主題

액티브 보안 기술

한국전자통신연구원 방효찬, 나중찬, 손승원, 박치항

차 례

요 약

현재의 네트워크 보안 기술에 비해서 보다 강력한 대응을 수행할 수 있는 보안 메커니즘을 지니며, 새로운 환경 변화에 대한 필요한 보안 메커니즘을 보다 신속하게 도입하고, 중앙 집중적으로 효율적인 보안 관리를 지원하는 데 목표를 두고 연구되고 있는 분야가 액티브 보안 분야이다.

본 논문의 목적은 인터넷 인프라 자체가 취약하다는 근본적인 문제점을 해결하기 위해 호스트 단위 또는 소규모 네트워크 단위를 보호하는 것을 포함하여 유해한 트래픽이 사용자 컴퓨터 내지는 사용자 네트워크에 도달하기 이전에 차단하는 네트워크 생존성 차원에서 새로운 네트워크 보안 기술인 액티브 보안 기술에 대한 아이디어를 소개하는 것이다.

Abstract

It is an active security that has the research field which has more powerful responding mechanism comparing to current network security technology, has an ability to introduce new security mechanism according to changing our environments, and can support effective security management.

Our goal is to introduce a new category of internet security technologies on network survivability: active security technology. It is a new security technology that blocking network or computers, before malicious traffics are reached to them, including protecting hosts or small area network from hackers.

I. 서 론

네트워크가 고속화 고도화됨에 따라 정보통신 서비스는 인터넷을 통해 보편적으로 제공되는 생활기반

서비스로 발전하고 있으며, 서비스를 이용하는 편리성에 더하여 시스템 및 네트워크 차원에서 보안 기능에 대한 요구도 날로 증가하고 있다. 특히 보안 관리 범위는 지엽적 네트워크가 아닌 광역 네트워크 차원으로 확대되고 있다. 또한 네트워크 차원에서 제공해야 하는 보안 서비스와 새로운 요구 기능의 출현 주기도 점점 짧아질 뿐만 아니라, 서비스와 요구 기능 자체의 다양성도 점차 증가하고 있다.

이러한 기대에 부응하여 현재의 네트워크 보안 기술은 점차 기능의 고도화, 지능화, 고성능화를 지향하면서 단일 보안 솔루션에서 다양한 보안 기능을 결합한 통합 솔루션으로 변화되고 있다. 그러나 현재의 기술은 침입자에 대한 대응에 중점을 두기보다는 자신의 도메인(네트워크)를 어떻게 효율적으로 방어할 것인가에 주안점을 두고 발전하고 있는 상태이다. 따라서 해당 침입자의 공격을 탐지하였음에도 불구하고, 침입자에 대한 대응이 자신의 도메인 상에 그침으로써 침입자는 우회 경로를 통해 인터넷을 자유로이 이용할 수 있게 되고, 이로 인해 제 2, 제 3의 공격이 가능하다.

또한 새로운 기술을 채택한 공격 방법이 등장하였을 경우, 이에 대한 탐지 및 대응 기술과 이를 수용하는 시스템을 개발하여 실제 사용되기까지는 많은 시일과 비용이 소요된다. 이로 인해 사용자의 보안 기능에 대한 요구 조건의 변화 속도와 이를 지원하기 위한 시스템 및 네트워크의 변화 속도에는 차이가 발생하게 되어 이들 서비스 및 요구 기능을 시기 적절하게 반영할 수 없는 것이 현재의 정적인 보안 프레임워크의 문제점이다.

이를 극복하기 위해 향후의 보안 프레임워크는 네트워크에 존재하는 각 보안 시스템간의 상호 결합적인 운용을 통해 전체 네트워크 차원에서 공격에 대한 탐지 및 대응이 가능해야 할 것으로 보인다. 또한 현재의 네트워크 보안 기술에 비해 보다 강력한 대응을 수행할 수 있는 보안 메커니즘을 지니며, 그 실행 구조에 있어서는 새로운 공격 기술에 대한 보안 메커니즘을 보다 신속하고 경제적으로 도입하고 효율적으로 보안 관리할 수 있는 유연하고 개방된 구조를 지녀야 할 것으로 보인다.

본 논문의 목적은 인터넷 인프라 자체가 취약하다는 근본적인 문제점을 해결하기 위해 호스트 단위 또는 소규모 네트워크 단위를 보호하는 것을 포함하여 유해한 트래픽이 사용자 컴퓨터 내지는 사용자 네트워크에 도달하기 이전에 차단하는 네트워크 생존성 차원에서 새로운 네트워크 보안 기술인 액티브 보안 기술에 대한 아이디어를 정립하고자 하는 것이다. 2장은 새로운 네트워크 보안 프레임워크 진화 단계를 정의한다. 3장에서는 액티브 보안 프레임워크와 관련한 현존하는 관련 연구를 기술한다. 4장에서는 액티브 보안 기술을 실현하는데 있어 기술적, 제도적, 사회적인 관점에서 고려해야할 사항을 기술한다. 마지막으로 액티브 보안 기술의 전망을 간략히 기술하면서 결론을 맺는다.

Ⅱ. 액티브 보안 프레임워크

최근 시스템과 네트워크에 대한 공격의 탐지 및 대응을 위한 프레임워크에 대한 연구가 활발히 진행되고 있다. 두 시스템이 독립적으로 운용되는 초기의 프레임워크에 반해, 현재는 두 시스템을 상호 연동하여 공격의 탐지 및 그에 대한 대응을 자동적으로 수행할 수 있는 통합 보안 시스템이 출시되어 각 기관에서의 도입이 증가하고 있는 상황이다[1,2,3]. 하지만 두 시스템 간의 상호 연동을 위한 프로토콜이 각 업체별로 존재하며, 적용범위가 특정 시스템 또는 해당 기관의 내부망으로 한정되기 때문에 향후의 보안 프레임워크로는 사용되기는 어려울 것으로 보인다. 그리고 발생하는 공격 유형이 점점 복잡해져서 단일 보안 시스템으로는 이에 대한 탐지 및 대응이 불가능해질 것으로 보이며, 공격이 일어나는 네트워크 범위가 광역화되고 공격 시간도 점점 길어지고 있다. 특히 보안 환경의 경우, 시스템 또는 네트워크에서 수

용하는 서비스의 추가 및 변경이 수시로 발생함에 따라 보안 정책 및 관련 기술의 해당 시스템에 대한 반영 요구가 매우 빈번할 것으로 보인다. 따라서 향후의 보안 프레임워크는 다음과 같은 요구 조건의 변화를 충족시켜야 할 것으로 보인다.

- o 각 보안장비의 독립적인 운용에서 전체 네트워크 차원에서의 상호결합적인 운용
- o 공격에 대한 지엽적인 대응보다는 전체 네트워크 차원에서의 보다 강력한 대응
- o 새로운 보안 정책 및 관련 기술의 수용이 용이한 개방적인 실행 구조를 제공

인터넷 상에 존재하는 보안 메커니즘이 고정된 현재의 기술과는 달리, 프로그래밍이 가능한 향후의 보안 프레임워크에서 새로운 보안 메커니즘 또는 기존의 보안 메커니즘을 유연하게 확장하기 위한 상기의 요구조건을 만족시키는 성질들은 아래와 같으며, 이와 같은 성질은 향후의 보안 프레임워크의 축을 형성할 것으로 보인다.

- o 확장성(extensibility)
  수행시간에 동적으로 보안 메커니즘 적재 가능
- o 유연성(Flexibility)
  새로운 보안 환경 또는 기업 조직 변화에 따른 보안 장비 위치 및 보안 장비 증가에 대한 자기 적응이 가능
- o 상호연동성(Interoperability)
  각 벤더들이 제시하고 각각의 Firewall IDS(Intrusion Detection System) 항바이러스(Anti-Virus) VPN(Virtual Private Network) 등의 보안 장비 또는 응용들간에 상호연동을 통하여 계층적인 중앙집중의 관리 환경 제공이 가능하며, 이는 단일 콘솔 상의 단순화된 보안관리가 가능함으로써 효율적인 보안 기술 적용이 가능

확장성, 유연성, 상호연동성 이외에도 향후의 보안 프레임워크를 정립하는데 있어 확장성과 유연성으로 인한 상호 배타적인 요소인 보안성과 효율성에 상반관계를 가지며, 상호연동성의 적용 범위에 따라 향후의 보안 시스템의 배치와 상반관계를 갖는 점 등을 고려해야 한다.

향후의 보안 프레임워크의 축을 형성하는 주요 세 가지 특징은 상호보완적이 성격을 갖는다. 즉, 액티브 보안 시스템 설계를 고려하는데 있어 이전의 주요 세 가지 축을 삼차원 공간으로 표시하면 그림 1과 같다.

현존하는 보안 프레임워크는 상기의 세 가지 관점에서 적절한 지점을 선택하고 있다. 향후의 보안 프레임워크는 궁극적으로는 상기 세 가지 관점의 최적점을 선택하여 발전할 것으로 보인다. 단, 확장성과 유연성에 상반되는 효율성이 선결되지 않고는 실용적인 측면에서 부딪힐 것으로 예상되기 때문에, 향후의 보안 프레임워크는 상호연동성에 초점을 두고 진행될 것으로 예측된다.

다음 장에서는 향후의 보안 프레임워크가 가져야 하는 요구조건을 만족시키는 액티브 보안 프레임워크와 관련된 연구 분야에 대해 다루고자 한다[10,11]. 특히 언급하는 각 관련 분야는 확장성, 유연성, 상호연동성에 초점을 두면서 적용 정도를 비교하고자 한다.

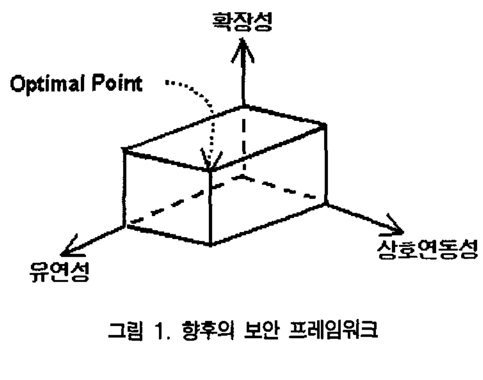


그림 1. 향후의 보안 프레임워크

Ⅲ. 관련 연구

현재 많은 정보보안 업체에서 보안 문제를 해결하기 위해 firewall, filtering router, guards 등과 같은 다양한 보안 장비들을 선보이고 있지만, 이들 장비들은 모두가 지엽적인 침입탐지와 이에 대한 개별적인 대응을 수행하고 있다. 설사 시스템 전반적인 협력을 통해 침입을 감지하고 대응하는 구조를 갖추려 해도 원격적인 공격자 차단 기능을 구현할 만한 표준 모델이 존재하지 않고 있다. 따라서 현재의 시스템적 대응 한계를 극복하기 위해 서로 다른 네트워크 시스템 간에 공격자 탐지 정보를 공유하고, 이를 통해 모든 시스템 환경에서 일정한 대응을 유도해내기 위한 인프라 구축과 관련된 많은 연구가 진행되고 있다.

1. NAIs ActiveSecurity[1]

NAI의 ActiveSecurity는 이동형 센서를 이용하여 신속하고 효율적인 대응을 제공하는 각 보안 장비간의 통합된 보안 솔루션이다. 그림 2는 ActiveSecurity의 구성 요소들간의 관계를 나타낸 것으로서, 센서는 네트워크 장치들을 감시하고 의심스러운 행위가 감지되면 중재자에게 보고한다. 중재자는 센서로부터 받은 정보를 바탕으로 최적의 대응 방안을 결정하고 행위자에게 취해야 할 대응 방법을 전달한다. 행위자는 중재자로부터 받은 대응을 대상 노드에 행하는 역할을 가지고 있다. 위의 모든 동작은 보안 정책을 기반으로 이루어지고, 이 정책들도 상황에 맞게 동적으로 변화할 수 있다.

각 구성요소는 Gauntlet Firewall, Cyber Cop Scanner, CyberCop Monitor, Event Orchestrator 등이 있다. 여기서 중재자에 해당되는 Event Orchestrator는 NAI 제품뿐만 아니라 다른 보안 제품들을 위한 이벤트 관리로써 네트워크 내의 보안 센서로부터 발생되는 이벤트를 중재하고 보안 정책을 관리하며, 이를 바탕으로 최적의 대응방안을 결정하여 행위자가 취해야 할 대응 방법을 결정한다.

NAI의 ActiveSecurity는 보안 환경에 유연하고 신속한 적응성을 지니는 보안 시스템 및 환경을 제공하는 것을 목적으로 하고 있으며, 모듈 접근방식을 토대로 구현되었기 때문에 자신이 필요로 하는 제품을 쉽게 통합할 수 있다.

2. OpenService's SystemWatch[3]

OpenService사의 SystemWatchsms 보안 장비 및 응용으로부터 발생하는 이벤트를 분석하고 상호연동을 통해 시스템과 개인이 취해야 할 적절한 대응방법을 결정하고, 벤더들의 보안 장비와 응용을 통합하여 하나의 콘솔로 관리함으로써 자동화된 보안 관리 솔루션을 제공한다. 또한 표준 플랫폼을 사용함으로써 우연성을 제공하며, 보안 장비의 증가와 기업 조직 변화를 만족시키기 위한 적응성을 갖는다. 중요한 보안 응용프로그램과 제품들을 자동 관리하기 위

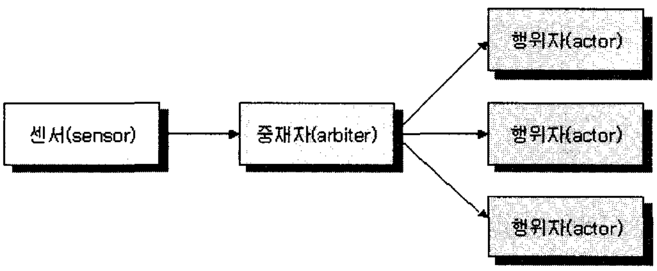


그림 2. NAI의 Active Security 구성요소

한 목적으로 다른 벤더들의 보안 제품들에게 공개 인터페이스를 제공한다.

위의 그림 3는 SystemWatch 구조를 나타내는 것으로, SystemWatch Security Agent는 각 보안 장비에 상주하여 각 장비로부터의 데이터 및 상태 정보를 수집 · 분석하고, 보안 어플리케이션의 감시 및 관리를 수행한다. 각 에이전트로부터 실시간으로 수집된 이 정보는 SystemWatch의 상위 콘솔(Open Management Console: OMC)로 전달되고, OMC는 이를 웹 환경으로 보여준다. 이러한 계층적인 SystemWatch의 구조는 모든 보안 장비들이 하나의 콘솔로 통합 관리를 가능하게 한다.

3. AN-IDR[6,7,8]

AN-IDR(Active Network Intrusion Detection and Response)는 1999년에 NAI Lab.과 Boeing 사를 주축으로 하여 DARPA (Defense Advanced Research Projects Agency) ITO (Information Technology Office) 산하의 Active Network 프로그램 아래에서 수행되던 것으로 현재는 FTN(Fault Tolerant Network) 프로그램으로 옮겨져서 수행되고 있다. 또한 단독으로 수행되기보다는 Active Network 프로그램의 많은 프로젝트들의 결과를 이용하고 있는 특징이 있다.

이 프로젝트는 침입자를 탐지하고 추적하여 공격자와 인접한 네트워크 노드에서 공격자의 네트워크에 대한 연결성을 단절함으로써 공격자에 대해 보다 강력한 대응을 하기 위한 목적으로 수행되고 있다.

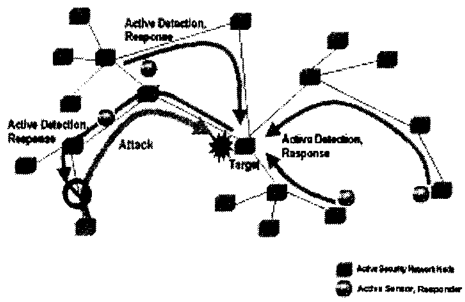


그림 4. AN-IDR 개념

AN-IDR은 이전에 수행되었던 ITO SLSS (Survivability of Large Scale System) 프로그램에서 수행한 IDIP(Intrusion Detection and Isolation Protocol) 프로젝트의 수행결과를 그대로 사용하고 있다[8]. 다만 IDIP가 가지는 정적인 특성으로 인한 유연성의 부족함과 특정 기능 수행상에 있어서의 효율성 저하를 해결하기 위해 액티브

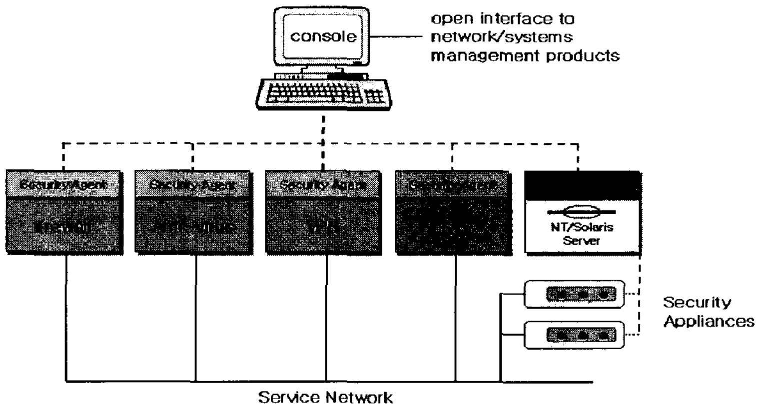


그림 3. OpenService's SystemWatch 구조

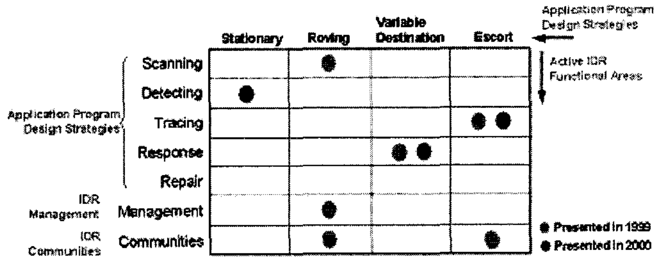


그림 5. AN-IDR 연구대상 영역

네트워크 기술을 적용하고자 하였다. 따라서 AN-IDR은 IDIP과 액티브 네트워크 기술을 결합하여 상호운용 함으로써 환경변화에 대한 적응성과 대응방법에 있어서 좀더 발전된 탐지 및 추적 메커니즘을 제공하고자 한다.

AN-IDR에서 연구대상으로 삼고 있는 기능에는 주로 IDR 기능, IDR 관리 기능, IDR 도메인 관리 기능 등이 있으며, 이 기능들을 중심으로 네트워크 상에서 이동하고 실행되는 방식에 따라 그림 5와 같이 분류하여 연구하고 있다.

그림 5에서 행은 각 기능들이 네트워크 상에서 이동하고 실행되는 방식을 나타내며, 열은 각 IDR 기능을 나타내고 있다.

상기 연구는 사이버 공격에 대한 기존의 수동적인 대응에서 벗어나 능동적이고 공격적인 대응을 할 수 있다는 측면에서 매우 훌륭한 개념이다.

4. Checkpoint's Smart Defence[9]

CheckPoint사는 차세대 보안 관리 솔루션으로 2002년 3분기에 능동형 보안 관리 시스템 부류의 첫 출시 솔루션으로 SmartDen- fense를 선보이기 시작하였으며, 주요 특징으로는 그림 6와 같다.

SmartDefense는 현재 알려진 모든 공격을 비롯하여 알려지지 않은 공격에 대해서도 침입에 대한 유형적인 구분에 따라 지능적인 보안 기술을 이용하여 대응한다. 탐지 차단 감사 경보에 대한 실시간 정보를 하나의 콘솔로 제공함으로써 중앙집중적인 보안 관리 환경을 제공하며, DoS, IP 공격, 네트워크 프

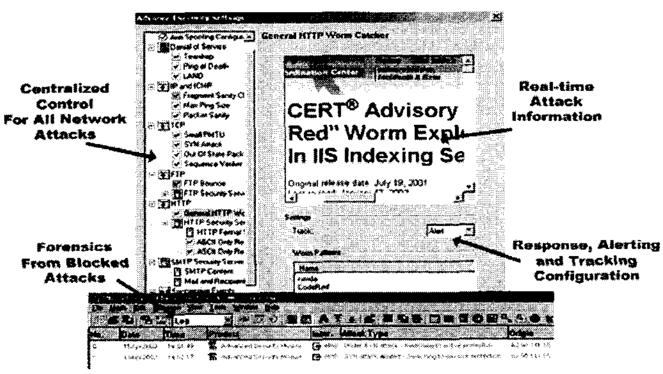


그림 6. Checkpoint사의 SmartDefense 특징

로빙, 웹과 응용들의 취약점 등을 포함한 공격 유형에 대처하고, 완전한 네트워크 방어를 위해 추가적으로 경보, 추적 감사 기능을 중앙에서 설정한다. 또한 새로운 공격 유형에 대한 보안 서비스를 온라인으로 업데이트하여 보안 관리 시스템의 확장성을 제공하며, 공격 방식에 대한 세부적인 설명과 특징을 포함한 인터페이스를 제공하며 보안관리자에게 네트워크 공격에 대한 이해와 적절한 대응 방법을 알려 준다.

이는 기존의 장비간의 상호연동을 고려한 통합보다는 새로운 기술이나 기능 요구 변화와 보안 시장의 확장에 따라 더불어 진화하는 형태로 발전을 기본으로 하고 있다.

Ⅳ. 액티브 보안 고려사항

현재 향후의 보안 프레임워크의 요구사항을 충족시켜줄 수 있는 보안 기술을 확보하기 위해 DARPA를 중심으로 보안 프레임워크 구조 정의 및 통신 프로토콜, 보안 시스템 실행 구조 등과 같은 요소기술들에 대한 활발한 연구가 진행되고 있다[4,5]. 이와 관련하여 액티브 보안 프레임워크에 대한 주요 고려사항은 다음과 같다.

- o 통합된 계층적인 보안 관리 구조
  보안 관리 시스템은 각 벤더들이 제시하고 있는 보안 장비와 응용들이 혼합되어 있는 환경에서 접근 및 통합되어져야 하며, 단일 콘솔 상의 단순화된 효율적인 보안 관리 기술을 허용해야 한다. 따라서 설정된 보안 정책에 따라 효율적인 집중화된 제어를 갖게된다.
- o 전체 네트워크 차원의 상호 연동을 통한 자동화된 대응
  보안 관리 시스템은 정보를 수집하고, 적절한 보안 관리를 위한 행위를 할 수 있어야 한다. 이러한 행위에는 자동화된 사전 방어 또는 응답 시스템 기능을 포함한다.
- o 보안 환경 변화에 따른 유연한 보안 프레임워크
  보안관리 시스템은 기업의 특정한 요구에 따라 적절히 적응할 수 있는 유연한 구조를 가져야 한다. 즉, 기업 조직 변화에 따른 보안 장비 증가에 대한 자기 적응성을 가져야 한다.

이외에도 사회적인 요구, 기술적인 측면에서 침입자에 대한 추적, 고립화 기능에 대한 분위기는 점점 무르익어가고 있는 상태이다. 다만, 임의의 호스트에서 어느 수준까지 추적이 가능한지는 아직 불명확한 상태이며, 이러한 기술적인 문제와 추적을 위해 패킷 헤더 부분을 검사하는 범위를 결정하는 규제적인 문제가 남아 있는 상태이다. 하지만 이런 기능들에 대한 요구가 점차 증가함에 따라 규제적인 문제는 자연스럽게 해결될 것이고, 기술적인 진전도 이루어질 것으로 보인다.

Ⅴ. 결 론

액티브 보안 기술은 보안 프레임워크에 유연성을 부여함으로써 다음과 같이 네트워크 보안 분야에서 보안 신뢰도를 한 차원 향상시킬 것으로 보인다.

- o 사이버 공격에 대한 탐지 및 대응 기능을 보안 시스템이 설치된 지역에만 한정하지 않고, 이동코드로 구현함으로써 사이버 공격에 대한 신속하게 대응할 것으로 보인다.
- o 사이버 공격에 대한 탐지 및 대응 기능을 이동코드를 활용하여 보안 취약 지점에 집중적으로 배치하게 함으로써 효율적인 대응을 수행할 수 있으며, 이동코드를 통하여 네트워크 말단(해커가 네트워크에 접속하는 지점)에 대응 방안을 강구함으로써 해커를 망으로부터 고립화를 시키거나 보안 도메인간의 유연한 상호 결합을 통해 우회적으로 침투하는 사이버 공격을 원천적으로 대응하여 보다 강력한 대응을 수행할 것으로 보

인다.

- o 보안 시스템의 실행 환경 및 네트워크 노드의 실행 환경을 동적으로 구성함으로써 보안 환경 변화에도 하드웨어나 소프트웨어 변경 없이도 자동적으로 전체적인 보안 도메인 상에서 보안 기능의 업그레이드가 가능하게 된다.
- o 전체 도메인의 보안 구조의 구조를 동적으로 재구성하거나, 변경할 수 있으므로 새로운 사이버 공격에 대한 즉각적인 대응 기술을 적용할 수 있고, 전체 도메인의 방어 능력을 향상시킬 수 있을 것으로 보인다.

향후 국내 각 기관들의 보안 정책과 의지를 반영하고, 액티브 보안 기술을 적용하기 위해서 국내에서 운용중인 여러 네트워크 플랫폼에 공통적으로 적용될 수 있도록 각 장비별 플랫폼에 이식이 가능한 프레임워크 작업이 이루어져야 할 것이다. 이를 바탕으로 액티브 보안을 위한 시스템들간의 통신 프로토콜 정의 및 구현, 공격 및 대응의 동작 양식을 기술할 수 있는 언어, 액티브 보안 메커니즘 실행을 위한 각 플랫폼별 실행환경, 시스템들간의 인증, 암호화 기술들에 대한 연구가 신속히 이루어져야 할 것이다.

참 고 문 헌

[1] Gerhard Escelbeck, "Active Security : A Proactive Approach for Computer Security System", Journal of Network and Computer Application, Vol.23, 2000.

[2] CheckPoint, "Open Platform for Security(OPSEC)", http://www.checkpoint.com/op- sec

[3] OpenService Inc., "A Flexible Architecture for Internet Security Management", http::/www.open.com, White Report, 2000.

[4] DARPA, "DARPA Information Survivability Program", http://www.darpa.mil/ito/res- earch/is

[5] CICS, "High Confidence System FY2000 BlueBook", http://www.ccic.gov/pubs/blue- 00/hcs.html

[6] Intrusion Detection and Response (AN-IDR), DARPA ANETS PI Meeting, Jun. 5, 2001.

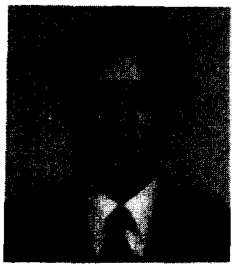
[7] Dan Sterne and Sandra Murphy "Secure Active Intrusion Response to DDoS", DARPA ANETS PI Meeting, Dec.6, 2000.

[8] Dan Schneckenberg, Kelly Djahandari and Dan Sterne, "Infrastructure for Intrusion Detection and Response", DISCEX 2000, Jan. 25~27, 2000.

[9] CheckPoint, "SmartDefense: An Active Defense Solution", http://www.check-point.com/products/downloads/smartdefense_datasheet.pdf

[10] 손승원, "Active Security 기술 발전 전망", 정보처리학회 Sigcom Review Vol. 1, pp.95-107, March 1999.

[11] 방효찬 외 3인, 액티브 네트워크를 이용한 능동 보안 관리 프레임워크", Proc. of COMSW2002, pp200-303, July 2002.

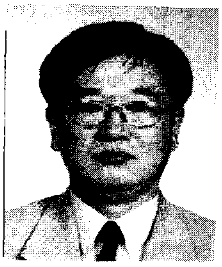


방 효 찬

1995년3월 : 북해도공업대학 경영공학과 졸업 1997년3월 : 북해도공업대학 기계시스템공학과 석사 졸업 1997년6월 ~ 1999년10월 : 한국통신 운용연구단 전임연구원 2000년8월 ~ 현재 : 한국전자통신연구원 능동보안기술연구팀 연구원 〈관심분야〉 네트워크보안, 액티브네트워크, 네트워크관리

나 중 찬

1986년 2월 : 충남대학교 계산통계학과 졸업 1989년 2월 : 숭실대학교 전자계산학과 석사 1998년 3월~현재 : 충남대학교 컴퓨터과학과 박사과정 1989년 2월~현재 : 한국전자통신연구원 능동보안기술연구팀 팀장 〈관심분야〉 네트워크 보안, 액티브 네트워크, 실시간 시스템



손 승 원

1984년 2월 : 경북대학교 전자공학과 졸업(공학사)
1994년 2월 : 연세대학교 전자공학과 졸업(공학석사)
1999년 2월 : 충북대학교 전자공학과 졸업(공학박사)
1991년 ~ 현재 : 한국전자통신연구원 네트워크보안연구부 부장/책임연구원
〈관심분야〉 네트워크 보안, 차세대 네트워크, Active Network

박 치 항

1974년 2월 : 서울대학교 응용물리학과 졸업(이학사)
1980년 2월 : 한국과학원 전자계산학과 졸업석사(공학석사) 1987년 12월 : 파리6대학 전자계산학과 졸업박사(공학박사) 1974년 2월 ~ 1978년 2월 : 한국과학기술연구소 1978년 2월 ~ 현재 : 한국전자통신연구원 정보보호연구본부 본부장/책임연구원 〈관심분야〉 정보보호, 멀티미디어, 차세대 네트워크