제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

능동보안 컴포넌트 개발에 관한 연구

김상영*, 황선명*, 나중찬**
*대전대학교 컴퓨터공학과
**한국전자통신연구원 정보보호기술연구본부
e-mail:jayusop@zeus.dju.ac.kr, sunhwang@dju.ac.kr, njc@etri.re.kr

A Study on Development of Active Network Component

Sang-Young Hwang*, Sun-Myung Hwang*, Jung-Chan Na**
*Dept of Computer Engineering, Daejeon University
**Information Security Technology Division, ETRI

요 약

최근 들어 네트워크 응용 분야의 수요가 기아급수적으로 증가하면서 네트웍 관리자나, 사용자들로부터 네트워크에 대한 요구사항이 증가라고 있으며 이에 대한 서비스들은 QoS(Quality of Service)보장을 요구하고 있다. 그래서 최근에는 네트워크 노드들에 대하여 에이전트 기술이 포함되는 능동네트워크로의 전환이 이루어지고 있다.

본 연구에서는 능동보안 컴포넌트에 대하 살펴보았으며 이에 적용가능한 능동 보안 컴포넌트 아키텍쳐를 제안하고, 능동 보안 컴포넌트를 개발할 수 있는 접근 단계와 명세 작성을 위한 명세서 규격을 제안하였다.

1. 서론

최근 들어 네트워크 응용 분야의 수요가 기아 급수적으로 증가하면서 네트웍 관리자나, 사용자들로부터 네트워크에 대한 요구사항이 증가라고 있으며 이에 대한 서비스들은 QoS(Quality of Service)보장을 요구하고 있다. 그래서 최근에는 네트워크 노드들에 대하여 에이전트 기술이 포함되는 능동네트워크로의 전환이 이루어지고 있다.

능동 네트워크 기술에서도 기존의 네트워크 기술들과 마찬가지로 네트워크에 대한 공격기법의 다양화 및 지능화함에 따라 국가적으로 중요한 정보통신망에 대한 사이버 공격 위험이 증대하고 있다. 이 공격자들의 특징으로는 분산 환경에서 다수 공격 에이전트를 이용하여 특정 상용 서버의 서비스 제공을 마비시키는 분산 서비스 거부 공격의 출현과 해외 해커들의 국내 전산망의 우회 루트를 활용한 사례의 증가 등 사이버 공격 행위가 점차 강력해 지고 있다.

또한 정부부처 및 기업의 모든 정보 유통이 컴퓨터와 인터넷에 크게 의존함에 따라 국내의 해커, 불만그룹, 적성적 내부자 분 아니라 외국정보기관, 군사조직, 테러리스트, 범죄자, 산업경쟁상대 등으로부터의 사이버 공격 위험이 증대되고 있다. 이런 환경 변화에 따라 사이버 공격에 대해 기존 네트워크 보안에 비해 사용자 지향적이고, 능동적이며 좀더 강력한 대응을 할 수 있는 네트워크 보안 기술의 개발 필요성이 대두되었고, 이러한 요구사항에 의해 능동 보안 네트워크가 발생되었다.

그리고 현재 소프트웨어 개발 기본 패러다임이 OOP에서 개별 부품(컴포넌트)에 의한 시스템 개발 방법인 CBD로의 전환이 이루어지고 있다. 이러한 CBD 기법은 향후 유사 시스템 개발시 실행 가능한 독립적인 비즈니스 로직인 해당 컴포넌트를 재사용함으로서 최소한의 노력으로 개발되어 질 수 있으며, 일부 기능의 성능 향상 및 오류 수정을 위하여 해당되는 최소한의 비즈니스 로직 컴포넌트의 수정으로 유지보수시의 노력을 감소할 수 있고, 이렇게

†이 논문은 한국전자통신연구원의 "능동보안 컴포넌트에 관한 연구"의 지원에 의한 것임

CBD기법으로 개발시 향후 개발되어질 시스템에 대하여 품질을 예측할 수 있다.

본 연구에서는 능동 보안 네트워크의 노드 개발시 CBD를 적용하기 위하여 능동보안 네트워크의 요구사항을 분석하고 이에 대한 능동보안 도메인을 분석하며, 분석되어진 내용을 이용하여 능동보안 네트워크에 적용가능한 아키텍처를 정의 및 이들에 대한 분류 및 식별을 하고 해당 컴포넌트에 대한 명세를 작성할 수 있도록 명세 양식을 제안한다.

2. 컴포넌트 아키텍처

2.1 컴포넌트 악키텍처의 정의

일반적으로 컴포넌트 아키텍처는 독립 목적을 가진 관련된 컴포넌트들을 유기적으로 연관시키기 위한 표준 계층 구조를 이야기하며, 이러한 아키텍처는 컴포넌트의 생산, 배포, 획득, 이해, 조립을 위한 레이아웃을 제시하고 다음과 같은 기능을 제공한다.

가) Standard Infrastructure

CBD에 의해 응용 프로그램을 개발하기 위하여 각기 다른 비즈니스 로직이고 재사용 가능한 공통 프로세스를 제공한다.

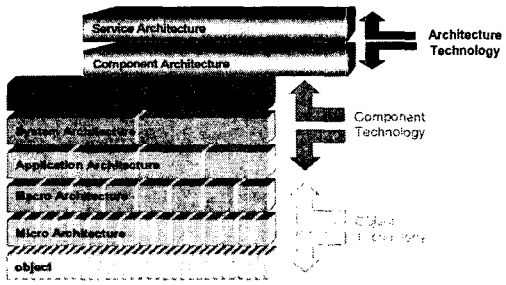
나) Evolution Program Model

개별 컴포넌트들의 조립과 확장을 통한 생산성 있는 소프트웨어 시스템으로의 전개를 위한 모델이다.

2.2 컴포넌트 아키텍처의 기능

컴포넌트 아키텍처는 표준하부 구조와 응용 S/W 구축을 위한 프로세스 구조를 제공하며, 소프트웨어로의 전개 모델을 제시한다. 그리고 다중 플랫폼 상에서 운영 되어지거나 저장소에 저장되어 있는 컴포넌트를 통합하며, End-User에 의한 컴포넌트 식별, 검색, 이해의 메타 정보를 제공한다. 컴포넌트 생성 및 저장을 위한 체계적 스키마를 확보하며, 저장소 구축시 검색과 카탈로깅을 위한 기능을 제공하고, 컴포넌트의 확장 및 조립을 위한 요구 기준을 마련하며, 컴포넌트 분류를 위한 물리적 또는 논리적 계층을 제공한다. 또한 관련된 다른 컴포넌트들을 연관시키기 위한 메소드를 제공한한다.

이러한 아키텍처는 [그림 1]과 같이 하부로부터 Enterprise Architecture 까지 개발 프로세스를 제공한다.



[그림 1] 소프트웨어 아키텍처의 계층구조

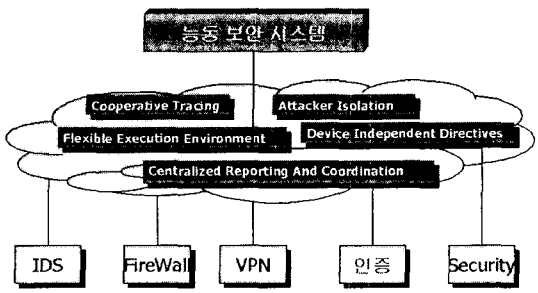
3. 능동보안 컴포넌트

3.1능동보안 컴포넌트

능동보안 컴포넌트의 목적은 특화된 고객(네트워크 관련 종사자 및 해당 도메인을 요청하는 고객) 지향 서비스 및 능동적인 통합 관리 솔루션을 제공하는 것으로서 특징은 다양한 보안 시스템 지원을 가능하게 하기 위한 표준 개발 환경(EJB, COM CORBA.)을 준수하며, 실시간적으로 모니터링 및 보안대응이 가능한 실행성의 인터페이스 통신을 지원하고 능동 보안 네트워크 개발자들에게 실시간 프로그래밍 기술을 제공한다.

3.2 능동 보안 도메인

능동 보안 네트워크를 위한 기술로는 Cooperative Tracing, Attacker Isolation, Flexible Execution Environment, Device Independent Directives, Centralized Reporting and Coordination을 필요로 하며 이러한 요구사항을 분류하면 [그림 2]와 같이 네크워크 침입탐지에 관련된 IDS, 비인가자의 출입을 통제하는 Firewall, 조직 내부자들만을 위한 가상 사설망인 VPN, 허가된 사용자나, 페킷에 관련된 인증, 보안에 관련된 Security의 5개의 서브 도메인으로 분류되어질 수 있다,



[그림 2] 능동 보안 도메인

3.3. 능동 보안 컴포넌트 아키텍처

능동보안 컴포넌트에 대한 도메인 분석을 통해 이에 적용 가능한 아키텍처를 정의하면 주요역할 3가지로 나타내어 질 수 잇다.

가) Stackholder 사이의 의사소통 수단

End User(보안관리자, 네트워크관리자)나 보안시스템 개발자 또는 보안 컴포넌트 개발자들사이에 표준화된 방법을 통하여 의사소통이 원활하도록 한다.

나) 능동보안 시스템 개발의 초기 결정 사항을 정의

구현상의 제약점들을 정의하고 보안 시스템의 기능적인 구조를 제공하며, 보안 시스템 특징들의 선택적 적용이 가능하며, 보안 시스템에 대한 진화적인 프로토타입을 지원하고 변경 관리가 용이 하다.

다) 재사용 모델

개발자들은 유사 능동 보안 관련 시스템 개발시 선택적으로 비즈니스 로직을 적용하여 재사용할 수 있다.

능동보안 컴포넌트 아키텍처는 능동보안 도메인 컴포넌트와 이들을 처리할 수 있는 분산 서비스가 (EJB, COM CORBA)가 포함되어져 있으며, 공통 컴포넌트로의 이원화, 컴포넌트 참조 모델에서 지원하는 공통 컴포넌트 그리고 능동 보안 컴포넌트 모델 3가지로 아키텍처의 기능을 나눌 수 있다.

가) 공통 컴포넌트로 이원화

능동 보안 도메인 내에 존재하는 컴포넌트 중 필수로 사용되어져야 하는 컴포넌트 그룹과 선택적으로 사용되어 질 수 있는 컴포넌트 그룹으로 이원화 시킨다.

나) Componentr REference Architecture에서 지원하는 공통 컴포넌트

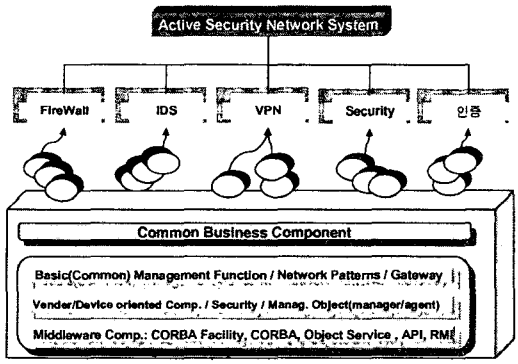
IBM의 센프란시스코 프로젝트와 같은 참조 모델을 적용함으로서 분산 환경 구축 및 객체서비스 그리고 미들웨어를 위한 컴포넌트를 제공 받는다. 그리고 벤더나 장비 지향적 속성의 확장성을 포함하는 베이스 컴포넌트를 제공받는다.

다) 능동 보안 컴포넌트 모델

능동 보안 컴포넌트는 총 3개의 계층으로 나누어서 분류한다.

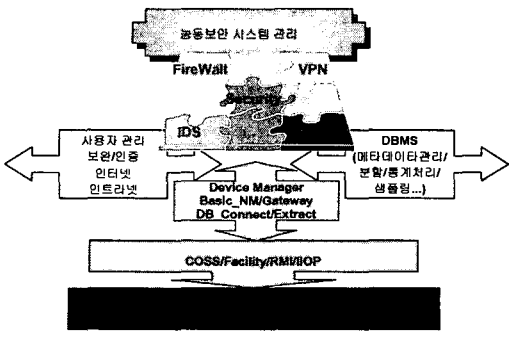
- Layer 1 : 개별적인 단위 보안 컴포넌트
- Layer 2 : 보안 관리 컴포넌트
- Layer 3 : 관리 응용 컴포넌트

능동 보안 아키텍처에 능동보안 도메인을 적용시키면 [그림 3]와 같이 되며 하부의 하드웨어에 관련된 컴포넌트와 분산 및 배포에 대한 컴포넌트는 Base 레이어에 존재하고 네트워크 하부구조와 능동 보안 네트워크를 위한 컴포넌트가 아니어도 다른 도메인과 공용으로 사용할 수 있는 컴포넌트는 Common Business Component로 분류하며, 그 상위 계층에 능동 보안 컴포넌트 모델에서 제시한 3개의 레이어에 의한 컴포넌트 분류를 두고, 이들 3개의 레이어가 모여 능동 보안 도메인 내에 존재하는 하나의 서브 도메인을 구성한다. 그리고 마지막으로 서브도메인들이 모여 하나의 능동 보안 도메인으로 분류 되어진다.



[그림 3] 능동 보안 네트워크 아키텍처

이러한 능동보안 컴포넌트 아키텍처에 의해 [그림 4]와 같이 조립되어 능동 보안을 위한 개발 프로세스가 완성되어 지게 된다.



[그림 4] 능동 보안 컴포넌트 개발 프로세스

3.4 능동보안 컴포넌트 개발 접근 단계

능동 보안 컴포넌트를 개발하기 위한 접근 단계는 다음과 같이 총 5단계로 이루어져 있다.

가) 능동보안 도메인 분석

CBD에서 도메인 및 시스템 요구 분석을 통해 목표로 하는 능동 보안 시스템에 대한 전반적인 구성을 이해한다.

나) 능동보안 시스템의 계층적 구조정의

능동보안 시스템에서 요구되는 기술들을 분류 하고 계층화 한다. 그리고 분류되어진 기능적 계층은 컴포넌트 식별 및 능동 보안 컴포넌트 아키텍처 정의의 기초를 제공한다.

다) 능동보안 시스템의 컴포넌트 계층 정의

CBD 기반의 능동보안 시스템 구축을 위해 요구되어지는 컴포넌트 획득과 조립의 기본 시나리오를 정의한다.

라) 컴포넌트를 식별하고 계층에 매핑

능동 보안을 위해 필요한 컴포넌트를 식별하고 이를 능동 보안 시스템을 위해 정의된 컴포넌트 아키텍처에 매핑 시킨다.

마) 컴포넌트 생성 명세 정의

식별된 컴포넌트들을 실제 개발하고, 시스템 개발자가 식별하며 획득하기 위해 컴포넌트명세를 제안된 표기법에 따라 작성한다.

3.5 능동 보안 컴포넌트 명세

일반적인 컴포넌트 명세는 개발하기 전에 작성되어 지는 문서로서 명확한 의미적인 프러그인 지점을 확보하고 구현 및 보완, 성능 조건을 명시하여 컴포넌트 식별과 품질적 계층화를 할 수 있으며, Component Diagram을 제공하여 컴포넌트 내부 구조나 또는 다른 컴포넌트들 사이의 상호관계를 이해하도록 한다. 그리고 해당 컴포넌트의 레이어를 제시하고 구현 환경을 제시함으로서 개발자가 식별 및 조립시 환경을 알 수 있도록 한다.

그래서 본 연구에서는 <표 1>과 같이 능동 보안 컴포넌트를 위한 명세 양식을 제안하였다.

<표 1> 능동보안 컴포넌트 명세

컴포넌트 명	컴포넌트 식별 이름
영문 명	컴포넌트 식별 영문 이름
분류코드	컴포넌트 분류코드
컴포넌트 개요	컴포넌트의 개략적 설명
용어 및 약어	명세에 사용되어지는용어 정리
Component Context Diagram	명세하고자 하는 컴포넌트와 그 컴포넌트의 외부 객체와의 관계
Component Diagram	컴포넌트 자체의 명세를 간략하게 설명하기 위한 컴포넌트 이름과 컴포넌트 인토페이스로 구성
Component Interaction Diagram	컴포넌트와 외부 객체들이 어떤식으로 상호 작용하는가를 명세
Component Interface	컴포넌트가 제공하고 제공받는 인터페이스 정보
Version	컴포넌트 버전 정보
Vender	컴포넌트 제공자(업체)
Implement Elements	Base Model
Layer	컴포넌트가 속한 계층

3,6 분류코드

분류코드는 개발자가 컴포넌트를 식별하는 중요한 정보중의 하나로서 다음과 같은 표기법에 의해 작성되어진다.

{A|B|C|D}+AN-X1-X2-X3-X4

{A|B|C|D} : 계층 레이어

AN : Active Network Domain

X1 : 서브도메인 분류번호

X2-X3 : 능동 보안 컴포넌트 모델의 3계층에 대한 분류번호

4. 결론

본 연구에서는 능동보안 컴포넌트에 대하 살펴보았으며 이에 적용가능한 능동 보안 컴포넌트 아키텍처를 제안하고, 능동 보안 컴포넌트를 개발할 수 있는 접근 단계와 명세서 작성을 위한 명세서 규격을 제안하였다.

향후 연구로는 능동보안 시스템을 위한 컴포넌트 모델을 개발하여 컴포넌트 명세에 기반한 능동 보안 시스템의 개발 레이아웃을 제시하고 능동 보안에 대한 컴포넌트를 식별하여 능동보안 컴포넌트 체계화를 정립하며 명세화 작업을 향후 연구 과제로 한다.

참고문헌

[1] http://www.kanf.or.kr/

[2] 네트워크보안, 차세대 인터넷을 위한 능동보안 기술 백서, ETRI, 2001.

[3] http://www.n3soft.com