액티브 네트워크에서의 연합을 통한 보안 관리

(Security Management by Zone Combination in Active Networks)

장 범 환 † 김 동 수 †† 권 윤 주 ††† 남 택 용 †††† 정 태 명 †††††

(Beom-Hwan Chang) (Dong-Su Kim) (Yoon-Ju Kwon) (Taek-Yong Nam) (Tai-Myoung Chung)

요 약 인터넷은 개방 프로토콜의 영향으로 빠르게 성장하여 글로벌 네트워크 환경으로 진화하였지만, 많은 위협들로부터 자산을 보호해야하는 문제를 초래하게 되었다. 정보보호에 있어서, 조직 내 전체 보안시스템들을 완전 가동하여 사고 발생 이전에 침입을 차단하는 것은 최선책이지만, 사고 발생 이전 또는 새롭게 개발된 공격들을 차단하기는 대단히 어렵다. 보안연합은 신뢰할 수 있는 보안영역들간의 신속하고 정확한 보안 정보 교환과 긴밀한 상호 협력을 통해 잠재적인 공격들을 사전에 준비하여 대응할 수 있으며 새로운 보호 기능들을 능동적으로 갱신하여 보다 강력한 보안 기능과 신속하게 대응할 수 있는 구조이다.

키워드 : 액티브 네트워크, 통합 보안 관리, 보안영역 연합

Abstract The Internet has evolved into the global computer network due to the openness of its protocol, but such evolution brings about new risks and threats. To protect computer networks safely, it is the best way that preventing an attacker from intruding beforehand. However, to provision against all attacks causes the degradation of network performance as well as to prevent unknown attacks is very hard. Secure Combination, the framework which establishes a mutual collaboration and cooperation between the trusted zones, could protect systems from the potential attacks. This framework can predict attacks by exchanging security information and cooperating with each zone. It is a dynamic and powerful security architecture that rapidly enables updating security policy and deploying response modules.

Key words : Active Network, Integrated Security Management, Secure Zone Combination

1. 서 론

지금까지 컴퓨터 네트워크에 산재하고 있는 다양한 위협들과 공격들로부터 자원 및 정보를 보호하고자 많은 연구가 진행되어 오고 있다. 서비스와 시스템 자원에 대한 접근제어 기술, 사용자 인증 기술, 암호화 및 전자 서명 기술, 채널 암호화 기술, 네트워크/호스트/서비스 단위의 접근 제어와 통신 정책을 적용할 수 있는 침입차단시스템(Firewall), 악의적인 사용자나 침입 및 공격행위를 탐지하는 침입탐지시스템(IDS), 인터넷 웜이나 바이러스 프로그램들 제거하는 방역시스템, 그리고 신뢰되는 개체들간의 안전한 통신과 통신품질을 보장하기 위한 VPN 시스템 등 다양한 보안 기술과 시스템이 개발되어 그 성능이 향상되었고, 메커니즘 또한 점점 견고해지고 있다[1].

보안관리 활동은 분산된 여러 지점에서 개별 보안시스템들이 독립적으로 수행하기보다는 단일 관리지점에서 다양한 보안시스템들을 상호 유기적으로 연동시켜 일관성있게 관리하는 통합관리 방식이 효율적이다[2]. 하지만, 현재의 보안 문제를 근본적으로 해결할 수 있

† 학생회원 : 성균관대학교 전기전자컴퓨터공학과
bhchang@rtlab.skku.ac.kr
†† 비 회 원 : 성균관대학교 전기전자컴퓨터공학과
dskim@rtlab.skku.ac.kr
††† 비 회 원 : 한국과학기술정보연구원 슈퍼컴퓨팅센터 연구원
yulli@kisti.re.kr
†††† 비 회 원 : 한국전자통신연구원 정보보호연구본부 연구원
tynam@etri.re.kr
††††† 비 회 원 : 성균관대학교 정보통신공학부 교수
tmchung@ece.skku.ac.kr
논문접수 : 2002년 2월 2일
심사완료 : 2002년 11월 5일

는 방법은 아니다. 공격자들은 모든 공격 및 방어 가능성 중에서 단일 취약점 찾아 공격을 시도하거나 새로운 형태나 방법으로 공격을 시도한다. 이는 조직 내에 보유하고 있는 보안 시스템들을 완전 가동한다고 해도 완전한 대응이 불가능하다는 것을 의미한다.

구조적으로 컴퓨터 네트워크의 보안관리는 네트워크를 운영하는 각각의 조직 단위에서 조직의 영향력 하에 있는 도메인에 대해서만 감시 및 검사를 수행하는 관리가 주를 이루고 있다. 하지만, 자신들의 네트워크 내에 존재하는 시스템이 공격의 최종 목표지점은 아니더라도 중간기점이 되는 경우가 많으며, 자신의 네트워크에 대한 보안 취약점에 의해 타 조직의 네트워크 뿐만 아니라 결과적으로는 자신들의 네트워크의 피해로 이어지기도 한다. 이는 조직의 대외 이미지와 신뢰도라는 중요 자산에 대한 피해는 깊이 고려하지 못한 경우이다[3].

공격자들은 보통 해커 집단, 크래커 집단과 같이 특정 단체를 결성하거나 상호협력 하에 공격 목표를 장악하기도 한다[4]. 그들의 조직적인 공격 형태는 추적을 피하기 위해 다른 네트워크를 경유지점으로 사용하는 경우가 일반적이며, 한 네트워크의 피해는 곧 타 네트워크로의 피해로 이어지는 경우가 대부분이다. 따라서, 단일 관리 권한하의 네트워크 보안 관리로는 집단적인 공격 형태의 대응에는 역부족이며, 한 조직의 네트워크에 대한 보안 관리 책임을 그들 네트워크로 한정해서는 안되고 신뢰되는 타 네트워크의 보안에 대한 책임도 있는 것이다.

결과적으로, 현재와 같은 개방형 글로벌 네트워크 환경에서의 보안은 관리 능력의 부재나 보안 기술자의 부족, 보안 시스템들의 복잡성 등의 문제에도 원인이 있겠으나, 근본적으로 각 네트워크 단위들 간의 협력 체계가 거의 전무하다는 점에 그 원인이 있다. 이는 상호 협력 체계를 구축하기 위한 네트워크 하부 구조나 기반 기술의 부족으로 풀이된다. 능동 노드를 이용하여 네트워크 기능을 확장성있고 유연성있게 제공하는 액티브 네트워크 구조 및 기술은 보안시스템들의 능동적인 배치와 운용, 그리고 보안시스템들간의 상호 협력 가능한 보안 메커니즘을 구축할 수 있다.

보안연합체는 공격 정보, 예방 정보, 대응 정보 등의 보안 정보 교환을 통해 공격에 대한 면역력을 확산시킬 수 있는 네트워크 환경, 즉 신뢰되는 모든 네트워크 단위에서 사용자나 관리자가 개별 시스템 혹은 단위 네트워크에 대한 보안에 크게 신경을 쓰지 않고도 안전하게 전산 자원을 활용하거나 정보 교환을 할 수 있는 환경의 구축이다.

본 논문에서는 차세대 네트워크 기술인 액티브 네트워크를 이용한 보안 관리 구조와 이와 같은 환경 내에서 상호 협력을 통한 보안 정보의 전파 및 대응 기술에 대해서 논하고자 한다. 2장에서는 본 연구의 배경이 되는 통합보안관리와 액티브 네트워크의 개념 및 개요와 특징들에 대한 간략한 소개와 보안관리 현황에 대해 기술한다. 3장에서는 제안하는 보안 관리 구조 및 구성 요소들에 대해 기술한다. 4장과 5장에서는 보안 사건의 위험 단계 및 보안 정보 전파를 위한 프로토콜에 대해 설명하고, 6장에서는 대응 시나리오에 대한 이론적 분석을 언급하고자 한다. 마지막으로, 7장에서는 결론 및 향후 계획에 대해 기술한다.

2. 연구배경 및 보안관리 현황

인터넷을 통한 사이버 공격에 대해 각 보안 시스템들의 개별적인 대응은 다양한 형태의 공격을 발견하고 차단하기에는 한계가 있다. 또한, 언제, 어디서 발생할지 모르는 사이버 공격을 탐지하고자 조직 내의 전체 보안시스템들의 보안 기능을 완전(full) 가동시키거나, 또는 보호차원에서 네트워크 서비스 자체를 제한하고 차단하는 것은 네트워크 본연의 기능과 성능을 떨어뜨리는 원인이 된다.

통합보안관리는 이종의 다양한 보안 시스템들을 유기적으로 연동시키고 통합 운용 관리하여 사이버 공격에 종합적으로 대응할 수 있는 구조이다[2, 5, 6]. 하지만, 보안 관리 정책이 수동적이고 보안시스템들의 동적인 배치 및 활용이 불가능하여 보안시스템들의 느린 대응이 발생하고 이종의 보안 제품들 간의 연동 문제가 생겨난다. 또한, 공격 시기와 형태를 예견할 수 없어서, 즉 보안 사건과 사고의 감시 및 판단은 항상 단일 조직 내에서 이루어지기 때문에 조직 내 전체 보안시스템들은 언제나 모든 보안 기능을 가동하여 공격을 대비해야만 한다. 따라서, 능동적인 통합보안관리가 이루어지기 위해서는 상황에 맞게 보안시스템들의 기능을 변화시켜 운용·배치할 수 있고, 능동적인 정책을 생성 및 적용할 수 있는 기반 구조가 필요하다. 또한, 보안 정보 공유는 단일 조직만으로 국한시킬 것이 아니라 네트워크를 공유하고 있는 전체 조직으로 확산되어야 한다.

액티브 네트워크는 네트워크 및 서비스들에게 유연성과 능동성을 부여할 수 있다. 액티브 네트워크 기반의 보안관리는 앞서 기술한 것과 같은 통합보안관리 및 기존 보안관리 기술이 갖는 문제점, 즉 보안서비스

와 보안시스템의 능동적인 배치와 활용, 보안시스템간의 자율적 협력을 통한 공격 정보의 공유와 자동 대응 등과 같이 신속하고 효과적인 대응을 가능하게 한다. 본 논문은 액티브 네트워크 기술을 이용하여 보안시스템들의 능동적인 운용·배치와 보안 정보의 전파·공유가 가능한 네트워크 기반 구조에 대해 설명하고, 이를 통해 보안시스템들의 능동적인 통합보안관리를 제안하고자 한다[7, 8].

2.1 통합보안관리

통합보안관리는 다양한 보안시스템들, 예를 들면 네트워크/호스트/서비스 단위의 접근 제어와 통신 정책을 적용할 수 있는 침입차단시스템(Firewall), 악의적인 사용자나 침입 및 공격행위를 탐지하는 침입탐지시스템(IDS), 그리고 신뢰되는 개체들간의 안전한 통신과 통신품질을 보장하기 위한 VPN 시스템을 유기적으로 연관시켜 손쉽게 관리하고 종합적으로 공격에 대응하기 위한 구조이다. 이는 보안시스템들의 개별 대응에서 발생하는 중복 대응이나 연관 공격 대응 불가능과 같은 문제점, 그리고 분산된 보안시스템들의 복잡한 관리를 단일 관리지점으로 옮겨 중앙에서 효율적으로 관리할 수 있게 한다[2, 5, 6].

보안 시스템들은 분산된 여러 지점에서 독립적으로 수행·관리되기보다는 단일 관리지점에서 관리되는 중앙관리 방식이 효율적이다[2, 5]. 통합보안관리시스템의 장점으로는 다음과 같은 것이 있다.

① 보안정책의 전체적인 파악

관리자는 통합된 인터페이스를 통해 네트워크 전반에 걸친 보안정책을 한 눈에 파악할 수 있다. 각 보호시스템들의 정책에 문제점이 발생하였을 경우나, 정책의 수정이 필요한 경우에 관리자는 보안시스템들의 정책을 전체적으로 점검하여 문제가 발생할 수 있는 정책의 유무와 정책 수정에 따른 결과를 예측할 수 있다.

② 정책의 무결성 보장

전반적이며 통합적인 정책 검사에 의해 일차적으로 관리자의 판단으로 정책 무결성에 대한 검사를 할 수 있으며, 중앙 보안관리 서버가 제공하는 정책 무결성 점검기능을 통해서 다수의 보안시스템들 간의 정책 무결성을 보장할 수 있다.

③ 정책복구 용이

중앙에서 관리되는 보안정책은 마치 각 보안시스템들의 정책에 대한 사본 역할을 하여 보안시스템에 이상이 발생하였을 경우나, 여타 다른 이유로 보안시스템의 정책과 설정 정보가 손상되었을 경우, 중앙에서 관리되는 정책을 이용하여 문제가 발생한 보안시스템의 정책을 최근의 상태로 복구할 수 있다.

④ 정책 제어 기능의 확장

각 보안시스템들의 직접적인 제어를 수행하는 에이전트를 통해 정책설정 인자를 다양화시킬 수 있으며, 정책제어의 유연성과 확장성을 가져올 수 있다. 즉, 각 보안시스템들이 지원하는 정책설정인자 외에 에이전트가 제어할 수 있는 다른 정책제어항목을 추가하여 이 항목에 따라 정책을 제어할 수 있다.

⑤ 보안 도메인 형성

각 보안시스템들이 필요한 정보를 중앙 보안관리 서버를 통해 공유함으로써 보안서비스 활동에 필요한 경우, 이 정보를 능동적으로 요구하여 사용할 수 있다. 이러한 보안관리 정보의 공유를 통해 보안 도메인을 형성한다.

⑥ 보안관리의 자율성과 안전성 제공

보안관리자가 설정한 보안정책은 중앙 보안관리 서버에 의해 관리되며, 이 정책 정보와 보안정보는 각 보안시스템으로 분배된다. 중앙 보안관리 서버는 정책을 분배하기 전에 정책의 이상 유무, 무결성 등을 점검하여 관리자가 수행하여야 할 역할의 일부를 대행한다. 각 보안관리 에이전트는 보안 사건을 중앙 보안관리 서버에 통보하고, 중앙 보안관리 서버는 설정된 규칙에 따라 스스로 보안 사건에 대한 대응 동작을 수행한다. 즉, 보안 도메인 내의 보안 유지 활동이 자율성을 갖게 되고, 관리자의 개입을 최소화 할 수 있으며, 관리자의 실수에 의한 보안 피해를 최소화 할 수 있다.

이 외에도 관리비용 절감 등과 같은 다양한 편리성과 장점으로 인해 현재 보안시장은 보안시스템들의 보안성 향상과 성능개선, 기능확장이라는 영역과 이들 보안시스템들을 통합관리하는 통합보안관리 모델에 대한 영역이 주목받고 있다[9].

정책적으로 신뢰되는 외부영역은 신뢰 도메인(trusted domain)으로 정의할 수 있으며, 통합보안관리에 의해 직접적으로 관리되는 보안도메인은 신뢰 도메인과 안전한 채널을 이용하여 연결될 수 있다.

2.2 액티브 네트워크

액티브 네트워크[10, 11, 12]는 스위치나 라우터 내에 사용자의 접근을 허락하여 스위치의 컴퓨팅 능력을 이용할 수 있는 새로운 네트워크 구조에 대한 대안이다[13]. 네트워크는 기존 네트워크와 마찬가지로 스위치들과 호스트들로 구성되지만, 스위치는 프로그램 가능한 능동적인 속성을 포함하고 있는 액티브 노드이다. 결국, 사용자들에게는 단순 기능만을 수행하는 스위치의 속성은 숨기고 액티브 노드로만 구성된 가상

네트워크를 제공한다. 가상 네트워크 개념은 네트워크 중간 노드들을 변경하지 않고 신속히 새로운 네트워크 서비스의 제공과 개발을 가능하게 하고, 능동적으로 서비스들을 네트워크와 중간 노드 상에 배치하고 활용할 수 있게 한다[14, 15].

인터넷을 비롯한 현재 운용중인 대부분의 네트워크 구조는 그림 1에서 보는 바와 같이 네트워크 종단에 위치하여 다양한 서비스를 이용하는 컴퓨터(호스트)들과 이들을 연결하고 패킷 헤더 내용에 따라 단순히 패킷 전달 기능만을 수행하는 스위치 혹은 라우터들로 구성된다[14].

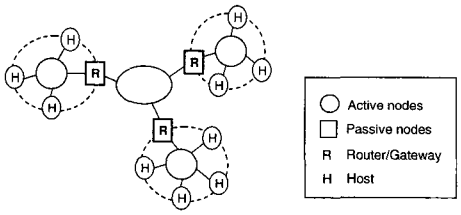

그림 1 전형적인 네트워크의 구조

네트워크 종단의 호스트들을 연결하고 있는 스위치나 라우터들이 단순한 패킷 전달 기능만을 수행한다고는 하지만 이들은 호스트 이상의 고속 연산과 강력한 컴퓨팅 능력을 가지고 있다. 그러나, 대부분의 스위치들은 자신의 컴퓨팅 능력을 단순한 패킷 전달에만 이용하고 있는 실정이며, 스위치에 새로운 기능을 추가하거나 그 기능을 네트워크에 반영하기 위해서는 모든 스위치 생산업체들의 지원과 관리자들의 수동작업, 즉 스위치 상에 동작하는 적절한 소프트웨어들을 선택 및 설치해야 한다[14].

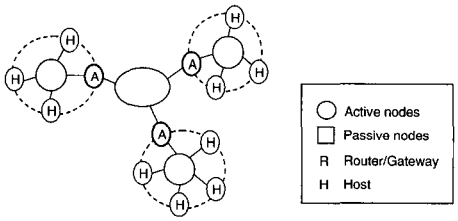

그림 2 액티브 네트워크의 구조

그림 2는 액티브 네트워크의 구조를 나타낸 것이다. 기존 네트워크에서 보안시스템들의 새로운 또는 추가적인 배치와 운용은 많은 시간과 경비를 필요로 한다. 예를 들면, 네트워크 중간 노드인 스위치나 라우터 내에 이종의 방화벽이나 VPN과 같은 보안 서비스를 제공하고 변경하기 위해서는 관리자가 소프트웨어들을 수동으로 설치해야만 한다. 이와 반대로, 스위치들이 액티브 노드로 구성된다면 관리자들은 수동적인 소프트웨어의 설치와 설정이 아닌, 소프트웨어의 다운로드를 통한 능동적인 변경과 구성이 가능하며 많은 다른 네트워크 응용 서비스들을 쉽게 제공할 수 있게 된다[10, 13, 14].

결과적으로, 액티브 네트워크는 네트워크에 프로그램 가능한 라우터나 스위치를 배치하여 전송되는 패킷들을 서비스 특성이나 사용자 요구에 따라 적합하게 연산(처리)할 수 있는 차세대 네트워크 구조에 대한 새로운 접근 방법으로써, 이에 대한 연구와 개발은 보안 관리뿐만 아니라 네트워크의 관리와 여러 네트워크 서비스의 개발 등 매우 다양하게 진행되고 있다[13, 15].

2.3 보안관리 현황 및 문제점

사이버 공격의 최근 특성 및 동향은 분산화, 에이전트화, 자동화, 은닉화, 협력화로 나타나고 있다. 이는 기존 보안시스템들의 개별적 방어로는 대응과 차단이 대단히 어렵고, 향후 발전하는 미래의 지능적 공격에 대해서는 단순한 통합보안관리로는 대응이 불가능하다. 따라서, 보안시스템들의 단순한 연관이나 연동이 아닌 보다 능동적이고 적극적인 새로운 보안 구조와 메커니즘에 대한 연구와 개발이 불가피한 실정이다.

① 기존의 정책기반 보안관리[3]와 통합보안관리 시스템에 있어서, 새로운 공격에 대응한다는 것은 거의 불가능하며 정책의 갱신과 변경은 수동적이기 때문에 최신 보안 정보에 따른 정책 유지와 대응은 대단히 어렵다. 그리고, 해당 공격에 대한 대응체계를 구축하기 위해서는 보안 시스템의 수동적인 재설치나 기능의 갱신이 필요하다.

새로운 공격에 대해 보안 정보 공유와 전파가 가능하고 보안시스템들의 능동적인 배치가 가능한 보안 구조, 그리고 보안 정책이나 보안시스템 자체의 변경과 갱신 등이 원활하게 이루어질 수 있는 기반 기술 및 하부 구조가 구축되어야 한다. 액티브 네트워크 기술은 네트워크 내의 능동적인 중간 노드들을 기반으로 보안시스템들의 능동적인 배치와 활용을 가능케 한다. 중앙관리시스템은 관리자의 개입없이 액티브 패킷을 이용한 보안 정책의 전파와 보안시스템 자체 모듈의 변경·갱신 등 기존 통합보안관리가 가지고 있던 수동적이고 느린 대응과 같은 문제점들을 해결할 수 있다.

② 사이버 공격의 특성은 앞서 지적하였듯이, 분산화, 에이전트화, 자동화, 은닉화, 협력화로 나타나고 있

다. 예를 들면, Trinoo와 같은 DDoS(Distri- buted Denial of Service) 공격이나 Nimda 바이러스 등은 이와 같은 특징을 뚜렷이 보여준다 [16, 17]. 이는 기존 보안시스템들의 개별적 방어로는 대응과 차단은 거의 불가능하며, 단일 조직 내의 보안시스템들을 이용한 기존 통합 대응도 많은 한계를 보여주고 있다. 이와 같이 향후 발전하는 예측 불가능한 지능적 공격에 대해 기존의 대응 방식들은 보안 관리의 관점을 단일 자신의 조직 내에 국한시킴으로써 스스로 신뢰 구간으로부터 고립된다. 즉, 자신의 조직에서 검출된 공격과 공격 시도를 포함한 보안 사건의 내용이나 대응 방법을 이웃 조직과 공유하지 못함으로 인해 전체 네트워크는 비신뢰 구간이 되고 결국, 자신의 네트워크도 공격의 대상이나 경유지가 되고 만다.

오늘의 보안관리는 하나의 개별 조직 내에서 보안시스템들을 연동시켜 운용하는 통합보안관리의 개념에서 벗어나 조직들 간에도 보안 정보의 공유와 전파 등과 같이 상호 협력을 바탕으로 한 관리 구조가 되어야 한다. 각각의 조직들이 상호 협력하여 공격 정보와 대응책을 제공 및 공유하는 고신뢰 네트워크 즉, 전역적인 보안연합체를 구축해야만 한다. 이는 국제적인 보안센터와 범국가적인 보안센터의 운영을 통해 보안 경고 발령과 대응책 배포, 그리고 각각의 조직 및 단체들은 보안 사건의 감시자(monitor) 역할들을 수행하고 보안 정보들을 보안센터에 보고하여 이웃 조직들과 공유하는 개념으로 이런 일련의 과정들이 자동으로 이루어지는 구조이다. 보안 정보를 수신한 해당 조직들은 협력적이고 통합적인 보안시스템 운영으로 향후 발전하는 사이버 공격을 사전에 막거나 피해를 최소한으로 줄일 수 있다.

③ 네트워크의 보안 강화를 목적으로 조직 내의 보안시스템들의 모든 보안 기능들을 완전 가동하는 것-예를 들면, 침해사고를 막고자 모든 보안 규칙을 적용하는 행위(실제로 모든 보안 규칙을 적용하는 것은 타당하지만 현실적으로 불가능하다), 침입을 탐지하고자 조직 내에 유입·유출되는 모든 패킷과 패턴을 감시하는 행위, 악성 코드를 검사하는 행위 등-과 취약점이 알려진 서비스의 제한은 네트워크의 전반적인 성능 저하를 야기하고 매우 비효율적이다. 하지만, 네트워크의 성능을 높이고 다양한 서비스를 제공하고자 네트워크 자체의 안전을 무시할 수는 없는 현실이다. 즉, 이 둘은 모순(trade-off) 관계가 있으며, 어느 선에서 절충을 취해야만 한다. 사전에 공격 정보를 입수할 수 있다면, 평시에는 보안시스템들의 기본적인 보안 기능만을 유지하고, 인지된 공격에 대해 대비, 즉 공격의 수준에 따라 적절하게 보안시스템들을 운용하면 네트워크의 성능과 안전, 양쪽 모두를 향상시킬 수 있다.

④ 보안 관리에 있어서 최선의 대응책은 공격 이전에 해당 공격을 대비하고 차단하는 것이다. 하지만, 지속적인 네트워크 서비스의 개발과 안전 장치의 추가와 더불어 공격자들은 새로운 공격 메커니즘을 개발하고 발전시켜 오고 있다. 이와 같이 공격과 방어는 모순관계처럼 양립하고 있으며, 공격자들은 방어가 허술한 틈새로 공격을 시도한다. 결국, 방어의 완벽한 구조는 없기 때문에 사후 조치로써 사이버 공격자들에 대한 역추적(traceback) 기능은 보안 관리에 있어서 반드시 필요하다. 기존 네트워크의 구조와 보안관리에서는 로그 파일에 의존하는 수동적인 추적 기능만이 가능하였지만, 로그파일 역시 공격자들의 조작에 의해 변경된다면, 추적은 포기해야 한다. 그러나, 보안연합체 개념은 사이버 공격자들에 대한 역추적 기능을 제공하기에도 매우 용이한 구조가 될 것이다.

3. 보안연합

일반적인 상황에서 모든 악의적인 행동을 검출하고자 조직 내 모든 보안시스템의 전 기능을 가동시키는 것은 네트워크의 보안을 강화시킬 수는 있겠지만 성능면에서 매우 비효율적이다. 예를 들면, 알려지지 않은 악의적인 행동은 모든 패킷을 감사한다고 해도 검출하기는 매우 어려우며, 네트워크 자원을 많이 소모하는 DoS나 DDoS 공격일 경우에 자원의 낭비는 더욱 심하게 된다. 그러나, 해당 공격을 사전에 인지하여 패킷을 필터링하거나, 더 나아가 근원지 네트워크에서 공격을 차단하면 네트워크 공유자원을 소비하지 않기 때문에 매우 효율적이다. 또한, 공격 특성상 DDoS 공격은 공격하는 지점들보다 공격받는 지점에서 공격을 검출하기가 용이하기 때문에 공격하는 지점—DDoS 공격에서 공격을 개시하는 지점도 이미 공격을 당한 경유지로 볼 수 있다—의 관리자에게 공격하고 있는 사실이 통지된다면 네트워크를 관리하는 측면에서 매우 유용할 것이다. 보안연합(Security Combination)은 이와 같은 보안 정보를 보안영역간에 상호 교환하고 협력하는 고신뢰 네트워크 영역들의 집합을 의미한다.

3.1 보안영역과 구성요소

보안영역(Zone)이란, 보안시스템들을 통합적으로 운용, 관리할 수 있는 ZK(Zone Keeper)와 접근 정책 적용이 가능한 보안 게이트웨이(SG: Secure Gateway), 보안 사건의 탐지 및 차단이 가능한 시스템 등이 운영

되는 논리 영역이다. 즉, Zone은 기본적인 접근 제어와 보안 사건 탐지를 수행하는 보안 시스템이 운영되고 자체적으로 보안 사건에 대해 대응이 가능한 논리적 영역 집합으로 정의된다. 그리고, 보안 연합은 보안 영역들과 계층적인 보안센터(GZ: Gazette)들의 논리적인 집합으로 구성된다.

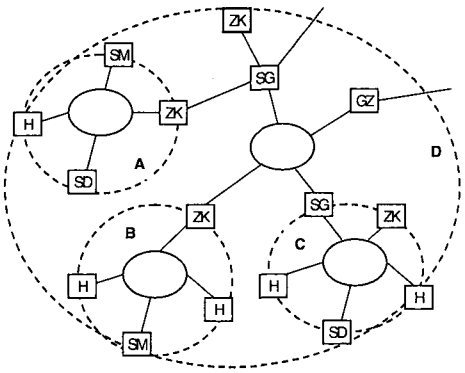

그림 3 보안영역(Zone)의 구조

Zone은 정책기반 네트워크 관리나 X.500에서 언급하고 있는 디렉토리 또는 도메인[3, 18]과 매우 유사한 개념으로 볼 수 있으나, 도메인이 관리 정책을 정의하기 위한 객체들의 그룹인 반면, Zone은 하나의 보안시스템, 즉 ZK가 다른 보안시스템들을 제어·운용할 수 있는 관리 영역을 의미한다.

그림 3은 Zone의 구조를 나타낸 것이다. 대등한 수준의 Zone들은 중복(overlap)되지 않으며 독립관계를 유지하고, 수직 관계에 있는 Zone들간에는 포함관계로 이루어진다. 그림 3에서 A, B, C는 전자의 경우이고, D는 A, B, C를 포함하는 후자의 경우이다. 각 Zone들은 대표되는 하나의 ZK(Zone Keeper)를 통해 식별되며, ZK는 자신이 관리하는 Zone이 항상 안전한 상태로 유지될 수 있도록 보안시스템들을 조율하고 운용하는 역할을 한다. Zone을 구성하는 요소들은 표 1과 같으며 크게 ZK, GZ, 보안시스템들로 구성된다.

구성 요소들 중에서 ZK과 GZ은 반드시 액티브 노드 상에 구현·운영되어야 하고, 다른 보안 시스템들은 액티브 노드 기반의 운영이 필수 사항은 아니다. 하지만, 보다 능동적인 보안관리, 즉 능동적인 보안시스템들의 배치 및 활용을 위해서는 모든 보안 구성 요소들이 액티브 노드 상에 구현·운영되어야 한다. 예를 들면, ZK는 현재의 보안 상황과 정보를 고려하여 보안시스템의 재설치, 정책 적용 및 갱신, 기능 변경 및 추가 등을 수행해야 하기 때문이다. 실제로 대부분의 보안 시스템들은 응용계층의 프로그램들로서 액티브 노드 기반에서 동작들을 수행하고 있다. 단지 기반 구조가 액티브 네트워크 요소인 NodeOS와 EE(Execution Environment) 요건을 전부 만족시키지 못하는 상태이지만, 보안시스템들이 EE와 같은 실행 환경 내에서 동작 및 변경 가능하도록 재작성되면 된다.

표 1 Zone의 구성 요소들

구성요소		기 능 설 명	예
Zone Keeper		Zone 내의 보안 사건을 수집하고 Zone의 보안 상태를 결정하는 기능과 Zone 내의 전체적인 보안 정책을 판단하고 배포하는 기능을 수행한다.	없음
		보안 사건을 수집하고 정해진 정책에 따라 보안 시스템들을 통합적으로 운용, 관리한다.	ESM
Gazette		보안 경고 수준을 발령하거나 수정, 패치, 업데이트를 주관하는 국가 혹은 사회적, 공식적으로 인정받은 조직(단체)에서 운영하는 보안 시스템	없음
보안시스템	SecureGateway	Zone 내의 시스템/서비스들에 대한 접근 제어 기능을 수행	FW IDS VPN
	Secure Monitor	Zone 내의 보안 사건들을 감시하는 기능을 수행	FW IDS
	Secure Doctor	Zone 내의 보안 사건들에 대해 방역 기능을 수행	Vaccine

ZK는 빠른 대응과 제어를 위해 SG나 SM(Secure Monitor)과 같은 보안 시스템의 기능을 부가적으로 노드 내에 함께 가질 수도 있다. 예를 들면, 보안 위협 사건을 감지하는 모니터링 기능, 모니터링 결과를 반영할 수 있는 네트워크 제어 기능, 네트워크 제어 시스템에서 각 공격형태에 따라 대응할 수 있는 대응 기능들을 포함할 수 있다.

3.2 보안센터

보안센터(GZ: Gazette)는 국가 혹은 각각의 단체에서 공식적으로 운영하는 보안시스템으로서 ZK에 대해 보안 경고 발령과 대응책 배포를 담당한다. 이는 ZK로부터 수신한 보안 사건들을 통합, 분석하여 대응책을 마련하고 배포함으로써 사이버 공격을 각 Zone들이 사전에 대응할 수 있도록 하는 것이다. GZ는 계층적인 구조를 이루며, 최상위 GZ는 범국가적으로 운영되는 GZ이며, 다음 단계는 각각의 국가 혹은 공인 단체에서 운영하는 GZ으로 구성될 수 있다. GZ은 하나

의 Zone에 포함될 수도 있고, 포함되지 않을 수도 있다. 다시 말하면, GZ은 Zone을 구성하는데 반드시 필요한 구성요소는 아니다.

3.3 보안 연합

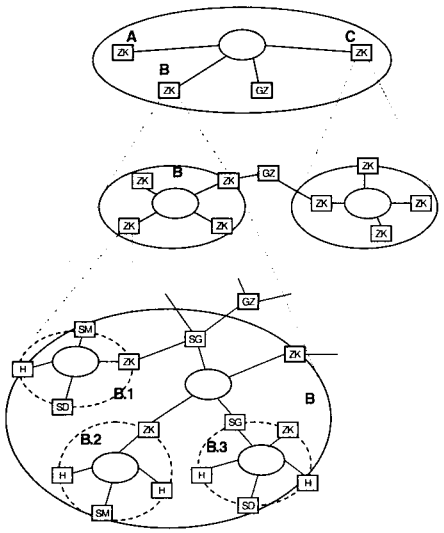

그림 4 보안 연합

보안연합은 보안영역들과 GZ들의 계층적인 논리 집합으로 구성된다. 그림 4는 보안연합을 계층적인 보안영역들의 그룹으로 나타낸 것이다.

각각의 Zone에서 탐지된 보안 사건과 정보들은 이웃 ZK, GZ과 상위 ZK, GZ으로 전달되고, 각 ZK은 자신의 Zone에 설정된 정책에 따라 보안시스템을 조율하여 가동시키고 이웃 ZK들과 상호 협력하여 사이버 공격에 대해 빠르게 대응한다. 각각의 Zone은 자신의 영역으로부터 시작되는 악의적인 행동에 대해 책임이 있으며 이웃 ZK로부터 문제 상황을 제공받을 수 있다.

4. 보안경고수준

보안경고수준(SAL: Security Alert Level)은 GZ나 공격 징후를 탐지한 ZK에 의해 발령된다. 보안 경고수준의 구분은 위험도에 따른 상하의 수직 관계가 아니라, 공격 징후에 대한 대응 행동들을 명시하기 위한 것이다. 따라서, 보안경고수준에 따라 각각의 조직이나 단체마다 위험을 판단하는 수위가 다를 수 있고 대응 행태도 틀릴 수 있다. 다시 말해서, 보안경고수준은 전적으로 각 보안관리 단위 영역에서 주관적으로 판단 및 적용된다.

보안 경고 수준은 하나의 Zone과 관련된 공격 근원지와 공격 대상 시스템의 관계를 기반으로 분류되고, 현재 발견된 보안 사건 정보로부터 얻어지는 공격 근원지와 공격 대상의 수에 따른 사상(mapping) 관계에 의해 그림 5와 같이 1:1, 1:N, N:1, N:N으로 정의된다.

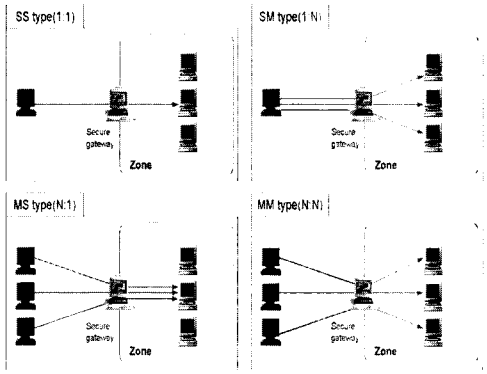

그림 5 보안 경고 수준

Zone 개념을 이용한 보안 모델에서는 공격 근원지와 공격 대상의 관계에서 1:N 관계보다 N:1 관계가 상대적으로 위험한 상태로 정의된다. 그 이유는 N:1의 공격 유형에서 상대적으로 낮은 가능성을 갖는 우연성을 배제한다면, 다수의 협력관계에 있는 공격자들이 명시적인 목적으로 갖고 계획적으로 공격을 실행 중인 경우로 판단되기 때문이다. 그리고, 각 공격 유형별로 세부 경고 수준이 정의되는데, 세부 경고 수준은 현재 단일 시스템을 대상으로 진행중인 공격이 타 시스템에게 보안과 관계된 영향을 줄 수 있는가에 의하여 구분된다. 즉, 이는 현재 진행중인 공격이 공격 대상 시스템의 피해를 넘어 인근 시스템 혹은 공격대상 시스템이 속한 네트워크 혹은 Zone으로 정의되는 관리대상 영역, 나아가 조직이 운영하고 있는 네트워크 전반으로 피해가 확산될 가능성이 있는 경우는 '심각함(high)'으로, 그렇지 않고 타 시스템으로의 확산 가능성이 없는 경우에는 '경미함(low)'으로 정의된다. 타 시스템으로의 피해 확장 여부에 관한 평가는 현재 진행되고 있는 공격 유형에 대한 정확한 판단과 함께, 해당 공격유형에 대한 타 시스템들(아직 공격 대상이 되지 않은 시스템들)의 방어 준비(공격에 대한 내성 혹은 취약성에 대한 패치 등) 정도에 대한 평가를 바탕으로 결정된다.

탐지된 공격에 의한 피해 범위가 단일 시스템이나

현재 공격 대상 시스템들로 국한되는 경우 즉, 세부 SAL이 '경미함(low)'의 경우, 명시적인 공격 근원지와 공격 대상 시스템들을 보안 정책 인자에 포함시키는 명시적인(explicit) 대응 조치를 취한다. 이 경우는 공격에 대해 방어 행위를 수행하여야 하는 대상이 명확히 결정되므로 상대적으로 확실하고 신속한 대응이 이루어질 수 있다. 한편, 공격 대상 시스템이 조직의 업무 수행이나 서비스 제공에 크게 중요하지 않은 경우, 물리적으로 네트워크 접속을 차단시킴으로써 공격 진행을 막을 수도 있다. 이와 같은 경미한 보안 사건이 발생한 경우, 최소한으로 요구되는 보안 대책을 수행하여 과잉 대응을 방지함으로써 대응 정책의 적용에 드는 자원과 비용 문제를 고려한 효율성을 얻어야 한다. 즉, 요구되는 수준을 넘어서 적용되는 대응 조치 및 보안 정책은 타 서비스의 가용성에 영향을 주거나 사용자의 편의성을 저하시키며, 보안 시스템의 성능, 네트워크의 품질을 저하시키는 등의 비효율성을 초래할 수 있기 때문이다.

탐지된 공격에 의한 피해가 다른 시스템으로 확장될 가능성이 존재하는 경우 즉, 세부 SAL이 '심각함(high)'의 경우, 피해 확산을 방지하기 위해서 공격 근원지로부터 Zone 전체에 대한 접근 제어 정책을 적용하는 것과 같이, Zone 전체를 대상으로 하는 포괄적(comprehensive) 대응 조치가 취해져야 한다. 예를 들면, 심각한 취약성을 내포하고 있는 서비스나 호스트에 대한 공격 또는 상당한 피해 파급효과를 가진 공격이 진행되고 있는 경우, 그리고 민감한 정보들을 저장 및 처리하는 시스템이 공격받고 있는 경우, 보안 게이트웨이(Secure Gateway)는 연관된 서비스들이나 호스트들에 대한 외부 접촉을 전면적으로 차단하여 더 큰 재난을 막아야 한다.

표 2는 SAL의 세부적인 구분과 그에 대한 설명 및 각각 구분된 SAL 유형에 따른 대응 형태를 나타낸 것이다. 네트워크/호스트에서 별다른 사건이 보고되지 않고 안전한 상태라고 판단되는 CLR의 경우 이에 대한 대응 활동은 일반적인 관리 및 취약성 점검, 공격 유형, 바이러스 정보 갱신 등의 유지보수 활동이 주가 되며, 수상한 사건이 발견되었으나 뚜렷한 공격 징후가 없는 SPS의 경우에는 보안 감시활동, 취약성에 대한 점검 강화 등 그 감시 강도를 높이는 대응 수단을 적용한다.

SAL의 세부 유형 중 현재 감지된 공격의 예상 파급이 경미한 경우에는 여타 서비스나 네트워크 접근의 방해를 최소화하기 위해 명시적인 근원지 혹은 근원지 집단으로부터 명시적인 공격 대상에 대한 접근만을 통제한다. 이는 적절한 수준으로 대응하여 보안 정책에

표 2 보안 경고 수준(SAL)

단계	정 의	대 응
CLR	비교적 안전한 상태이다. Zone 내에서 특별한 공격징후나 수상한 행위가 발견되지 않는 상태이다.	취약성 점검 및 일반관리 활동 수행
SPS	명확한 공격이라 판단되는 행위는 없으나 평소와는 다른 특이하거나 의심이 가는 활동이 감지된 상태이다.	보안 감시활동 강화
SSL	단일 근원지에 의한 단일 대상에 대한 공격이 탐지되었으며, 다른 시스템으로의 피해 가능성은 없는 상태이다.	해당 근원지로부터 대상 시스템으로의 접근 통제, 블랙리스트 갱신
SSH	단일 근원지에 의한 단일 대상에 대한 공격이 탐지되었으며, 다른 시스템으로의 피해가 예상되는 상태이다.	해당 근원지로부터 Zone으로의 접근 통제, 블랙리스트 갱신
SML	단일 근원지에 의한 다수 대상에 대한 공격 징후가 탐지되었으며, 다른 시스템으로의 피해 가능성은 없는 상태이다.	해당 근원지로부터 대상 시스템들로의 접근 통제, 블랙리스트 갱신
SMH	단일 근원지에 의한 다수 대상에 대한 공격 징후가 탐지되었으며, 다른 시스템으로의 피해가 예상되는 상태이다.	해당 근원지로부터 Zone으로의 접근 통제, 블랙리스트 갱신
MSL	다수 근원지에 의한 단일 대상에 대한 공격이 탐지되었으며, 다른 시스템으로의 피해 가능성은 없는 상태이다.	다수 근원지로부터 대상 시스템으로의 접근 통제, 블랙리스트 갱신
MSH	다수 근원지에 의한 단일 대상에 대한 공격이 탐지되었으며, 다른 시스템으로의 피해가 예상되는 상태이다.	다수 근원지로부터 Zone으로의 접근 통제, 블랙리스트 갱신
MML	다수 근원지에 의한 다수 대상에 대한 공격 징후가 탐지되었으며, 다른 시스템에 대한 피해 가능성은 없는 상태이다.	다수 근원지로부터 대상 시스템들로의 접근 통제, 블랙리스트 갱신
MMH	다수 근원지에 의한 다수 대상에 대한 공격 징후가 탐지되었으며, 이후 피해가 Zone 전체로 확장될 가능성이 있는 상태이다.	다수 근원지로부터 Zone으로의 접근 통제, 블랙리스트 갱신

의한 서비스나 네트워크 품질에 미치는 영향을 최소화하기 위함이다. 예상되는 파급효과가 심각한 경우에는 Zone 전체에 대한 보호를 위해 명시적인 목적지 혹은 다수 목적지 집단에서 Zone에 대한 접근을 통제한다. 이 경우에는 서비스나 네트워크 품질에 어느 정도 영향이 미치더라도 Zone 영역에 대한 보안이 우선 시 되는 경우이므로 최대한의 대응 정책을 적용하는 것이다.

ZK에 의한 SAL의 발령은 새로운 보안 사건(security event)이 감시 시스템에 의해 발견되고 ZK가 이러한 사건을 보고 받은 경우에 이루어진다. 한편, GZ에 의한 SAL의 발령은 새로운 유형의 공격 형태가 발견되었거나 새로운 형태의 바이러스 혹은 웜이 발견되어 확산되고 있는 경우 등 전역적인 보안 사건 혹은 징후가 나타난 경우에 GZ은 각 ZK에 이런 정보를 알리는 형태로 진행된다. GZ에 의해 이러한 정보를 수신한 ZK는 실제적인 공격 징후가 보이지 않더라도 Zone의 SAL을 SPS로 발령하여 예상되는 보안 사건에 대한 대비를 함으로써 경계와 보안을 강화할 수 있다. 즉, 탐지시스템에 대해 새로운 공격 유형 정보를 입력하고 바이러스나 인터넷 웜에 대응할 수 있도록 진단 및 치료 시스템의 정보를 갱신하는 등의 대응 활동을 수행한다.

SAL은 해당 공격 징후에 대한 적절한 대응조치가 취해진 경우(주로 보안 정책, 접근 정책의 갱신 혹은 취약성에 대한 패치, 수정이 이루어진 경우이다), ZK에 의해 CLR 수준으로 되돌아 갈 수 있다. 또한, ZK는 탐지된 보안 사건들에 대한 정보를 사건 전파 정책에 따라 인근 Zone으로 전달하며, 이러한 정보를 수신한 인근 Zone의 ZK들은 공격 가능성에 대한 대응 활동을 수행하거나 만약, 이들 정보로부터 공격이 자신이 담당하는 Zone을 경유하는 공격인 경우 이를 분석하여 자신의 Zone에서 취할 수 있는 접근 통제를 수행하고 이에 대한 보안 책임을 지게 된다.

5. 보안영역 정보 프로토콜

ZK는 상호 간에 정보를 교환하면서 각각 자신의 Zone들을 안전한 영역으로 유지한다. 이때 Zone 간에 교환 또는 배포되는 정보 중에서 보안 협력 정책을 보안영역 정책(Zone Policy)이라고 한다. Zone Policy는 보안영역 정보 프로토콜(ZIP: Zone Information Protocol)을 이용하여 정책 정보를 교환함으로써 Zone 간에 상호 의견 교환을 수행한다.

5.1 보안영역 정책

보안영역 정책(Zone Policy)이란 자신의 Zone의 관리 체제에 영향을 끼치는 정보로서 접근 제어 또는 자원 관리의 측면에서 사용된다. 정책의 배포는 각각의 Zone Keeper들이 담당하게 되는데, Zone Keeper는 모니터링 시스템으로부터의 이벤트를 감지하고 그에 대한 대응으로써, 상대 Zone으로 정책를 전파하기도 하고, 자신의 Zone에 정책을 적용시키기 위해서 네트워크 제어 시스템으로 정책을 배포하기도 한다. 이와 같이, Zone Policy는 Zone의 안전한 상태를 유지하기 위한 행위의 지표이며, Zone 간의 협력을 도모하기 위해 상호 교환하는 보안 정보와 행위로 구체화된다. Zone Keeper는 자신의 Zone에서 발생한 공격에 대한 정보 즉, Zone Policy를 신뢰관계에 있는 모든 Zone으로 전달함으로써 연대관계에 있는 Zone들이 돌발적이거나 지속적인 사이버테러에 대해 공동으로 대처할 수 있도록 한다.

Zone Policy는 대등 관계의 영역(sibling Zone) 간에 적용될 수 있는 Cooperation Policy, 영역 내부 의 보안시스템들을 제어하고 관리하기 위해 사용하는 Coordination Policy, 그리고 상·하위 즉, 포함 관계의 영역 사이에 적용될 수 있는 Propagation Policy로 구분된다.

Cooperation Policy : $ZK \leftrightarrow ZK$

이웃 ZK에 도움을 요청하거나 또는 자신의 Zone에서 발생한 이벤트에 대해서 상대 ZK에 정보를 주기 위해서 사용되는 정책으로 강제력은 없으나, Zone 간의 협력관계를 유지하여 사이버공격에 대한 안전성을 유지하기 위해 사용되는 정책

Coordination Policy : $ZK \leftrightarrow SS$

Zone 내부의 보안 시스템들이나 하위 ZK들이 수행해야 할 행위를 전달하기 위해서 사용하는 정책으로서 내부 보안시스템들이 외부에서 발생한 보안 사건에 대해 대비하고, 하위 Zone으로 이를 전달하기 위해 사용한다.

Propagation Policy : $GZ \leftrightarrow ZK$

GZ에서 실시간적인 보안 경고와 보안 소식(행동)들을 ZK들로 전파하기 위해 사용한다. 수신한 ZK들은 각 조직에 맞는 대응 정책들을 이용하여 공격을 대비할 수 있다.

5.2 보안영역 정보 프로토콜

보안영역 정보 프로토콜(ZIP : Zone Information Protocol)은 Zone 간의 정책 정보 교환을 위한 프로토콜이다. Zone Policy는 신뢰관계에 있는 Zone의 관리 체제에 영향을 미치는 정보이기 때문에 안전한 통신채

널을 통하여 전달되어야만 한다.

통신을 하고자 하는 두 개체 사이의 메시지 보안을 위해서는 트랜젝션 보안 메커니즘(TSM: Transaction Security Mechanism)이 필요하다[19]. TSM의 표준화된 프로토콜로는 IPSec, SSL(Secure SocketLayer) 등이 있으며, 비 표준적 방법으로는 응용프로그램의 특성에 적합하도록 통신을 하고자 하는 두 개체 사이에 세션키를 생성 및 분배하여 세션 단위로 통신을 보호하는 방법이 있다[20]. 세션키를 이용하는 메커니즘은 응용프로그램의 특성에 따라 설계자의 입장에서 암호화 메커니즘이나 키 분배 메커니즘을 결정하여 사용할 수 있다.

메시지의 보호를 위해 표준적인 프로토콜을 따르는 목적은 호환성을 보장하기 위함이다. 호환성을 보장하는 다른 방식으로는 응용프로그램의 통신 기반 구조에 접목될 수 있는 통신 API를 제공함으로써 얻어질 수 있다. 전자의 경우 다양한 환경을 고려하여 설계된 이유로 호환성이 보장되는 반면 overhead가 따르며, 후자의 경우는 호환성이 상대적으로 떨어지지만 응용프로그램의 특성에 최적화된 프로토콜의 설계가 가능하다.

어떤 트랜젝션 보안 메커니즘을 사용하던 간에 필수적으로 필요한 것은 공개키 기반구조(PKI: Public Key Infrastructure)이다. 왜냐하면, 트랜젝션 보안을 위한 키 분배는 공개키를 이용한 방법이 보편적이고, PKI는 다양한 개체들이 공개키를 이용하여 상호 인증, 메시지 암호화 및 무결성 보장이 가능하도록 하는 표준적인 구조이기 때문이다. PKI에서 중심이 되는 역할은 각 개체들의 신뢰성을 보증하고 인증서를 발급하는 제삼의 신뢰되는 개체, 즉 인증기관(CA: Certification Authority)이다[21].

본 논문에서 제시하는 Zone System은 서로 신뢰되는 개체들의 안전한 통신을 위해 PKI를 이용한다. 단일 Zone 내부의 보안시스템 사이의 CA 역할은 ZK가 담당하며, ZK간의 CA 역할은 GZ가 담당한다. 그리고, 최상위 CA의 역할은 최상위 GZ가 담당한다. 즉, ZK에 대한 인증서 발행 및 신뢰성 보증은 GZ의 책임이다. Zone System에서 보안 통신 과정을 간략하게 요약하면, 송신자는 통신 개시 전에 무작위 세션 키를 생성하여 PKI 메커니즘을 통해 세션키를 상대방에게 분배한다. 이후, 해당 세션동안 메시지들은 이 세션키를 통해 대칭키 암호화 방식을 이용해 보호된다[21].

ZIP 메시지는 정책에 따라 네 가지 종류가 있으며, 그림 6에서 보는 바와 같이 메시지 헤더와 페이로드로 구성된다. ZIP 메시지 헤더는 모든 메시지에 포함되고,

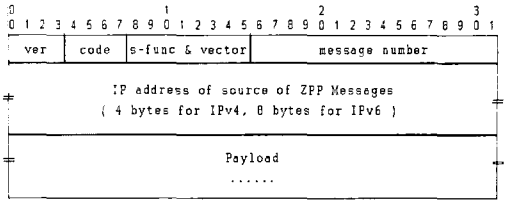

그림 6 ZIP 메시지 헤더 구조

그 요소들로는 프로토콜 버전, 메시지 종류(정책 유형), 메시지를 생성한 ZK 또는 GZ 지시자(s-func & vector), 그리고 메시지 식별자가 있다. 페이로드 필드는 메시지 종류에 따라 다양하다. 예를 들면, 현재 감지된 공격의 경고 수준, 이웃 ZK에 요청하는 행동, 공격에 대한 대응방안으로써 실행되어야 할 프로그램이 있다면 그 프로그램의 실행코드, 그리고 하위 보안 시스템들에게 전달할 추가 정보들을 포함하게 된다. 각 필드에 대한 설명은 아래와 같다.

Common Header

필 드	설 명
Version	ZIP 버전 식별자 (초기값은 0)
P.T (Policy Type)	정책 유형 0 Cooperation Policy 1 Coordination Policy 2 Propagation Policy
s func & vector	GZ 또는 ZK 지시자 (보안 모듈 식별 번호와 벡터 값)
Msg Number	메시지 번호 메시지에 대한 식별자
Source Address	메시지를 생성한 주체의 IP 주소

Propagation Policy Payload (GZ ↔ ZK)

필 드	설 명
Alert Level	현재 감지된 공격의 경고 수준
Required Action	GZ에서 요청하는 행위 0 download 1 update
Executable Code	각 Zone Keeper들은 자신이 공격받은 것에 대한 대응 프로그램이나 검사 프로그램을 넣어 보낼 수 있다. 이러한 경우 자신의 정책 데이타베이스에는 아직 등록되어 있지 않은 백신이라던가 패치 프로그램 등이 포함될 수 있다.

Cooperation Policy Payload (ZK ↔ ZK)

필 드	설 명
A.T: Attack Type	공격 유형 식별자 현재 감지된 공격 형태나 징후
Attacked Point	공격 대상 지점 - 현재 공격을 받은 지점의 IP 주소
Attacker Point	공격 주체 지점 현재 공격을 진행하고 있는 지점의 IP 주소
T.S: Timestamp	리플레이 공격을 방지하기 위한 시점을 제공하기 위해 사용
Required Action	상대방 Zone에서 요청하는 행위
Executable Code	각 Zone Keeper들은 자신이 공격받은 것에 대한 대응 프로그램이나 검사 프로그램을 넣어 보낼 수 있다. 예를 들면, 자신의 정책 데이타베이스에는 아직 등록되어 있지 않은 백신이라던가 패치 프로그램 등이 포함될 수 있다.

Coordination Policy Payload (ZK ↔ SS)

필 드	설 명
Required Action	ZK에서 요청하는 행위로서, 보안 시스템의 실질적인 행위가 기술된다. 현재는 다음의 6가지 행위로 분류된다. 0 accept SG로 분배 1 reject SG로 분배 2 check(detect) SD로 분배 3 authenticate IPSec으로 분배 4 encrypt IPSec으로 분배 5 execute - 호스트 또는 바이러스 치료 서버로 분배 현재 배포하는 실행코드를 실행
Executable Code	각 Zone Keeper들은 자신이 공격받은 것에 대한 대응 프로그램이나 검사 프로그램을 넣어 보낼 수 있다. 이러한 경우 자신의 정책 데이타베이스에는 아직 등록되어 있지 않은 백신이라던가 패치 프로그램 등이 포함될 수 있다.
Specific Policy	해당 보안 시스템이 정책 설정시 필요한 정책 요소들 ex) FW, IDS 근원지,목적지,대상서비스(FTP, Telnet)/대상공격/치료모듈,추가정보

6. 보안영역의 대응 구조

Zone들은 보안 정책을 이용한 협력구조를 통하여 어떤 공격에 대해 지역 압박(Zone Press) 형태를 구축할 수 있다. 지역 방어라는 것은 공격에 대한 근원지 원천 봉쇄인 외부 영역 압박(Outer Zone Press)과 내부 영역의 보호를 위한 내부 영역 압박(Inner Zone Press)을 의미한다. 다시 말하면, 한 Zone에서 다중 근원지로부터 공격을 받았을 때, 그러한 공격에 대한 방어를 자신의 제어시스템의 책임과 함께 공격 근원지의 ZK들에게 해당 호스트에 대한 제어를 요청하는 것이다. 특히, 공격의 근원지에 대한 제어를 함으로써 자신의 Zone을 안전한 영역으로 만드는 것 뿐만 아니라 공격자 역추적 및 다른 Zone으로의 공격 확산 가능성을 제거함으로써 다른 영역의 안전성까지 추구할 수 있다.

ZK가 어떤 공격을 감지하거나 GZ에 의해 경고 레벨이 발령되면, ZK는 공격에 대응하는 Coordination 정책을 내부 보안시스템들에 배포하여 Inner Zone Press를 취하고, 다른 ZK에게는 협력을 요청하는 Cooperation 정책을 보낸다. Cooperation 정책을 받은 ZK는 정책의 내용에 따라 하위 Zone 또는 동급 Zone으로 정책을 보낼 수 있다. 만약 그 공격의 근원지를 알 수 있다면 그 근원지 혹은 근원지로 판단되는 지점의 ZK에게 패킷 필터링과 같은 적절한 조치를 취할 것을 요청한다. 이와 같이, 각각 서로 다른 형태의 Cooperation 정책을 통한 Outer Zone Press는 독립 Zone 간에 협력을 요청하거나 자신이 받은 공격을 리포팅함으로써 상대 Zone은 정책이나 공격에 대하여 능동적으로 대처할 수 있다.

Zone 간의 협력 구조는 바이러스 같이 쉽게 전염되는 공격이나 분산 환경의 서비스거부 공격 등에 대해서 빠르게 대처할 수 있다. 각 Zone은 대응기술 데이타베이스를 통해서 보고된 바이러스에 대한 백신을 이용하여 방역을 하거나, 백신이 갖추어져 있지 않은 경우에는 GZ이나 다른 ZK로부터 전달받음으로써 공격의 보고뿐만 아니라 그 해결책에 대해서도 협력을 가질 수 있다.

6.1 DDoS: 분산 환경에서의 서비스 거부 공격

최근 분산환경에서의 서비스 공격 도구들이 많은 시스템에 불법적으로 설치되고 있으며, 이 해킹도구들은 서로 통합된 형태로 패킷을 범람시켜 심각한 네트워크 성능저하 및 시스템 마비를 유발하고 있다. 대표적인 서비스거부 공격 도구로는 Trinoo(혹은 trin00)와 tribe flood network(TFN)이 있다.

Trinoo는 많은 소스로부터 통합된 UDP flood 서비스거부 공격을 유발하는데 사용되는 도구로써, Trinoo 공격은 몇 개의 서버(마스터들)들과 많은 수의 클라이언트들(데몬들)로 이루어진다. 공격자는 Trinoo 마스터에 접속하여 마스터에게 하나 혹은 여러 개의 IP 주소를 대상으로 서비스 거부공격을 수행하라고 명령을

내린다. 같은 방법으로 Trinoo 마스터는 여러 데몬들과 통신하여 공격을 수행한다[16].

Trinoo와 같은 분산 환경에서의 서비스 거부 공격은 공격 대상이 일정치 않기 때문에 공격과 피해는 1차, 2차 등으로 확산되며, 데몬들이 설치된 곳 역시 이미 공격 피해 지역인 것을 보안 관리자가 인식하기에 어렵다는 것이 문제로 작용한다. 또한, Trinoo와 같은 분산 서비스 거부 공격은 네트워크 성능을 저하시키는 주원인이 되며, 해당 근원 지역 보안시스템들이 상호 협동, 즉, 패킷 필터링을 하지 않는 이상 네트워크의 성능은 현저히 감소하게 된다.

실제 타지역의 보안시스템들이 도움을 주지 않는 이상 검출과 차단에도 많은 어려움이 있다. 예를 들면, 보안 감시 시스템이 구비되지 못한 지역이나 비록 감시 시스템이 동작하는 지역이라고 해도 최신 정보를 업데이트하지 못한 곳은 대응이 불가능하다. 본 논문에서 제안하는 보안연합체는 이와 같은 문제점을 해결할 수 있다.

Trinoo 공격은 일반적으로 다음과 같은 세 가지 상황에서 보안시스템에 의해 탐지될 수 있다.

- Trinoo 데몬에 의한 UDP flooding 공격을 감지한 경우
- Hacker가 Trinoo 마스터에게 접속하는 공격 징후를 감지한 경우
- Trinoo 마스터에서 Trinoo 데몬으로 전달되는 공격 징후를 감지한 경우

그림 7은 Trinoo 공격과 ZC를 이용한 대응 절차를 나타낸 것으로써, 공격 대응 절차는 다음과 같다.

① 공격자는 공격을 위해 Trinoo 마스터에 접속하여 공격대상의 IP 주소를 지정하여 공격 명령을 내린다.

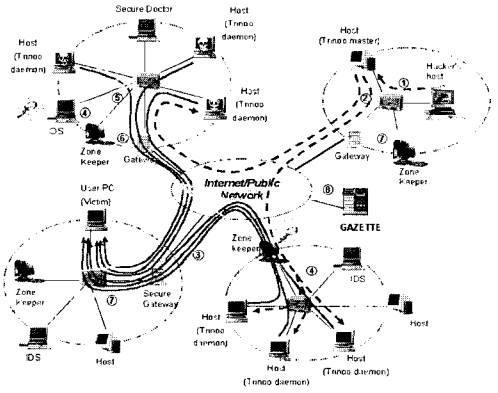

그림 7 Trinoo 공격과 대응 시나리오

② Tnoo 마스터는 자신이 알고있는 각 Trinoo 데몬에게 공격대상의 IP 주소와 함께 공격 명령을 전달한다.

③ Trinoo 데몬은 동시에 공격 대상 시스템을 공격한다.

④⑤⑥ 침입탐지 시스템이나 침입탐지 기능이 있는 ZK는 Trinoo 공격인 UDP flooding을 감지하여 내부의 방역 정책을 보안 시스템들에게 지시하고, 이를 이웃 ZK와 GZ에 보고한다.

⑦ 보고를 전파 받은 ZK는 해당 Trinoo 데몬에 대한 감시를 수행하여 Trinoo 마스터와 데몬을 축출하고 차후에 있을 공격을 차단한다.

⑧ GZ은 보안 정책, 방역 모듈들을 확인한 후, 등록된 ZK들에게 SAL을 발령한다.

6.2 Nimda Worm(W32/Nimda worm)

Nimda 웜(worm)은 전파를 용이하게 하기 위해서 웹의 콘텐츠를 변경하는 것을 제외하고는 시스템 내에서 특별한 파괴적인 행위를 하지는 않는다. 그러나, 네트워크 탐색(scanning)과 전자우편(e-mail) 발송으로 인한 DoS(Denial of Service) 공격을 발생시키기 때문에 문제가 되고 있다. Nimda 웜의 감염경로는 아래와 같이 크게 다섯 가지로 조사되고 있다[17].

- 전자우편을 통한 클라이언트에서 클라이언트로
- 공유 네트워크 자원을 통한 클라이언트에서 클라이언트로
- 감염된 웹사이트 접속을 통한 웹서버에서 클라이언트로
- Microsoft IIS 4.0/5.0 directory traversal 취약점 통한 클라이언트에서 웹서버로
- Code Red II와 sadmin/IIS 웜에 의해서 만들어진 백도어를 통한 클라이언트에서 웹서버로

Nimda 웜과 같은 감염에 대해 ZC를 이용한 대응 방안은 매우 다양하지만, 대표적인 두 가지 경우에 대해 기술하고자 한다.

시나리오-1 : 바이러스 근원지가 Zone cooperation이 가능하며, 바이러스가 전자우편을 통해 전파되는 경우

① Nimda 바이러스에 감염된 PC는 바이러스 코드가 첨부된 전자우편을 Zone 내부 사용자의 전자우편 주소로 발송한다.

② 사용자는 메일서버에 접속하여 바이러스 코드가 첨부된 전자우편을 수신한다.

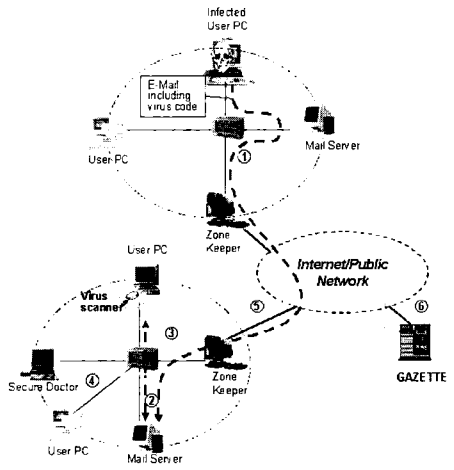

그림 8 Nimda 바이러스와 대응 시나리오-1

③ 사용자 PC의 바이러스 검색 소프트웨어가 바이러스 코드를 발견하고 이를 ZK에게 보고한다.

④⑤ ZK는 방역 정책을 내부 보안시스템들에게 지시하고, 이웃 ZK와 GZ에 보고한다.

⑥ 보고를 전파 받은 각 ZK들은 Nimda 방역 정책을 가동한다. 해당 바이러스 진단 및 치료 기능이 Zone 내에 없다면, GZ이나 이웃 ZK로 기능을 다운로드 받아서 방역 기능을 수행한다.

시나리오-2 : 바이러스 근원지가 Zone cooperation이 가능하지 않은 네트워크며, 감염된 웹 서버 접근에 의해 감염되는 경우

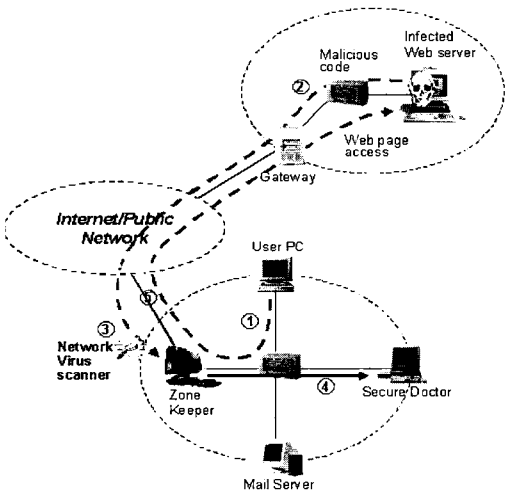

그림 9 Nimda 바이러스와 대응 시나리오 - 2

① 사용자가 바이러스에 감염된 웹 서버의 서비스를 요구한다.

② 감염된 웹 서버는 서비스 요구에 대한 응답으로 바이러스를 전파하는 악성 코드가 포함된 페이지를 전송한다.

③ ZK에 네트워크 트래픽 상의 악성코드 검출기능이 있는 경우 Zone Keeper가 악성코드를 탐지한다.

④ ZK는 방역 정책을 내부 보안시스템들에게 지시하고, 이웃 ZK와 GZ에 보고한다.

⑤ 보고를 전파 받은 각 ZK들은 Nimda 방역 정책을 가동한다. 해당 바이러스 진단 및 치료 기능이 Zone 내에 없다면, GZ이나 이웃 ZK로 기능을 다운로드 받아서 방역 기능을 수행한다.

7. 결론 및 향후 과제

컴퓨터 네트워크의 개방성과 전산 자원의 중요성에 따른 보안 시스템의 필요성이 대두되고, 이들에 대한 효율적인 관리의 필요성과 함께 네트워크 환경의 확장 및 복잡성 증가에 따라 보안 관리는 더욱 어려워지고 있다. 현재 국내외적으로 이러한 문제점을 해결하기 위해 통합 보안 관리 시스템을 개발하거나 출시하고 있지만, 공격자들의 기술이 날로 복잡화, 지능화, 조직화되고 있는 현실에서 다양한 보안 시스템들에 대한 관리 활동과 공격에 대한 대응은 단일 보안 관리 권한을 갖는 조직이 단독적으로 대처하기에는 부족한 점이 많다는 사실이다. 이에, 본 논문에서는 통합 보안관리의 필요성을 역설하고 능동적으로 이를 지원하기 위한 효과적인 차세대 네트워크 환경인 액티브 네트워크 기술에 대해서 설명하였다.

본 논문에서는 Zone이라고 하는 논리적 보안관리 단위를 구성하고 이들간에는 액티브 네트워크 기술을 바탕으로 보안 사건 및 보안 정책의 전파 기술을 제안하고 설계하였다. Zone은 단일 보안 관리 권한에 속하여 보안 관리가 이루어지는 논리적인 단위로서, Zone 내부에는 공격에 대한 대응, 접근 제어를 수행할 수 있는 대응 및 차단 시스템과 보안 사건을 탐지하고 분석할 수 있는 탐지 시스템이 하나 이상 존재하며, 통합 보안관리 기술을 적용하여 이들 간의 일차적인 상호 연동을 통해 단독적이며 능동적인 보안 관리가 이루어지는 논리적 단위로 정의한다. 또한, 이들 Zone 간에는 보안영역 정보 프로토콜을 이용하여 보안 사건에 대한 정보 및 적절한 대응 정책을 전달할 수 있으며, 각 Zone들은 상호 협력을 기반으로 조직화된 공격

에 대해 대응할 수 있다.

Zone 내부에서는 세분화된 보안 상태가 정의되어 효과적인 탐지, 차단, 방역 행위가 이루어지며, 보안 사건 탐지 시스템들에 의해 보고된 정보를 바탕으로 Zone Keeper는 단일 Zone의 보안 상태를 결정한다. 각각의 보안 상태는 대응 행위를 차별화하여 정의할 수 있으며, 적절한 수준의 보안 정책을 보안시스템들에게 적용하여 효율적인 네트워크 서비스 제공과 보안 관리를 수행할 수 있다.

향후 과제로는 제안된 보안영역 및 연합을 구현한 시스템의 시제품과 함께 그 성능에 대한 검증이 이루어져야 하며, 액티브 네트워크 상의 액티브 노드에 대한 보안 설계가 이루어져야 하겠다. 또한, 정확한 자산 분석과 위험 분석을 통한 대응 수준의 결정 방법이 정의되어 서비스 제공 측면과 보안 관리 측면에서 비용 대비 효율에 대한 고려가 이루어져야 한다.

참 고 문 헌

[1] C. Kaufman, R. Perlman, and M. Speciner, *Network Security: PRIVATE Communication in a PUBLIC World*, Prentice Hall PTR, 1995

[2] Open Platform for Security(OPSEC) Technical Note, Check Point Software Technology, Inc., 2000. *http://cgi.us.checkpoint.com/rl/resourcelib.asp?state=1&item=opsectech*

[3] J. Zao, L. Sanchez, M. Condell, C. Lynn, M. Fredette, P. Helinek, R. Krishnan, A. Jackson, D. Mankins, M. Shepard, and S. Kent, "Domain Based Internet Security Policy Management," *Proceedings of DARPA Information Survivability COnference and EXposition 2000 (DISCEX '00)*, Jan 25-27, 2000.

[4] S. McClure, J. Scambray, and G. Kurtz, *Hacking Exposed - Network Security Secrets & Solutions*, McGraw Hill Companies, 1999.

[5] Check Point OPSEC SDK Version 4.1 Release Notes, Check Point Software Technology, Inc., Nov 2, 1999. *http://cgi.us.checkpoint.com rl resourcelib.asp?state=1&item=opsectech*

[6] Secure Virtual Network Architecture: A Customer focused White Paper, Check Point Software Technologies Ltd., Nov. 2000. *http://cgi.us.check point.com/rl/resourcelib.asp?state=1&item=SVNWP20*

[7] Active Security Getting Started Guide Version 5.0, Network Associates, Inc., 1999.

[8] Automating Security Management while Reducing Total Cost of Ownership : Active Security and WMI - White Paper, Network Associates, Inc., 1999.

[9] D.Y. Lee, D.S. Kim, K.H. Pang, H.S. Kim, and T.M. Chung, "A Design of Scalable SNMP Agent for Managing Heterogeneous Security Systems," *NOMS2000*, 10 15 April 2000.

[10] D.S. Alexander, W.A. Arbaugh, A.D. Keromytis, and J.M. Smith, "Safety and Security of Programmable Network Infrastructures," *IEEE Communications Magazine, issue on Programmable Networks*, Vol. 36, No. 10, pp.84-92, Sep. 1998.

[11] D.L. Tennenhouse and D.J. Wetherall, "Towards an Active Network Architecture," *Computer Communication Review*, Vol. 26, No. 2, April 1996.

[12] D. Wetherall, U. Legedza, and J. Guttag, "Introducing New Internet Services: Why and How," *IEEE Network Magazine, July/August* 1998.

[13] Konstantinos Psounis, "Active Networks: Applications, Security, Safety, and Architectures," *IEEE Communications Surveys*, First Quarter, 1999. *http://www.comsoc.org/pubs/surveys*

[14] A. Jeffrey and I. Wakeman, "A Survey of Semantic Techniques for Active Networks," 1997. *http://www.cogs.susx.ac.uk/users/ianw/papers/an-survey.ps.gz*

[15] D. Raz and Y. Shavitt, "Active Networks for Efficient Distributed Network Management," *IEEE Communications Magazine*, Vol. 38, No. 3, pp.138 143, March 2000.

[16] 이현우, 정현철, 분산 환경에서의 서비스 거부 공격 분석보고서, CERTCC KR, 1999. *http://www.certcc.or.kr paper/tr1999/1999010/tr1999010.ht ml*

[17] 전익수, 이완희, Nimda Worm(W32/Nimda worm), CERTCC KR, 2001. *http://www.certcc.or.kr/paper/incident_note/2001/in2001_0 15.html*

[18] M. Sloman, "Policy Driven Management For Distributed Systems," *Journal of Network and Systems Management*, Vol. 2, No. 4, Plenum Press, pp.333 360, 1994.

[19] A.D. Rubin, D. Geer, and M.J. Ranum, *Web Security: Sourcebook*, John Wiley & Sons, Inc., 1997.

[20] V. Ahuja, *Network & Internet Security*, Academic Press, 1996.

[21] H.F. Tipton, and M. Krause, *Information Security Management Handbook*, 4th ed., CRC Press LLC, 2000.

장 범 환

1997년 성균관대학교 전자공학과 졸업(학사). 1999년 성균관대학교 전기전자 및컴퓨터공학과 졸업(석사). 1999년~현재 성균관대학교 전기전자및컴퓨터공학과 박사과정. 관심분야는 액티브 네트워크, 네트워크 관리, 네트워크 보안

김 동 수

1998년 성균관대학교 정보공학 졸업(학사). 2000년 성균관대학교 전기전자 및 컴퓨터공학과 졸업(석사). 2000년~현재 성균관대학교 전기전자 및 컴퓨터공학과 박사과정. 관심분야는 네트워크 관리, 네트워크 보안, 시스템 보안

권 윤 주

2000년 성균관대학교 정보공학과 졸업(학사). 2002년 성균관대학교 전기전자 및 컴퓨터공학과 졸업(석사). 2002년~현재 한국과학기술정보연구원 슈퍼컴퓨팅센터. 슈퍼컴퓨팅인프라개발실 연구원. 관심분야는 네트워크 보안, 그리드 컴퓨팅

남 택 용

1987년 충남대학교 계산통계학과 졸업(이학사). 1990년 충남대학교 대학원 계산통계학과 졸업(이학석사). 1987년~현재 한국전자통신연구원(ETRI) 정보보호연구본부. 네트워크보안구조연구팀 팀장. 관심분야는 정보보호, 네트워크구조, 통신망관리, 차세대인터넷, 액티브네트워크

정 태 명

1981년 연세대학교 전기공학과 졸업(학사). 1984년 University of Illinois Chicago, 전자계산학과 학사 졸업(학사). 1987년 University of Illinois Chicago, 컴퓨터공학과 석사 졸업(석사). 1995년 Purdue University, 컴퓨터공학 졸업(박사). 1985년~1987년 Waldner and Co., System Engineer. 1987년~1990년 Bolt Bernek and Newman Labs., Staff Scientist. 1995년~현재 성균관대학교 정보통신공학부 부교수. 관심분야는 네트워크 관리, 네트워크 보안, 시스템 보안, 전자상거래, 실시간시스템