 객관적이고 수치적인 보고기능 처리가 결여되기 때문에 결과에 대한 정확한 판단은 사용자의 직관적인 인지에 의한 의사결정에 맡길수 밖에 없는 단점이 있다.

3. 중복데이터 제거

디듀플리케이션이란 중복 데이터를 확인하고 제거하여 백업에 필요로 하는 디스크의 용량을 획기적으로 줄여 주는 기술이다 [8]. 이 기술을 활용하면 스토리지 내에서 중복되는 부분을 불필요하게 저장할 필요가 없게 된다. 이를 통해 많은 혜택들이 발생할 수 있다. 단순하게 살펴본다면 디스크의 용량이 줄어든다는 장점이 있을 수 있다. 디듀플리케이션 시스템에 따라 중복 데이터를 제거하는 방식이 다르긴 하지만, 대부분의 접근 방식은 서브파일(블록; block) 레벨에서 해당 데이터가 이전에 기록된 적이 있는지를 확인해서 제거하는 것이다. 디듀플리케이션 시스템은 다음과 같은 경우에 적용될 수 있을 것이다. 다섯 대의 서버에서 같은 파일이 백업한다. 95%는 중복되는 데이터 블록이고 주말 풀 백업의 5%만이 다른 데이터이다. 인크리멘탈 백업을 지원하지 않는 데이터베이스의 풀 백업 매일 변경되는 스프레드시트의 경우 해당 파일의 인크리멘탈 백업 디듀플리케이션의 최대 장점이라고 한다면 아마도 테이프 백업 체제에서 벗어난 온사이트(onsite)와 오프사이트(offsite) 백업을 할 수 있다는 점일 것이다. 디듀플리케이션 기능을 하는 VTL은 매번 백업 시에 유일한 블록만을 기록하게 된다. 그러한 유일한 블록은 VTL의 복제(Replication) 기능을 통해 오프사이트(offsite)로 쉽게 복제될 수 있다. 이렇게 함으로써 리플리케이션(Replication) 서비스가 보다 더 실용적으로 현장에 도입될 수 있는 것이다.

Ⅳ. 보안 관제 상화 강화 모델

보안관제 상황의 네트워크 망 고도화를 위한 접근통제 모델에서 고려되어야 할 점은 다음의 4가지로 요약될 수 있다.

1. 새로운 컴퓨팅 환경

미래의 컴퓨팅 환경은 고해상도 평면 디스플레이나 인스턴트 온(Instant-On) 같은 기기와 관련된 기술의 발전과 플랫폼의 자동 선택 등의 네트워크 컴퓨팅 기반구조의 추가기능을 바탕으로 새로운 스타일의 컴퓨팅 환경으로 변화할 것으로 예측되고 있다[52,53].

새로운 컴퓨팅 환경의 이점은 사용자가 장소와 환경을 바꿔도 작업과 동작에 계속성을 갖게 된다는 것이다. 지금까지 존재하지 않았던 방법, 즉 인터넷에 의하여 가정과 기업의 데스크톱에서 정보를 접속할 수 있었듯이 새로운 컴퓨팅 환경에 의해 더욱 더 광범위한 접속 포인트에서 디지털 컴퓨팅 세계가 확산될 것이다. 하지만 이러한 새로운 컴퓨팅 환경의 주요한 과제는 컴퓨팅 정보의 보관 및 접속에 이용하는 기기의 영역과 개수를 관리하는 것이다. 어떤 기기와의 접속 포인트가 중요하게 지원되어야 하는가를 판단하고 증가한 기기사이에 데이터를 동기화 할 때 보안 관련성이 철저하게 검토되어야 한다. 특히 어떤 사용자에게 어떤 기기에 대한 접근을 허용하고 불허할 것인지에 대한 접근통제에 대한 보안 측면에 대한 연구가 반드시 요구된다. 또한 차세대 접근통제 모델은 전통적인 컴퓨팅 환경보다 훨씬 많은 수의 주체와 객체를 지원해야 하므로 이들을 체계적

으로 표현하고 관리하는 기능이 필수적이다.

2. 미래의 응용 기기 지원

새로운 컴퓨팅 환경에서 사용자는 필요한 장소에서 실시간으로 정보를 입수할 수 있다. 이는 정보에 대한 접속과 정보 생성변화를 근본적으로 변화시킬 기술에 의해 가능하게 된다.

새로운 컴퓨팅 환경의 특징은 지금까지 존재하지 않았던 새로운 형태의 응용기기가 출현할 수 있다는 점이다. 예를 들면, 멀리 떨어져 있는 지하 미궁과 같은 장소에서 랩톱컴퓨터를 이용하지 않고 중앙제어 센터에서 보내오는 지시를 눈앞에서 그것도 3차원 영상으로 보게 하며 키보드에 의하지 않고 음성인식에 의한 입력이 가능한 새로운 미래형 응용기기를 생각할 수 있다. 미래형 기기의 기능에 따라 수많은 정보와 자원을 소유할 수 가 있는데 이에 대한 접근통제에 대한 지원은 매우 중요하다. 왜냐하면 이들은 독립적으로 동작하는 것이 아니라 상호 통신을 통해서 유기적으로 연결되어있기 때문이다.

3. 컨텍스트 인식 지원

컨텍스트형 환경이란 센서 기술 등을 사용하여 사용자의 작업 내용에 따라 장치와 인터페이스가 특화된 환경을 말하는데, 접근통제에서는 이를 또한 반영해야 한다. 예를 들어 시스템은 센서를 통해 먼저 사용을 하려는 사람이 누군지 확인을 한다. 이러한 과정이 끝나면 시스템은 그 사용자에게 할당되어 있는 역할을 활성화시키게 된다. 이 사용자 역할은 그가 접근할 수 있는 자원에 대한 권한 정보를 가지고 있게 된다. 만약 철수가 부엌으로 가서 인터콤 서비스를 사용하려고 할 때, 그의 요구는 현재 집의 보안규칙을 관리하는 중앙의 인가 서비스로 전달되게 되고, 이 규칙은 철수가 특정한 상태하에 있을 때만 이 요구를 허가하게 된다.

이처럼 생활 속에서의 컴퓨팅 시대가 도래함에 따라 실제 공간 속의 센서 기술이 컨텍스트를 인식해서 접근통제가 이루어지는 형태가 미래 인터넷 진화를 위한 연구망 환경의 핵심이 될 것이다.

4. 적응성(adaptation) 지원

새로운 테크놀로지의 도래는 응용기기 설정은 사용자가 일일이 해주지 않아도 스스로 설정하는 능력이 요구된다. 이는 새로운 응용기기는 생활환경 자체가 컴퓨팅 환경이므로 응용기기에 모두 환경설정을 해준다는 것이 생산성의 감소를 의미한다. 접근통제를 시행함에 있어 정책이나 특별한 설정이 되지 않아도 스스로 환경을 감지하여 접근통제를 시행할 수 있는 적응기술 또한 다가오는 차세대 접근통제에서는 요구된다.

Ⅴ. 보안 관제 상화 강화 모델

현재 DDoS 대응 기술은 L3 계층의 네트워크 대역폭 고갈형 공격대응 및 대용량 트래픽처리 성능 강화 위주로 개발되고 있으며, 최근 지능화된 웹기반 DDoS 공격에 대한 대응 능력은 미비한 상황이며, 기존 L3기반의 무작위적인 패킷차단은 불특정 다수가 이용하는 응용서비스 적용은 어렵기 때문에 L7기반의 대응 솔루션 필요하며, 통합보안 제어 분야에 있어서, 단순한 보안장비의 통합관리에서 점차 네트워크 장비까지 연계 제어해주는 시스템으로 진화 발전하고 지속적이고 안정적인 사이버 보안관리와 사이버위기 적시 대응을 위한 전역적 통합 보안제어 및 연동기술 개발의 필요성 대두되고 있다.

보안 이벤트 시각화 기술은 유선망에서 직관적인 인지를 위해 공격 이벤트를 시각화하는 기술이 연구되었으나, 무선망에 대한 공격 이벤트 수집 기술과 유무선망에 대한 N차원 속성간 시각화 기술 개발이 필요하였으며, 본 중간보고서에서는 통한 사이버 보안 관제를 위해 트래픽 정보와 이벤트 정보를 효과적으로 분석할 수 있도록 하는 연관성 분석 기술의 현황 조사, 분석하였다.

본 연구에서는 네트워크망을 위한 보안 서비스 강화를 위해 모델 및 구축을 지금까지 연구되어온 주요 접근통제 모델들을 조사, 분석하고 앞으로 요구되는 미래 인터넷 진화를 위한 연구망 환경에 대한 접근통제 모델에 대한 요구사항 및 핵심 기술에 대해 조사하였다. 차세대 접근통제 모델에 대한 해결책으로 기존의 접근통제 모델에 차세대 환경에서 요구하는 여러 요구 사항을 수행하는 방안을 제시하고, 또한 이를 반영할 수 있도록 시간, 장소 등 여러 제약조건을 반영하여 기존의 모델과의 통합하는 방안을 제안하였다.

따라서, 국가·공공기관 및 지방자치단체의 정보통신망을 안전하게 보호하기 위해서는 국가차원에서 이들기관에 대한 보안관제대책을 마련하여 모든 기관이 보안관제를 의무적으로 수행하도록 하고 그 이행 여부를 확

인 감독할 수 있는 장치를 강구하여 실효성을 확보함으로써 국가보안관리 수준도 높아질 것이다.

그러나, 보안관제를 아무리 철저히 한다고 하더라도 알려지지 않은 신종 사이버공격은 보안관제 과정에서 탐지되지 않으므로 알려지지 않은 사이버공격을 탐지, 차단할 수 있는 기술을 지속적으로 개발해 나가야 한다.

ACKNOWLEDGMENTS

This work was supported by the ICT R&D program of MSIP/IITP. [14-823-06-001, The Development of Cyber Blackbox and Integrated Security Analysis Technology for Proactive and Reactive Cyber Incident Response]

참고 문헌

[1] NIS, MSIP, KCC, MOSPA, KISA, NSRI, "2013 National Information Security White Paper" Apr. 2013.
[2] Tankard, Colin. "Advanced Persistent threats and how to monitor and deter them" Network security, pp.16-19, 2011.
[3] http://www.microsoft.com/ko-kr/security/default.aspx
[4] http://www.igloosec.co.kr/
[5] www.inzenss.com
[6] M. O'neil, "Unix System in a Large Enterprise Environment - Axent ESM", SANS Institute Information Security Reading Room, 22 June 2001.
[7] A. Sinha, A. Wang, and A. Chandrakasan, “Algorithmic Transforms for Efficient Energy Scalable Computation”, Proc. of ISLPED, 2000.
[8] K. Srinivasan, et al., iDedup: Latency-aware, inline data deduplication for primary storage, USENIX FAST 2012.

저 자 소 개

남승수 (학생회원)

2012년 2월 : 공주대학교 응용수학과(이학사)
2014년 8월 : 공주대학교 융합과학과(공학석사)
2014년 8월 - 현재 : 공주대학교 융합과학과 박사과정중
〈주관심분야 : 영상처리, 정보보호, 네트워크 보안〉

서창호 (정회원)

1990년 2월 : 고려대학교 수학과 졸업(학사)공학석사
1992년 2월 : 고려대학교 수학과(석사)
1996년 8월 : 고려대학교 수학과(박사)
1996년 8월 ~ 2000년 2월 : 한국전자통신연구원 선임연구원, 팀장
2000년 3월 ~ 현재 : 공주대학교 응용수학과 교수
〈주관심분야 : 암호알고리즘, PKI, 무선 인터넷 보안 등〉

이주영 (정회원)

1999년 2월 : 연세대학교 컴퓨터과학과 공학석사
2000년 2월 - 현재 : 한국전자통신연구원 선임연구원
〈주관심분야 : 정보보호, 디지털 포렌식, 네트워크보안〉

김종현 (정회원)

2000년 2월 : 오클라호마주립대 컴퓨터학과공학석사
2005년 2월 : 오클라호마주립대 컴퓨터학과공학박사
2005년 2월 - 현재 : 한국전자통신연구원 선임연구원
〈주관심분야 : 정보보호, 네트워크보안, 역추적기술〉

김익균 (정회원)

1994년 2월 : 경북대학교 컴퓨터공학과 졸업(공학사).
1996년 2월 : 경북대학교 컴퓨터공학과졸업(공학석사).
2009년 2월 : 경북대학교 컴퓨터공학과 졸업(공학박사).
2005 2월 : Purdue University 객원연구원.
1996년 2월 - 현재 : 한국전자통신연구원 네트워크보안연구실 실장/책임연구원.
〈주관심분야 : 네트워크 보안, 컴퓨터네트워크, 클라우드보안〉