능동 네트워크 기반의 능동 보안 관리 시스템

정회원 이 영 석*

Active Security Management on Active Networks

Young-seok Lee* *Regular Member*

요 약

인터넷 기반의 사이버 공격의 형태가 다양해지고 복잡해지면서 공격자를 탐지하고 신속하게 대응하는 것이 점차 어려워지고 있다. 또한, 기존의 네트워크 보안 메커니즘이 지엽적인 영역에서 방어적인 대응에 치중하고 있는 실정이다. 본 논문에서는 다양한 사이버 공격에 쉽게 대응할 수 있고, 보안 영역 간의 협력을 통해 공격자를 추적하고 고립화할 수 있는 능동적인 대응이 가능한 새로운 네트워크 보안 구조를 제안하고자 한다. 제안된 보안 구조는 능동 네트워크 상에서 능동 패킷 기술을 이용하여 위조 IP 공격이나 DDoS(Distributed Denial of Service) 공격 등을 효과적으로 대응하는 것이 가능하다. 제안된 보안 구조를 기반으로 설계된 능동 보안 관리 시스템은 보안 영역 내에서 능동보안노드와 능동보안관리서버로 구성되며, 다양한 보안 영역 내의 능동보안관리 시스템 간의 협업을 통해 기존의 사이버 공격 대응 방식보다 능동적으로 대응할 수 있다. 능동보안관리 시스템의 적용가능성을 검증하기 위해 테스트베드를 구축하여 실험하였고, 실험 결과를 분석한다.

Key Words : Active Network, Active Security

ABSTRACT

It has become more difficult to correspond an cyber attack quickly as a pattern of attack becomes various and complex. And, current security mechanisms just have passive defense functionalities. In this paper, we propose new network security architecture to respond various cyber attacks rapidly and to chase and isolate the attackers through cooperation between security zones. The proposed architecture make possible to deal effectively with cyber attacks such as IP spoofing or DDoS(Distributed Denial of Service) using active packet technology including a mobile sensor on active network. Active Security Management System based on proposed security architecture consists of active security node and active security server in a security zone, and is designed to have more active correspondent than that of existing mechanisms. We implemented these mechanisms in Linux routers and experimented on a testbed to verify realization possibility of Active Security Management System. The experimentation results are analyzed.

Ⅰ. 서 론

현재의 네트워크 보안 관리는 방화벽(Firewall), VPN(Virtual Private Network), IDS (Intrusion Detection System) 등 개별 기능이나 개별 제품 중심으로 지엽적인 네트워크(예: LAN, intranet 등)에 적용되고 있으며, 네트워크 관리도 운용자의 수동적인 방법에 의존하므로 네트워크가 대규모화됨에 따라 제어/관리 방법의 복잡도가 증가하고 있다. 또한, 다양한 유형의 개별적인 보안 시스템이 적용되어 시스템간의 연동이 불가능하고, 새로운 보안 기능 추가 시에 하드웨어 및 시스템의 교체가 수반되는 등 이종의 보안 장치간, 이종의 네트워크간, 이종의 사업자간의 상호 연동형 보안 서비스 환경을 제공

* 한국전자통신연구원(yslee@etri.re.kr)
논문번호 : 030424-0930, 접수일자 : 2003년 9월 30일

할 수 없으며, 사이버 공격에 대응하기 위해 사용자 종단간의 안전하고 효율적인 보안 관리가 불가능하다. 따라서, 사용자 요구에 적합한 고객 지향 서비스를 지원하고 서비스의 품질을 보호하기 위한 보안 기술의 개발이 요구되고 있다.

이를 위해 네트워크 관리 기능에 프로그래밍 가능성(Programmability)과 서비스 온 디맨드 (Service on Demand)라는 특성을 갖는 액티브 네트워크의 기술을 네트워크 보안관리 기능과 접목시키는 연구가 진행되고 있다[1,2]. 또한, 기존의 수동적인 네트워크 관리 문제, 네트워크 해킹 기술에 비해 느린 대응 문제, 정적인(static) 통합 보안 관리 솔루션의 문제 등을 능동적으로 해결하고 기능 향상을 신속히 할 수 있는 능동 보안 관리 기술 개발이 요구된다. 따라서, 네트워크의 동작 환경이나 위치에 무관하게 자유로운 서비스의 구성이 가능한 이동형 코드 기술과 네트워크의 제어 및 관리를 가능하게 하는 통신 기술인 액티브 네트워크 기술을 이용하여, 네트워크 보안관리를 동적으로 재구성(Dynamic reconstructing)할 수 있고 다수의 네트워크 구성 요소를 제어하기 위한 능동 보안 관리 기술을 개발하는 것이 필요하다.

한편, 네트워크 보안 기술의 발전 추세에 따라 앞으로의 네트워크 보안은 네트워크 전체 즉, intra-domain은 물론 inter-domain까지 보안 관리 영역을 확장하며, 실시간으로 공격에 대한 모니터링과 탐지 및 대응을 수행할 수 있고, 네트워크 내의 모든 노드가 보안 장치화되는 형태로 발전될 것으로 예상된다.

본 논문에서는 이런 요구 사항을 반영하기 위하여 액티브 네트워크를 기반으로 네트워크 상에 존재하는 보안 영역간, 보안 시스템 간의 협력이 가능하고, 보안 및 공격 기술의 변화와 보안 환경 변화에 따라 보안 기능의 능동적인 변화가 가능한 유연한 실행 구조를 갖는 네트워크 보안 프레임워크를 개발하고자 한다. 이를 위하여 새로운 네트워크 보안 프레임워크의 구조 및 보안 기능들을 도출하고, 프레임워크를 구성하는 능동보안노드 및 능동보안관리서버를 설계하고 이들 시스템을 구성하는 각 기능 블록을 개발하고자 한다.

논문의 구성은 다음과 같다. 2장에서는 인터넷 보안 기술 현황과 표준화 동향에 대해 소개한다. 3장에서는 이동형 코드를 이용한 능동 보안 관리 시스템의 형상을 기술하고, 4장에서는 능동 보안 관리 시스템 기반의 능동 대응 메커니즘을 소개한다. 5장에서는 테스트베드 상에서 제안된 메커니즘의 동작 과정에 대한 실험 과정을 기술하고 실험 결과를 분석한다.

Ⅱ. 보안 기술 현황 및 표준화 동향

인터넷 보안 기술은 크게 IPSec, SSL/TLS 등과 같은 네트워크 계층 보안 기술과 전자우편이나 JAVA 등과 같이 응용 프로그램에서 적용되는 응용 계층 보안 기술로 나누어 볼 수 있다. 보안 기술들은 상호 밀접한 관계를 가지고 있어서 하나의 보안 기술만을 이용하기보다는 다양한 메커니즘을 결합하여 안전하고 효율적인 보안을 제공해야 한다. IPSec은 네트워크 계층 가상사설망 기술로 현재 IETF IPSec 작업반을 중심으로 표준화 작업 중에 있다. IPSec은 AH(Authentication Header)와 ESP (Encapsulating Security Payload) 그리고 키 관리 메커니즘을 이용하여 IP 계층간의 패킷 송수신시 상위 계층에서 전달된 데이터의 인증, 무결성, 기밀성 보장을 통해 종단간 호스트 사이에서 안전하게 전송할 수 있도록 보안 서비스를 제공한다[3,4]. 현재 IPsec 가상사설망 제품들은 라우터나 스위치에 가상사설망 기능을 추가한 라우터/스위치기반 제품이 주를 이루고 있으며, 최근에는 침입차단 및 침입탐지 시스템에 추가한 시스템을 사용하고 있는 추세이다.

정보보호관리시스템은 정보보호정책에 기초한 관리 툴로서 시스템 보호, 사용자 관리 및 접근통제, 침입자 검출 및 대처 등 포괄적이면서 계층구조를 갖고 정보보호 관리업무를 수행하는 시스템이다. 외국의 경우에는 RADGUARD, DataLynx와 같은 업체들이 정보보호관리시스템의 개발을 주도하고 있는 실정이다[5]. NetGuard 보안관리시스템의 경우에 QoS(Quality of Service)와 보안성을 통합한 서비스를 제공하고 있으며, 보안성의 향상과 처리율을 증가시키기 위하여 하위 프로토콜 계층에서 패킷에 대한 관찰과 운용이 이루어지고 있다[6]. LanOptics의 보안관리시스템의 경우에는 중앙 집중화된 QoS 서비스들을 제공하고 있으며, 이들 서비스에는 방화벽, Network Address Translation, VPN, User Authentication, Bandwidth Control 등을 포함한다. Digital사의 방화벽 제품은 세 가지 범주인 엔트리 레벨, 미드레인지 및 하이엔드 제품군으로 분류하여 출시하고 있으며, 미드레인지 레벨 이상에서 정보보호정책 설정을 할 수 있는 기능을 제공하고 있다. OPSEC은 Check Point Software Technologies사가

제안한 산업 표준으로, 침입차단시스템을 중심으로 한 보안 시스템간의 상호 연동을 통해 자율적 보안 관리가 가능하도록 침입탐지시스템, CA 서버 등을 통합하여 전사적인 보안 환경을 제공하는 것을 목적으로 하고 있다. 보안 시스템간 상호 연동을 위해서는 CVP, SAMP 등 자체 통합용 프로토콜과 LEA, UAM 등의 어플리케이션으로 구성되어 있어 제3의 정보 보호 제품이 이러한 어플리케이션과 프로토콜을 수용해야 하는 단점과 인터페이스가 연결된 두 제품 사이에서의 통합만이 가능하다는 한계를 갖고 있다. 현재 OPSEC 프레임워크 파트너로 Symantec, Axent, RSA security, VeriSign, IBM, Novell 등 약 200개 업체가 참여하여 개발 중이나, 아직은 자사 제품의 통합에 치중하고 있다[7].

인터넷 보안 구조 측면에서는 개방형 네트워크 또는 분산형 네트워크 환경에서 보안 요구사항을 만족시키기 위해서 공개키 기반구조에 대한 연구가 활발히 진행중인 상태이다. 공개키 기반구조는 메시지 도청, 메시지 위조, 메시지 변조, 메시지 송수신 부인 등의 요소를 제거하기 위해 기밀성, 무결성, 인증, 부인 방지, 접근 제어 등을 제공하며, 전자 우편 보안, 웹 보안, 데스크탑 보안, 전자상거래 보안, 접근 제어, 가상사설망 보안등에 응용된다.

인터넷 보안기술의 표준화는 ISO/IEC JTC1/SC 27 과 ITU-T와 같은 국제기구에서의 공인 표준(de jure standard)보다는 IETF(Internet Engineering Task Force)와 같은 민간단체에서의 실용적인 사실 표준(de facto standard) 활동이 더욱 활발히 추진되고 있는 상태이다. IETF의 AFT(Authenticated Firewall Traversal) 워킹그룹은 침입차단시스템에 대해 응용계층에서의 프로토콜을 규정하고 침입차단 시스템의 인증에 대한 일반적인 구조와 함께 TCP와 UDP응용을 모두 지원하는 프로토콜 및 상호운용성을 위한 기본 인증 방법을 제안하고 있다[8]. 그러나, 현재까지 더 이상의 구체적인 진행은 없는 상태이다.

DARPA/ITO에서는 침입탐지시스템간 정보 교환 및 상호 운영을 위하여 CIDF(Common Intrusion Detection Framework)를 정의하고 있으며, 현재 공동 침입 탐지 프레임워크 아키텍쳐, 공통 침입탐지 프레임워크에서의 통신, 공통적인 침입 명세 언어, CIDF API(Application Programming Interface)와 같은 항목들이 정의되어 있다[9].

ISO/IEC JTC1/SC27 WG1에서는 침입탐지 표준화를 위하여 시스템에서 침입탐지에 대한 프레임워크를 정의하고 있으며 공통적 용어 정의, 침입 행위를 나타내기 위하여 사용되는 이벤트 정의, 데이터의 종류, 침입탐지 성능, 침입탐지 기법, 침입탐지시스템의 출력의 종류, 침입대응 등을 그 내용으로 하고 있다[10].

IETF IDWG(Intrusion Detection Working Group) 워킹그룹은 침입탐지시스템과 관리시스템 사이의 정보 공유를 위하여 데이터 포맷 및 교환 절차를 정의하고 있다. 또한, 두 시스템 간의 통신을 위한 요구사항과 이러한 요구사항에 대한 이론적 근거와 요구사항을 만족하는 데이터 포맷을 기술하는 공통 언어 스펙, 침입탐지 시스템간 통신을 위해 가장 잘 사용되는 현재의 프로토콜과 데이터 포맷을 연관시키는 방법 등에 관한 연구를 수행하고 표준을 제정하고 있다[11].

IETF IPSEC(IP Security Protocol) 워킹그룹은 IP 프로토콜을 보호하는 메커니즘, 즉 인증, 무결성, 접근통제, 비밀성의 조합들을 유연하게 지원하는 암호화 정보보호 서비스를 제공하기 위해 네트워크 계층에서의 정보보호 프로토콜을 개발하고 있는 상태이다[12].

Ⅲ. 능동 네트워크 기반의 능동 보안 관리 시스템

본 논문에서 제안된 능동 네트워크 기반의 능동 보안 관리 시스템은 단일 네트워크 내에서의 방어적인 보안 기능을 제공하는 기존의 보안 기반구조를 광역 망에서도 사용할 수 있도록 확장이 가능하며, 새로운 보안 메커니즘을 유연하고 동적으로 적용할 수 있는 기능을 제공하고, 네트워크 보안 환경 변화에 보다 민감하고 신속하게 대응할 수 있는 지능적인 보안 기능을 제공하는 것을 목적으로 한다. 그림 1은 광역 네트워크에서 능동 보안 관리 시스템을 이용한 능동 보안 관리 프레임워크를 도식화한 그림이다.

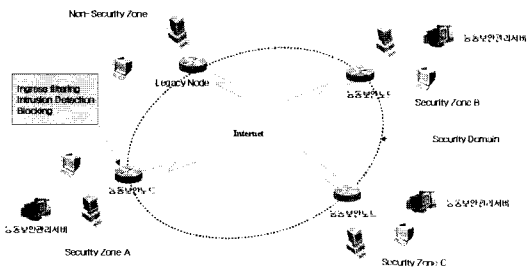

그림 1. 능동 보안 관리 프레임워크

본 논문에서 제안된 능동 보안 관리 프레임워크는 그림 1에 도시한 바와 같이 보안 관리 영역(Security Zone)의 경계에서 능동 보안 코드 처리 및 능동 대응 기능을 제공하는 "능동보안노드"와 이를 관제하는 "능동보안관리서버"로 구성되며, 두 시스템이 연동하여 하나의 보안 관리 영역을 관리하고 제어한다. 각 보안 관리 영역은 전체 네트워크 상에 분산적으로 배치되어 상호간의 연동 및 협업을 수행하지만, 이를 위한 별도의 관리 계층은 갖지 않는다. 즉, 모든 능동 보안 제어는 능동 보안 코드를 통해 이루어지며 보안 영역 간의 상호 연동과 협업 역시 능동 보안 코드에 의해 수행된다.

그림 1에서 보듯이, 각각의 보안 관리 영역은 능동 보안 코드를 통해 상호 연동함으로써 광역 네트워크 상에 논리적인 능동 보안 관리 도메인(*Security Domain*)을 형성한다. 이와 같이 기존의 네트워크(인터넷 백본)에 배치되어 있는 네트워크 시스템의 구성에 대한 변경 없이 새로운 능동 보안 관리 영역을 형성할 수 있는 것이 능동 보안 관리 시스템의 큰 특징 중 하나이다.

3.1 능동 보안 관리 시스템 구성

그림 2는 능동 보안 관리 시스템을 구성하는 능동보안노드와 능동보안관리서버의 기능 블록을 도식화한 그림이다. 능동보안노드 및 능동보안관리서버에는 보안 데이터를 수신하고 실행시킬 수 있는 능동 보안 데이터 처리 블록이 공통적으로 탑재된다. 또한, 능동보안관리서버에는 능동 보안 관리를 위한 기능 블록과 능동 보안 정책을 관리하기 위한 저장소가 추가적으로 탑재되며, 능동보안노드에는 능동 보안 데이터에 네트워크 차원의 실시간 대응 기능을 제공하는 능동 대응 블록이 추가된다.

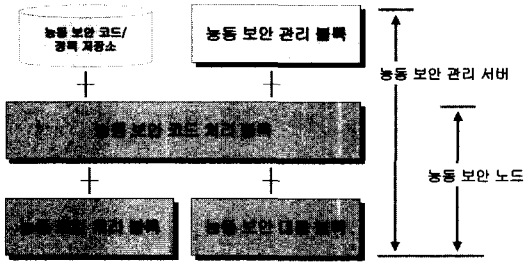

그림 2. 능동 보안 관리 시스템 구성도

능동보안관리서버는 보안 관리 영역 내에 배치된 보안 장비(능동보안 노드, NIDS, HIDS, Firewall 등)로부터 보고된 침입 행위에 대하여 능동 보안 대응을 수행함으로써 네트워크의 보안 상태를 자동적으로 제어하는 기능을 제공한다. 구체적으로, 보고된 침입 행위에 대하여 조치해야 하는 최적의 대응 정책을 선택한 후 능동 보안 데이터를 통하여 네트워크에 보안 정책을 적용시키는 기능을 수행한다. 즉, 보안 관리 영역 내의 능동보안노드를 제어함으로써 자신의 보안 관리 영역을 관리하며, 다른 보안 관리 영역을 관리하는 능동보안관리서버와의 협업을 통해 전역적인 네트워크 보안 관리 기능을 수행한다. 능동 보안 관리 시스템 상호간의 모든 제어 및 관리는 능동 패킷 내에 저장된 능동 보안 데이터에 의해 수행된다.

능동보안노드는 보안 관리 영역의 경계(가입자 네트워크의 Edge 라우터)에 능동 보안 데이터 처리 기능과 네트워크 차원의 실시간 보안 대응을 수행하는 능동 대응 기능을 탑재한 시스템이다. 능동보안노드는 보호하고자 하는 네트워크의 가장 전단에 위치하여 유입되는 네트워크 패킷을 필터링하고 차단하는 기능을 수행한다[13]. 또한, 위조 IP 역추적을 위한 MAC 주소 관리 기능과 DDoS 검출을 위한 트래픽 모니터링 기능 등을 제공한다. 이 외에도 전달된 능동 보안 데이터를 수행한 후, 다른 네트워크로 송신하거나 능동보안관리서버로 전달하는 등의 기능도 제공한다.

3.2 능동 보안 관리 시스템 기능 블록

능동 보안 관리 시스템의 기능 블록은 크게 능동 보안 관리 블록, 능동 보안 코드 처리 블록, 능동 패킷 처리 블록, 능동 보안 대응 블록, 그리고 능동 보안 코드/정책 저장소 블록으로 구성된다.

능동 보안 관리 블록은 보안 관리 영역 내에 배치된 보안 장비(능동보안 노드, NIDS, HIDS, Firewall 등)로부터 보고된 침입 행위에 대하여 능동적인 보안 대응을 수행함으로써 네트워크의 보안 상태를 자동적으로 제어하는 기능을 제공한다. 또한, 수신된 경보 데이터를 참조하여 이에 적합한 보안 대응 수위를 결정하고, 이를 실행시키기 위해 능동 보안 코드를 포함한 능동 패킷을 생성하여 네트워크에 송신함으로써 네트워크 보안 제어를 수행한다. 또한, 능동 보안 코드로부터 수집되는 네트워크 보안 상태 정보를 관리하고 이에 대한 보안 대응 수단(능동 보안 코드)을 네트워크에 제공함으로써 네트워크 차원의 보안 상태를 동적으로 제어하고 관리한다.

능동 보안 코드를 이용하여 네트워크의 보안 상태를 관리하기 위해서는 네트워크 계층에서 능동 보안 코드를 인지하고 이를 상위에 전달하여 실행시킬 수 있는 기능이 능동보안노드에 설치되어야 한다. 능동 보안 코드 처리 블록은 이러한 기능을 수행하는 소프트웨어 블록이며, 능동 패킷 처리 블록으로부터 능동 보안 코드를 수신하여 제한된 컴퓨팅 자원 내에서 실행시키는 기능을 수행한다. 이때 실행되는 코드가 능동 패킷 내에 포함되어 있지 않은 경우에는 능동 보안 코드/정책 저장소에서 다운로드 받아 실행한다. 능동 보안 코드의 수행에 필요한 자원 할당과 새로이 생성된 능동 보안 코드를 네트워크에 전송 하는 기능은 하위 계층의 자원 관리자인 능동 패킷 처리 블록에게 요구한다.

능동 패킷 처리 블록은 능동 패킷 형태로 전송되는 능동 보안 코드를 네트워크 계층에서 인식하고 수신하여 능동 보안 코드 처리 블록으로 전달하는 기능 및 새로 생성된 능동 보안 코드를 능동 패킷으로 캡슐화 하여 네트워크에 전송하는 기능을 수행한다. 능동 패킷 처리 블록이 송수신하는 패킷은 기존 네트워크에서 사용하는 IP 패킷 형태로 구성되어 네트워크에 존재하는 다른 일반 노드에서도 전달될 수 있다. 능동 패킷 처리 블록이 생성하고 수신하는 능동 패킷의 구조가 그림 3에 보여진다.

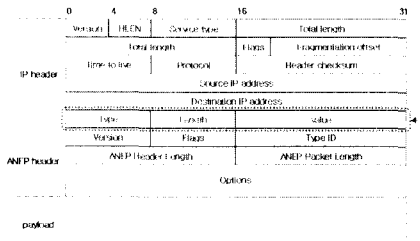

그림 3. 능동 패킷 구조

패킷의 IP 헤더와 ANEP 헤더는 능동 패킷 처리 블록에서 사용되며, 페이로드 부분은 상위 계층에 존재하는 능동 보안 코드 처리 블록에서 사용된다. 페이로드 부분에는 능동 보안 코드가 포함된다. 'IP Router Alert Option'은 라우터가 패킷의 목적지 주소가 자신이 아닌 패킷을 가로챌(intercept) 수 있도록 해주는 옵션으로써 일반 IP 패킷과 능동 패킷을 구분하는 표시자 역할을 한다.

능동 보안 대응 블록은 능동 보안 코드가 능동보안노드의 네트워크 보안 기능을 이용하기 위한 상위 인터페이스를 제공하는 블록이다. 즉, 능동보안 노드 상에서 실질적으로 수행되는 능동 보안 코드가 패킷 필터링 또는 블록킹과 같은 보안 대응 기능을 제어하기 위해 필요한 인터페이스들을 제공한다. 또한, 이들 인터페이스를 통해 수행되는 보안 대응 기능도 이 블록에 포함된다. 또한, 세션 관리, IP 관리, 위조 IP 관리, MAC 주소 관리, 그리고 DDoS 탐지 및 대응 기능을 제공한다.

능동 보안 코드 수행 정책은 보안 관리 서비스에 따라 관리자에 의해 생성되는 다양한 보안 데이터 정책을 저장하고 관리하기 위한 데이터베이스관리시스템으로 구성되며, 디렉토리 서버를 이용한다. 능동 보안 코드/정책 저장소는 능동보안노드 및 능동 보안관리서버와는 LDAPv3 프로토콜을 이용하여 능동 보안 코드 및 정책을 전달한다.

3.3 능동 보안 코드

능동 보안 코드는 능동 네트워크 상에서 보안 기능을 수행하는 일종의 능동 패킷이다. 이러한 코드는 네트워크 침입에 능동적으로 대응하기 위한 소프트웨어 모듈로써, 능동 패킷 내에서 실행 가능한 프로그램 형식으로 전달된다. 코드는 이동성 유무에 따라 상주형 코드와 이동형 코드로 구분한다. 상주형 코드는 능동보안노드에 상주하며 필요에 따라 새로운 코드를 생성하고, 이동형 코드는 능동보안노드와 능동보안관리서버에서 수행되며 코드 내의 데이터를 변경할 수 있고 다른 능동보안노드나 능동보안관리서버로의 이동성을 갖는다.

또한, 능동 보안 관리를 위해 위조 IP 역추적 기능, DDoS 역추적 기능, 역추적 완료 및 결과 보고 기능, 패킷 차단 및 차단 해제 기능, 트래픽 모니터링 기능, 트래픽 검출 기능을 수행하는데 필요한 데이터를 제공한다. 본 논문에서는 표 1과 같은 이동형/상주형 코드를 설계하였고 코드의 기능은 다음과 같다.

1) 위조 IP 역추적 코드(Spoofed IP Tracing Code)는 IP 패킷의 근원지 주소를 위조하는 위조 IP 공격 대응을 위한 역추적 기능을 수행한다.

2) DDoS 역추적 코드(DDos Tracing Code)는 트래픽을 세션별로 조사하여 임계치를 넘는 트래픽을 보내는 노드에게 DDoS 추적 코드를 재전송하는 기능을 수행한다.

3) 역추적 완료 및 결과 보고 코드(*Complete* Code)는 역추적 완료 후 실제 공격자를 네트워크로부터 고립시키는 기능과 역추적 결과를 각 능동보안관리서버에게 전달하는 기능을 수행한다.

4) 패킷 차단 및 차단 해제 코드(Complete Code)는 추적 센서 수신 후, 능동보안노드에서 침입자로부터 공격이 불가능하도록 패킷을 차단하는 기능과 추적 센서 수신 후, 능동보안노드에서 경유지로 사용되어 차단된 노드의 패킷을 차단 해제하는 기능을 수행한다.

5) 트래픽 모니터링 코드(DDoS Traffic Monitor Code)는 도메인 내로 유입되는 트래픽의 이상 변동을 감지하는 기능과 일정 수준을 넘는 트래픽이 발생했을 때 능동보안관리서버에게 보고하기 위해 새로운 코드를 생성하는 기능을 수행한다.

6) 트래픽 검출 코드(DDoS Traffic Detect Code)는 트래픽 모니터링의 결과를 능동보안관리서버에게 전달하는 기능을 수행한다.

각 코드의 수행 환경은 표 1과 같다.

표 1. 코드 이름 및 수행환경

코드 이름	종류	수행환경			
		피해도메인 능동보안 관리서버	피해도메인 능동보안 노드	공격도메인 능동보안 노드	공격도메인 능동보안 관리서버
Spoofed IP Tracing Code	이동형	X	O	O	O
Spoofed IP Tracing Complete Code	이동형	X	O	O	X
DDoS Traffic Monitor Code	상주형	X	O	X	X
DDoS Traffic Detect Code	이동형	O	X	X	X
DDoS Tracing Code	이동형	X	O	O	O
DDoS Tracing Complete Code	이동형	O	O	O	X

Ⅳ. 능동 보안 관리 시스템에서의 사이버 공격 대응 메커니즘

본 장에서는 능동 보안 관리 시스템이 실제 네트워크 상에서 어떠한 보안 기능을 제공하는지를 소개하고, 앞에서 설명된 능동보안기술이 능동보안관리 시스템을 통해 어떠한 모습으로 네트워크에 적용되는지를 알아본다. 현재 구현된 능동 보안 코드를 통해 제공 가능한 네트워크 보안 서비스는 아래와 같으며, 각각의 동작 메커니즘을 시나리오에 기반하여 설명한다.

4.1 위조 IP 공격 대응 메커니즘

위조 IP 공격에 대한 대응 기능은 해커가 IP 헤더 내의 근원지 IP 주소를 타인의 IP 주소로 위조하여 공격(IP Address Spoofing Attack)한 경우에 패킷의 실제 송신자를 추적하기 위한 역추적 메커니즘과 해커를 공격자 보안 영역에서 고립시키는 보안 서비스를 제공한다[14]. 능동 보안 관리 시스템이 제공하는 위조 IP 역추적 메커니즘은 기존의 네트워크 프레임워크를 수정하지 않고도 이동형 보안 센서를 통해 신속하게 실제 공격자를 검출할 수 있으며, 지금까지 수동적으로 이루어졌던 침입자 파악 수단보다 자동적이고 능동적인 대응을 가능하게 한다. 위조 IP 역추적 메커니즘은 다음과 같은 기능을 제공한다.

- 침입 탐지 및 차단을 위해 필요한 기존 보안 장비(NIDS)와의 연동 기능
- 침입 근원지를 파악하기 위한 역추적 기능, 침입자를 원천 봉쇄하기 위한 침입 근원지 고립화 기능
- 상기 기능의 유기적인 통합 관리를 통한 보안 관리 영역의 보안 상태 복구 기능

또한, 위조 IP 공격에 대한 대응 서비스를 제공하기 위하여 보안관리 영역의 망 접속 점(Edge Point)에 설치된 능동보안노드에서 "Ingress Filtering" 기능을 수행한다. "Ingress Filtering"을 통해 해커에 의한 타 영역 내의 IP 주소 위조 및

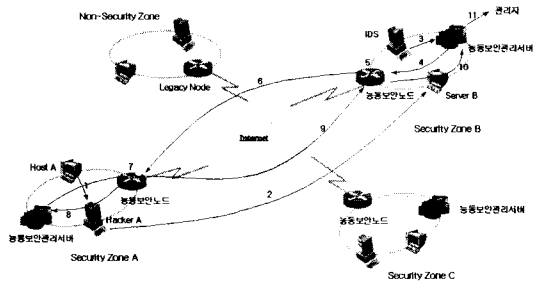

그림 4. 위조 IP 공격 대응 메커니즘

조작을 사전에 방지함으로써 해커에 의한 IP 위조 범위를 하나의 보안 관리 영역 내부로 한정한다. 위조 IP 공격 대응 메커니즘은 그림 4와 같은 절차에 의해 수행되며, 각 단계별 수행 기능은 다음과 같다.

(단계 1) 보안 영역(Secure Zone) A에 위치한 해커 A는 동일한 보안 영역 내에 위치하는 호스트 A의 IP주소를 자신의 IP 주소로 위조한다.

(단계 2) 보안 영역 B에 위치하는 서버 B에게 DoS(Denial of Service) 공격을 시도한다.

(단계 3) 보안 영역 B에 존재하는 IDS는 공격을 감지하여 침입 탐지 경보를 능동보안관리서버(B)로 송신한다.

(단계 4) 능동보안관리서버(B)는 수신된 침입탐지 경보 데이터를 참조하여 유해 패킷을 송신한 근원지 IP 주소를(보안 영역 A 내의 호스트A 근원지 IP주소) 목적지 주소로 하여 역추적 센서(Spoofed IP Tracing Sensor)를 생성하여 전송한다.

(단계 5) 패킷 역추적 센서를 수신한 능동보안노드(B)는 수행환경을 통해 수신된 센서를 실행하여 유해 패킷의 유입을 차단한다. 이 때, 능동보안노드(B)는 해커의 위조 패킷은 물론 IP 주소를 위조 당한 호스트A의 정상적인 패킷까지 차단한다.

(단계 6) 능동보안노드(B)는 능동보안관리서버(B)로부터 수신한 역추적 센서를 목적지 주소로 전송한다.

(단계 7) 보안 영역 A의 접속 점에 위치하는 능동보안노드(A)에서 수신된 센서는 로그에 기록된 Outgoing Ethernet 프레임 축약 정보를 검색하여 유해 패킷 정보와 일치하는 로그 정보를 추출한 후, 로그 정보에 기록된 MAC 근원지 주소와 ARP(Address Resolution Protocol) table에 저장된 IP 주소를 비교하여 위조 여부 및 실제 근원지 IP 주소를 파악한다. 위조 여부가 판별되면 해당 MAC 주소로 부터 유입되는 패킷을 차단한다.

(단계 8) 역추적 의뢰 정보, 성공 여부, 파악된 근원지 주소 등의 정보를 해당 보안 영역 내의 능동보안관리서버(A)로 송신한다.

(단계 9) 능동보안관리서버(A)는 역추적을 의뢰한 능동보안관리서버(B)에게 해커의 고립 결과를 역추적 보고 센서(Spoofed IP Tracing Complete Sensor)로 전송한다.

(단계 10) 전달 경로 상의 능동보안노드(B)는 역추적 보고 센서를 수신한 후, (단계 5)에서 IP 주소를 위조 당한 호스트A의 정상적인 패킷까지 차단한 세션을 복구하고, 능동보안관리서버(B)로 역추적 보고 센서 전송한다.

(단계 11) 능동보안관리서버(B)는 수신된 역 추적 보고 센서의 정보를 보안 관리자에게 통보한다.

4.2 DDoS 공격 탐지 및 대응 메커니즘

분산 서비스 거부 공격(DDoS)은 수십~수백개의 시스템이 하나의 목표 시스템을 집중 공격함으로써 피해 호스트가 서비스를 제공하지 못하도록 하는 공격 형태를 의미한다. 즉 다량의 호스트들에게 DoS 공격용 프로그램(DDoS Agent)을 분산시켜 설치하고, 이들을 중앙에서 제어함으로써 목표 시스템에 일제히 유해 패킷을 전송하도록 하여 시스템의 성능 저하 및 시스템 마비를 유발시키는 공격이다 [15].

능동보안관리 시스템은 이러한 DDoS 공격을 탐지하고 네트워크 상에 분산되어 있는 DDoS Agent를 찾아내기 위한 역추적 메커니즘과 유해 패킷을 공격자 근원지에서 고립시키는 보안 서비스를 제공한다. DDoS 탐지 및 공격 대응 메커니즘은 그림 5와 같은 절차에 의해 수행되며, 각 단계별 수행 기능을 다음과 같다.

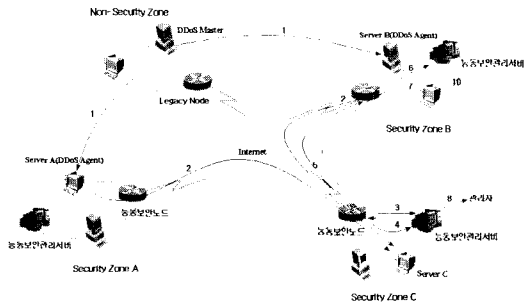

그림 5. DDoS 공격 탐지 및 대응 메커니즘

(단계 1) 비 보안 영역(Non-Secure Zone)에 위치한 해커는 보안 영역 C 내의 서버 C를 공격하기 위해 DDoS Master를 기반으로 보안 영역 A와 B에 위치한 서버(A,B)에 불법적인 방법을 사용하여 DDoS 에이전트를 설치한다.

(단계 2) 보안 영역 A와 B에 있는 DDoS 에이전트는 보안 영역 C에 위치한 서버 C로 DDoS 공격을 시도한다.

(단계 3) 능동보안노드(C) 내의 상주형 DDoS 트래픽 감시 센서(DDoS Traffic Monitoring Sensor)에서 입력 패킷을 분석하여 특정 시간 내에 입력된

전체 패킷의 양이 특정 값(Threshold)을 넘는다면 DDoS 공격으로 간주한다. DDoS 공격을 탐지하면 탐지된 결과를 포함하여 능동보안노드(C)는 DDoS 검출 센서(DDoS Traffic Detect Sensor)를 생성하여 능동보안관리서버(C)로 송신한다.

(단계 4) 능동보안관리서버(C)는 DDoS 검출 센서를 수신한 후, DDoS 검출 센서 내의 공격 정보를 분석하여 DDoS 역추적 센서(DDoS Tracing Sensor)를 생성하여 능동보안노드(C)로 전송한다.

(단계 5) 역추적 센서를 수신한 능동보안노드(C)는 수행환경을 통해 수신된 센서를 실행하여 보안 영역 C로 입력되는 패킷들을 분석한다. 만일 특정 근원지 주소(source IP)들로부터 입력되는 패킷의 수가 일정한 값을 넘는다면, DDoS 공격으로 간주하고 공격 패킷을 전송하는 DDoS 공격 에이전트 수와 동일하게 DDoS 역추적 센서를 생성한다. 생성한 DDoS 역추적 센서들은 DDoS 에이전트(서버 A,B)들을 목적지 주소로 하여 해당 보안 영역으로 전달된다.

(단계 6) DDoS 역추적 센서가 포함된 액티브 패킷은 전송 경로에 의해 능동보안노드(B)가 수신한다. DDoS 역추적 센서의 실행 코드에 따라 보안 영역 C의 서버 C로 나가는 패킷들을 검사한다. 검사한 패킷들이 서버 C의 특정 포트 번호(예, 23번)를 공격하는 것으로 판명되면, 능동보안노드(B)는 서버 B에서 서버 C로 나가는 패킷 가운데 특정 포트 번호(예, 23번)를 갖는 패킷들은 차단한다. 차단 이후에, 능동보안노드(B)는 DDoS 역추적 센서의 목적지 주소를 능동보안관리서버(B)로 변경하고 전송한다.

(단계 7) 능동보안관리서버(B)는 DDoS 역추적 센서를 수신하고, 처리 결과에 따라 DDoS 역추적 보고 센서(DDOS Tracing Complete Sensor)를 생성한다. DDoS 역추적 보고 센서의 목적지 주소는 DDoS 역추적 센서 내에 포함된 최초 전송자인 능동보안관리서버(C)의 주소로 결정된다. 전달 경로상의 능동보안노드(B)에서는 DDoS 역추적 보고 센서 수신 시, 별도의 실행 없이 재전송한다.

(단계 8) 능동보안관리서버(C)는 DDoS 역추적 보고 센서를 수신한 후, 센서 내에 포함된 정보를 분석하여 관리자에게 전달한다.

단계 5 ~ 7은 보안 영역 A에도 동일하게 적용된다. DDoS Master에 대한 추적 및 대응 기능은 본 논문의 영역 외로 한다.

V. 구현 및 실험 결과

본 연구에서는 능동보안노드와 능동보안관리서버를 Linux kernel version 2.4 상에서 구현하였고, 능동 보안 코드를 실행하기 위한 실행 환경으로서 SUN Java Virtual Machine version 1.4.2를 이용하였다. 능동보안관리서버에서 코드 수행 정책을 관리하기 위한 데이터베이스로서 PostgresSQL JDBC를 사용하였고, 능동 보안 코드를 저장한 저장소는 Netscape 사의 iPlanet Directory Server version 5.1을 사용하였다. 능동보안노드 상에서 유해 패킷의 필터링을 위해 libpcap 라이브러리(iptables 명령)를 사용하였다.

본 연구에서 개발한 능동 보안 메커니즘은 그 적용 범위가 광역 인터넷이라는 점에서 개발된 기능을 네트워크에 적용하고 검증하기가 매우 어렵다. 특히, 단일 로컬 네트워크 상에서는 개발된 기능을 검증할 방법이 없으므로, 능동보안관리 시스템의 적용 가능성 및 보안 기능 검증을 위한 테스트베드를 구축하여 개발된 기능을 검증하였다.

테스트베드는 인터넷 백본 환경과 능동보안관리 시스템으로 구성되는 복수의 보안 관리 영역을 포함하고, 테스트베드 상에서는 능동보안관리 시스템의 기능 검증, 네트워크 적용성 시험 등의 일련의 작업이 수행될 수 있는 제반 환경(NIDS, HIDS, ESM 등)을 제공한다. 또한, 능동보안관리 시스템의 각 기능들의 독립적인 시험 및 통합 연동 시험을 위한 제반 사항을 제공한다.

그림 6은 본 연구에서 개발된 능동 보안 메커니즘을 시험하기 위해 구성된 테스트베드를 보여준다. 중앙에 위치한 1개의 네트워크 도메인은 공중망의 역할을 하는 가상 ISP(Internet Service Provider) 도메인이고, 나머지 4개의 도메인은 ISP에 연결되어

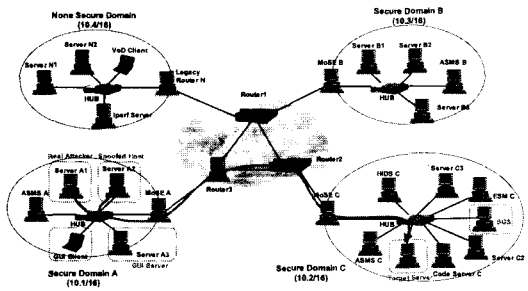

그림 6. 테스트베드 구성 및 위조 IP Flooding 공격도

있는 로컬 네트워크 도메인으로 공격자가 존재하는 네트워크 및 우회 공격 서버 또는 직접적인 피해를 입는 서버가 존재하는 피해자 네트워크로 이용된다. 현 시점에서는 실제 네트워크를 축소한 테스트베드 수준의 망으로 구성되며, 추후 필요에 따라 선도 시험망과 연결을 고려 할 수 있다.

테스트베드 시스템을 구성하는 각 주요 장비는 다음과 같다. ISP 경계(Edge) 라우터는 보안 관리 영역을 상호 연결하고, 가상 인터넷 환경을 구축하기 위한 Core 네트워크를 구성하기 위해 사용되는 라우터 시스템이다. 능동보안관리서버(ASMS, Active Security Management Server)는 각 보안 관리 영역에 구축된다. 능동 패킷을 처리할 수 있도록 확장된 리눅스 기반 커널로 동작하는 서버이며, 능동 보안 코드 정보를 관리하기 위한 데이터베이스(PostgreSQL)가 탑재된다. 능동보안노드(MoSE, Mobile Sensor Engine)는 각 보안 관리 영역의 접속점에 구축된다. 능동 패킷을 처리할 수 있는 확장된 리눅스 기반 커널로 동작하는 라우터이며, 패킷 차단, 프레임 모니터링(MAC, ARP 테이블 관리) 등 보안 대응 기능이 탑재된다. 가상 공격자 및 피해 시스템은 가상 해커를 가정하는 공격용 시스템과 공격 목표가 되는 시스템으로써 리눅스, SUN, Windows 등 다양한 플랫폼으로 구성된다.

5.1 위조 IP 공격 대응 시험 및 결과 분석

위조 IP 공격 대응 시험에서는 DDoS 공격용 툴이 Flitz를 이용하여 동일 도메인 상에 존재하는 다른 시스템의 주소를 이용하였고, 도메인 C에 존재하는 서버를 대상으로 "위조 ICMP Flooding" 공격을 수행하였다. 위조 IP 공격은 대부분 UDP 계열의 네트워크 공격이며, 본 실험에서는 이러한 공격을 탐지하기 위해서는 네트워크 기반 IDS 시스템을 설치하였다. 그림 6은 테스트베드 상에서 "위조 ICMP Flooding" 공격 경로를 보여준다.

본 시험은 5.2 절의 DDoS 공격과 성격상 유사한 점이 많지만, 단순히 위조 IP 기법을 사용하여 공격을 시도하였고, 그에 따른 능동보안관리 시스템의 보안 체계의 구동 및 대응과 관련된 동작을 시험하였다. 시험 절차는 다음과 같다.

- Flitz를 이용한 "위조 ICMP Flooding" 공격 수행
- IDS의 침입 탐지 및 능동보안관리 시스템으로 통지
- 능동보안관리 시스템의 구동 및 공격자 호스트 역추적
- 실제 공격자 호스트 MAC 주소 필터링
- 공격자 차단 확인

그림 7은 "위조 ICMP Flooding" 공격 시에, 능동 보안 관리 시스템이 능동 보안 코드를 이용한 대응 메커니즘에서 코드 수행 시간을 보여준다. Case A는 그림 6에서 피해 시스템이 속한 도메인 C의 경계에 위치한 능동보안노드(C)에서 수행된 위조 IP 역추적 코드의 수행 시간을 의미하며, Case B는 해커가 속한 도메인 A의 경계에 위치한 능동보안노드(A)에서 수행된 위조 IP 역추적 코드의 수행 시간을 의미한다. Case C와 Case D는 능동보안노드(C)와 능동보안노드(A)에서 수행된 위조 IP 역추적 보고 코드의 수행시간을 의미한다.

그림 7에서 보듯이, 능동보안노드(C,A)의 역추적 코드 수행 시간인 Case A와 Case B의 경우에서 해커의 1차 공격 시도인 경우는 1차 이후의 공격에서보다 수행시간이 길다. 이것은 센서의 실행 코드가 저장된 코드 서버(LDAP 서버)와 연결을 설정하고 코드를 다운로드 하는 시간을 포함하기 때문이다. 특히, Case B의 경우는 능동보안노드(A)에서 위조 IP 역추적 코드를 수신한 후, ARP를 이용하여 해커의 실제 MAC 주소를 블록킹하기 위해 수행되는 오버헤드가 포함되기 때문에 수행 시간이 가장 길다. 반면에, Case C와 Case D의 경우, 능동보안노드(C,A)에서는 역추적 보고 코드를 수신하지만 이미 연결되어 있는 코드 서버로부터 역추적 보고 코드를 다운로드 하며, 별도의 실행 없이 코드를 재전송한다. 따라서, 이 경우에서의 코드 수행시간은 아주 작다.

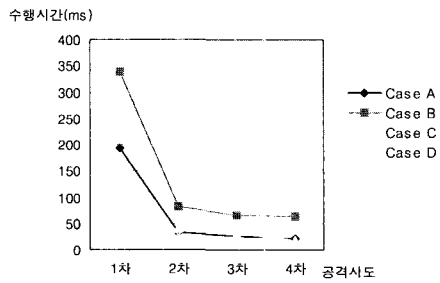

그림 7. 위조 IP 역추적 및 역추적보고 코드 수행시간

5.1 DDoS 공격 대응 시험 및 결과 분석

DDoS 공격은 목표 시스템의 서비스 제공을 방해하기 위하여 해당 시스템이 처리할 수 없는 요청을 보내는 공격으로써, 무수히 많은 에이전트에서 특정 서비스 요청을 전송하여 부수적으로 해당 네트워크 트래픽을 Flooding시키는 효과를 가지게 된다. DDoS 공격 툴의 구성은 공격 요청을 보내는 무수히 많은 에이전트와 해당 에이전트에 공격 명령을 시달하기 위한 마스터로 구성된다.

본 시험에서는 Flitz 툴을 이용하여 두개의 보안 도메인 상에 4개의 에이전트를 두고 비디오 스트리밍 서비스를 제공하는 서버를 공격하는 것으로 하였다. 또한 실제 네트워크 상황을 에뮬레이션하기 위해 iperf 툴을 이용하여 3.5M 정도의 백그라운드 트래픽을 생성하였다. 비디오 스트리밍 서비스로는 DVD 드라이브를 네트워크로 연결하여 DVD를 원격에서 구동하였다. 그림 8은 테스트베드 상에서 DDoS 에이전트들의 공격 경로를 보여준다.

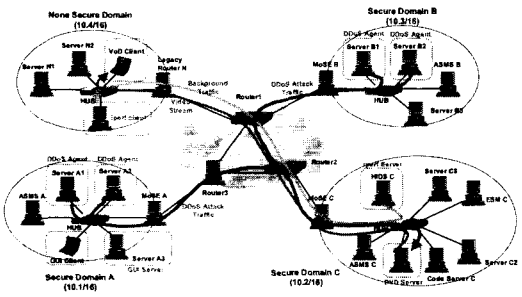

그림 8. DDoS 공격 시험 구성도

DDoS는 네트워크 기반의 IDS로 탐지하여야 하나 능동 보안 관리 시스템의 메커니즘을 이용하면 네트워크 기반 IDS가 필요하지는 않다. 즉, 능동보안관리 시스템을 구현한 각 도메인의 게이트웨이 라우터인 능동보안노드에서 네트워크 트래픽을 모니터링하고 이를 바탕으로 침입 경보를 발령하면 실제 트래픽이 과다하게 발생시키는 에이전트 위치를 추적하여 네트워크를 단절하게 된다. 실험에서는 공격이 이루어짐에 따라 비디오 스트링밍 서비스의 품질이 저하되는 것을 보여주었고, 능동 보안 관리 시스템의 동작에 따라 해당 서비스의 품질이 회복되는 것을 보여 주었다. 시험 절차는 다음과 같다.

- 비디오 스트리밍 서비스 제공
- Flitz를 이용한 DVD 서버에 공격
- 비디오 스트리밍 서비스의 품질 저하 확인
- 능동보안관리 시스템의 구동
- DDoS 공격 트래픽을 각 도메인의 게이트웨이인 능동보안노드에서 차단
- 비디오 스트리밍 서비스 품질의 회복
- 공격 트래픽 차단 확인

표 2는 DDoS 공격에 대해 능동 보안 관리 시스템이 능동 보안 코드를 이용한 대응에서 코드 수행 시간을 보여준다. 표 2에서 보듯이, 능동보안노드(C,B,A)에서는 DDoS 역추적 코드를 수신하고 DDoS 에이전트로부터 입력 트래픽을 블록킹하는 기능을 수행하므로 코드 수해시간이 길다. 그러나, DDoS 역추적 보고 코드는 능동보안노드(C,B,A)에서 별도의 실행 과정 없이 능동보안관리서버(C)로 전달되기 때문에 능동보안노드에 실행 부담이 없다.

표 2. DDoS 역추적 및 역추적 보고 코드 수행 시간

단위 : millisecond

코드종류 \ 공격시도	1차	2차	3차	4차
능동보안노드(C) DDoS 역추적 코드	10478	10933	10509	10747
능동보안노드(B) DDoS 역추적 코드	10672	10652	10778	10561
능동보안노드(A) DDoS 역추적 코드	10708	10889	10801	10693
능동보안노드(C) DDoS 역추적 보고 코드	30	17	22	29
능동보안노드(B) DDoS 역추적 보고 코드	22	24	27	20
능동보안노드(A) DDoS 역추적 보고 코드	25	28	24	21

Ⅵ. 결 론

본 논문에서는 네트워크 보안 환경 변화에 따르는 요구사항을 반영할 수 있는 확장된 보안 구조로서 액티브 네트워크를 이용한 능동 보안 관리 구조를 설계하였고, 위조 IP 공격이나 DDoS 공격에 대응하기 위한 메커니즘을 제안하였다. 제안된 능동 보안 관리 구조는 현재의 네트워크 보안 메커니즘에 비해 전체 네트워크 차원에서 공격자에 대해 강력한 대응을 수행할 수 있고, 새로운 공격 기술, 방어 기술의 등장이나 보안 환경 변화에 유연하게 적응할 수 있다. 능동 보안 관리 구조는 네트워크 보안 프레임워크와 해당 프레임워크를 구성하는 요소 기능 블록들로 이루어지며, 이러한 기능 블록을 통

합하여 능동보안관리 시스템을 구현하였다. 능동 보안 관리 시스템은 능동보안노드와 능동보안관리서버로 구성되며, 전체 네트워크 수준에서 수행할 보안 기능을 능동 보안 코드 형태로 수행하도록 설계되었다.

본 논문에서 제안된 능동 보안 관리 시스템의 적용 가능성을 증명하기 위해 테스트베드를 구축하고, 해당 테스트베드 상에서 실제 제공되는 서비스와 대표적인 공격 기법을 적용한 상태에서 시스템의 보안 기능을 시험하였다. 시험 결과 능동보안관리 시스템은 기존의 수동적인 침입 차단 및 침입탐지 시스템의 문제점을 해결하고 보다 능동적인 보안 서비스를 제공함을 보였고, 실제 필드에 적용할 수 있음을 확인하였다.

본 논문에서 제안된 능동 보안 기술이 실제 네트워크에 적용된다면 현재의 네트워크 보안 기술이 제공하는 보안 수준 보다 한층 더 강력하고 광범위한 대응이 가능한 보안 수준을 확보할 수 있을 것이다.

참 고 문 헌

[1] Dan Sterne, Active Network Intrusion Detection and Response(AN-IDR), Boeing and NAI Lab., DARPA FTN PI Meeting, Jul., 2000.

[2] Dan Schnackenberg, et. al., Cooperative Intrusion Traceback and Response Architecture(CITRA), DISCEX 2001, Jun., 2001.

[3] S. Kent, R. Ackinson, IP Authentication Header, IETF RFC2402, Nov., 1998.

[4] S. Kent, R. Ackinson, IP Encapsulating Security Payload, IETF RFC2406, Nov., 1998.

[5] 이수형, 나중찬, 손승원, 액티브 네트워크 기반 보안 기술 동향, 한국전자통신연구원 주간기술동향, 제1076호, 2002. 12.

[6] NetGuard Inc., GuardianPro V.5 Release Note V.5, Feb., 2002.

[7] 이영석, 나중찬, 손승원, ESM 개발동향, 한국전자통신연구원 주간기술동향, 2003. 5.

[8] M. Leech, Username/Password Authentication for SOCKS V5, IETF RFC1929, Mar., 1996.

[9] DARPA ITO, Dynamic Cooperating Boundary Controller, Project Introduction in http://www.darpa.mil/ito

[10] ISO/IEC JTC1/SC27 WG1 Meeting, Warsaw, Poland, Oct. 7~11, 2002.

[11] B. Feinstein, et. al., The Intrusion Detection Exchange Protocol (IDXP), IETF draft-ietf-idwg-beep-idxp-07, Oct., 2002.

[12] S. Kent, R. Ackinson, Security Architecture for the Internet Protocol, IETF RFC2401, Nov., 1998.

[13] P. Ferguson, D. Senie, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, IETF RFC2827, May, 2000.

[14] 이영석, 방효찬, 나중찬, 액티브 네트워크 기반의 위조 IP 공격 대응 메커니즘, 한국정보과학회 춘계학술발표논문집, Vol. 4, No.4, 2003.

[15] 김현주, 이수형, 나중찬, 손승원, 액티브 기술을 이용한 DDoS 공격 대응, 한국정보과학회 추계학술발표논문집, Vol. 14, No. 1, 2002.

이 영 석(Young-seok Lee) 정회원

1992년 2월 : 충남대학교 컴퓨터공학과 학사

1994년 2월 : 충남대학교 컴퓨터공학과 석사

2002년 2월 :충남대학교 컴퓨터공학과 박사

1994년~1997년 : LG전자 연구원

2002년~현재 : 한국전자통신연구원 선임연구원

<관심분야> 네트워크보안, 가상사설망, 이동컴퓨팅