논문 04-29-6C-17 한국통신학회논문지 '04-6 Vol.29 No.6C

# 분산보안시스템을 위한 적응형 침입감내 모델 및 응용

정회원 김 영 수*, 최 흥 식**

# Adaptive Intrusion Tolerance Model and Application for Distributed Security System

Young Soo Kim*, Heung Sik Choi** *Regular Members*

요 약

오늘날 정보에 대한 보안성보다는 가용성과 서비스의 지속성이 중요한 관심사가 되고 있다. 이는 개인과 기업이 점차 분산 시스템에 의존해서 중요 서비스에 액세스하고 핵심적인 업무를 처리하기 때문이다. 따라서 보안상 취약점에 대한 공격이 발생하더라도 서비스를 지속적으로 제공할 수 있는 시스템의 능력이 요구된다. 이의 해결책으로 다양한 보안 메커니즘과 적응 메커니즘을 사용하는 적응형 침입감내기술이 제시될 수 있다. 본 논문은 분산 시스템의 개발 구조의 개선과 보안을 위한 적응형 침입감내모델을 제안하고 이의 검증을 위하여 코바의 보안 모델로부터 분리 통합되는 형태로 침입감내시스템을 구현하였다.

키워드 : 분산시스템, 보안메커니즘, 적응메커니즘, 침입감내시스템, 적응형 침입감내모델

ABSTRACT

While security traditionally has been an important issue in information systems, the problem of the greatest concern today is related to the availability of information and continuity of services. Since people and organizations now rely on distributed systems in accessing and processing critical services and mission, the availability of information and continuity of services are becoming more important. Therefore the importance of implementing systems that continue to function in the presence of security breaches cannot be overemphasized. One of the solutions to provide the availability and continuity of information system applications is introducing an intrusion tolerance system. Security mechanism and adaptation mechanism can ensure intrusion tolerance by protecting the application from accidental or malicious changes to the system and by adapting the application to the changing conditions. In this paper we propose an intrusion tolerance model that improves the developmental structure while assuring security level. We also design and implement an adaptive intrusion tolerance system to verify the efficiency of our model by integrating proper functions extracted from CORBA security modules.

## Ⅰ. 서 론

네트워크 컴퓨팅 환경이 가속화되고 더욱이 인터넷이 기업의 주요 네트워크 인프라로 활용되면서 기업의 IT자원들을 네트워크로 연결하여 사용하는 분산 시스템의 구축이 활성화되고 있다. 그러나 분산 시스템은 구조적 특성상 불법적인 제3자에게 네트워크상의 시스템 노드들이 노출되어 있고 또한 각 시스템 노드가 협업 작업을 진행할 때 고의적인 방해와 공격으로 정상적인 작업수행이 불가능해지는 위험성을 가지고 있다[5]. 따라서 이러한 불법적인 공격에 대하여 시스템 노드와 자원을 보호하고 서비스를 지속적으로 제공할 수 있는 시스템의 능력이 요구된다. 이에 대한 한 가지 해결책으로 침입감

*국민대학교 정보관리학과
**국민대학교 비즈니스 IT학부
논문번호 : #KICS2004-05-004 접수일자 : 2004년 5월 10일

내기술이 제시될 수 있다.

침입감내기술은 우발적 사고 또는 악의적 공격에 대한 해결책을 찾을 때까지 적절한 대응을 통해 서비스의 품질 저하를 방지하면서 일정시간 동안 중요한 서비스를 지속적으로 제공할 수 있도록 하는 기술이다[2.4]. 이러한 침입감내는 보안 메커니즘과 적응 메커니즘을 이용하여 실현할 수 있다. 보안 메커니즘은 우발적 또는 악의적인 공격으로부터 애플리케이션을 보호함으로써 침입감내 기능을 강화할 수 있고 적응 메커니즘은 시스템의 상태 변화에 적응함으로써 침입감내 기능을 제공할 수 있다[10]. 따라서 침입감내 기능의 향상을 위하여 다양한 보안 메커니즘과 적응 메커니즘을 통합하여 사용할 필요성이 있다.

이를 위하여 본 논문에서는 그림 1과 같은 방법에 따라 코바로부터 분리 통합되는 형태로 관리되는 적응형 침입감내 모델을 제안하고 이를 사용하여 침입감내응용시스템을 코바 미들웨어상에서 구현하여 모델의 실용성을 검증하였다.

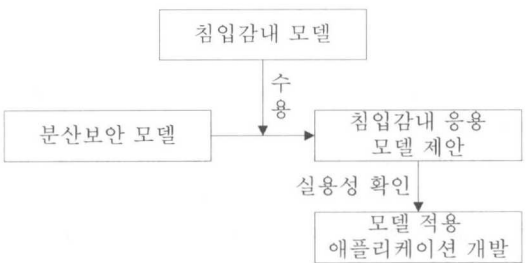


그림 1. 연구 모델

본 논문은 다음과 같이 구성된다. 2절에서는 코바의 분산보안시스템과 HACQIT시스템의 침입감내모델을 분석하고 3절에서는 침입감내시스템과 응용모델을 제안한다. 4절에서는 모델의 실용성을 검증하기 위하여 침입감내시스템을 구현한다. 5절에서는 결론과 시사점을 기술한다.

## Ⅱ. 침입감내시스템의 연구 모델

### 2.1 분산 시스템의 보안 모델

코바로 대표되는 분산객체기술은 객체지향의 이점을 분산 컴퓨팅에 적용하는 것에 의해 개발의 복잡성과 상호운용성의 문제를 해결하려 하고 있다[8]. 객체지향기술에서는 서비스를 제공하는 서버로서의 객체와 서비스를 이용하는 클라이언트가 객체의 인터페이스를 경계로 명확하게 구별되어 서버의 구현부를 클라이언트로부터 은폐시킨다. 또한 분산 기술은 네트워크 프로토콜을 은폐하고 기존 시스템의 서비스를 포장하는 것에 의해 기존 시스템을 통합한다.

그림 2는 코바의 클라이언트-서버 모델을 표현하고 있다. 객체 리퍼런스(reference)는 객체의 식별을 위한 정보를 포함한 데이터이고 객체 생성시 만들어지기 때문에 클라이언트는 생성된 객체 리퍼런스를 획득하여야 객체의 서비스를 이용할 수 있다. 클라이언트는 획득한 객체 리퍼런스를 사용하여 원격 객체를 마치 동일한 기억공간에 있는 것처럼 사용한다. 이는 운영체제에 의하여 지원되는 가상 메모리 기법처럼 가상의 실체인 코바 객체를 클라이언트가 호출하면 구현객체로의 매핑은 ORB에 의하여 수행된다. 코바 애플리케이션 개발은 인터페이스 정의 언어(IDL: Interface Definition Language)로 기술한 서비스 인터페이스를 컴파일하여 클라이언트 스터브(stub)와 서버로서의 역할을 수행하는 구현객체 스켈리톤(skeleton)을 생성한다. 스터브와 스켈리톤은 구현 객체에 대한 메서드의 호출과 응답을 메시지의 형태로 포장하고언마샬링(unmarshalling)한다.

ORB(Object Request Broker)는 메시지에 IIOP(Internet Inter ORB Protocol)헤더를 부착하거나 역캡슐화하고 POA는 구현객체에 대한 인스턴스의 생성과 제거를 수행한다.

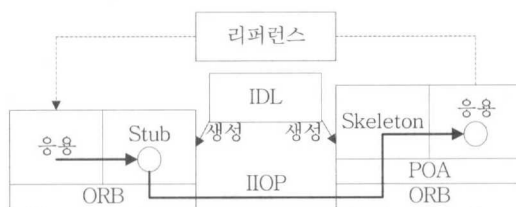


그림 2. 코바 시스템의 구조

이러한 분산 컴퓨팅 환경은 보안 문제를 확대한다. 이는 침입자가 공격을 수행할 수 있는 다양한 액세스 포인트를 제공하는 보안에 취약한 구조를 분산 시스템이 가지고 있기 때문이다. 따라서 코바는 접근 제어를 수행하는 다양한 보안 서비스를 제공하도록 규정하고 있다. 그림 3과 같이 코바 분산

객체 시스템은 미들웨어상에서 정책 기반의 보안 메커니즘을 사용하여 보안을 실현함으로써 보안계층과 응용 계층을 분리한다[1].

보안 관리자는 네트워크에 있는 자원들이나 서비스의 보안 수준을 정의하기 위하여 정책들을 생성한다. 정책 기반 보안 메커니즘은 이들 보안 정책들을 이용하여 정책에 의해 변경된 사항을 클라이언트/서버 응용 시스템에 적용한다. 보안정책은 그룹화 메커니즘인 도메인, 특권, 사용권한을 사용하여 일괄적으로 설정할 수 있다. 즉 보안 관리자는 객체를 도메인에 포함시키고 이들 객체들의 그룹에 대하여 일률적으로 보안정책을 설정하거나 사용자들을 동일 특권속성으로 그룹화하여 사용자 그룹에 대하여 보안정책을 실시한다. 그리고 객체의 메서드에 대해서는 동일한 사용 특권을 부여함으로써 메서드(method)를 그룹화하고 그룹화된 특권에 대하여 보안정책을 적용한다.

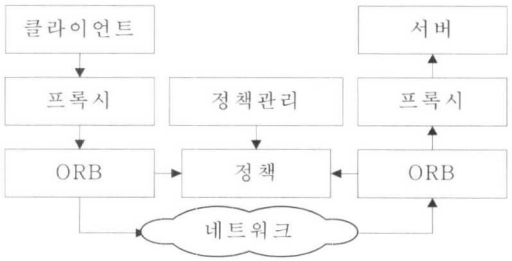


그림 3. 코바의 보안 메커니즘

### 2.2 HACQIT시스템의 침입감내모델

침입방지시스템과 침입탐지시스템을 뚫고 침입하는 고도의 기술을 가진 침입자들의 불법적인 침입이나 공격에 대응하여 일정시간동안 서비스를 지속할 수 있는 응용시스템은 보안시스템으로부터 얻은 침입 정보를 사용하여 상태 변화에 적응 할 수 있어야 하고 동일 서비스를 제공하는 대체 서버나 중복 사이트로 전환할 수 있어야 한다.

미국의 DARPA 프로젝트인 HACQIT(Hierarchical Adaptive Control of Quality of service for Intrusion Tolerance)시스템의 침입감내모델은 응용시스템에 쉽게 적용할 수 있는 대표적인 보안모델이다[7]. HACQIT 시스템은 그림 4와 같이 메인서버와 중복서버 그리고 방화벽, 컨트롤러 그리고 샌드박스로 구성된다. 사용자의 서비스 요청은 방화벽을 통과한 후에 스위치에 의해서 메인서버에 전달된다. 컨트롤러는 메인서버로 전달되는 요청 메시지를 인터셉터하여 허용된 요청인 경우에는 두 서버에게 포워드한다. 두 서버로부터 수신한 응답 결과값이 상이한 경우에는 결함으로 간주하여 샌드박스를 통하여 오류의 원인을 확인하여 중복서버를 메인서버로 전환하고 복구절차를 수행시킨다. 두 서버의 가상 인스턴스를 유지하고 있는 샌드박스는 결함을 야기한 요청 메시지를 입력으로 생성한 결과값이 프로세스 서버의 인스턴스와 동일한 경우에는 침입으로 간주하여 방화벽으로 하여금 이를 차단하게 한다.

이 모델은 구조가 간단하기 때문에 구현이 용이하다는 장점은 있으나 침입을 탐지하는 기능이 미약하고 서비스에 대한 요청 메시지가 서버로 바로 전달되지 않기 때문에 시간적 추가 비용이 존재하는 단점이 있다. 그리고 컨트롤러와 샌드박스가 외부에 노출되는 경우에 새로운 취약점이 될 수 있다.

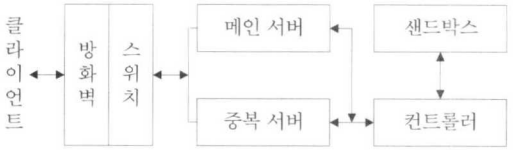


그림 4. HACQIT시스템의 침입감내 모델

## Ⅲ. 침입감내시스템의 응용 모델 및 구조

침입감내시스템은 침입 발생 후에도 정보의 가용성과 서비스의 지속성을 유지하는 것을 목표로 한다. 이를 실현하는 응용시스템은 다양한 보안 메커니즘과 적응 메커니즘을 사용하여 구축된다. 적응 메커니즘은 보통 중복을 사용하여 실현되나 이는 서비스의 가용성은 증가시킬 수 있는 반면 노출 가능성을 확대하게 되어 공격 위협은 증가한다[3]. 따라서 적응 메커니즘을 사용하되 적절한 보안 메커니즘에 의하여 보안성을 강화시키는 대비책이 있어야 한다. 또한 침입감내 애플리케이션의 개발구조의 개선과 보안 정책의 변화에 쉽게 적응할 수 있도록 하여야 한다.

이를 위하여 분산 보안 모델로부터 침입감내 기능을 분리하여 확장하는 형태로 침입감내 시스템을 구현할 수 있는 응용모델을 제안한다. 이는 다양한 보안시스템을 수용할 수 있고 응용서비스의 제공이 가능한 서버시스템으로 요청 메시지를 직접 전송함

으로써 분석대상 연구시스템인 HACQIT시스템의 침입감내 모델이 가지고 있는 보안위협에 대한 탐지 취약성과 요청메시지의 처리지연에 대한 해결책을 제공한다.

### 3.1 침입감내시스템의 응용모델

침입감내시스템은 보안과 적응 메커니즘을 사용하여 시스템에 대한 불법적인 침입이나 공격에 대한 대응책 마련을 위하여 시도되는 정보보호기술이다[6]. 보안 메커니즘은 취약성분석시스템과 침입차단시스템과 같은 공격 예방 기술과 미처 방어하지 못한 취약점을 뚫고 침입하는 공격을 탐지하는 침입탐지시스템과 같은 침입대응기술인 반면 적응 메커니즘은 침입의 결과로 발생된 결함을 감내할 수 있는 중복관리 시스템과 대역폭 관리 시스템과 같은 침입 허용 기술이다.

침임감내시스템의 응용 모델로 그림 5와 같은 코바 보안 모델을 확장한 형태를 제안한다. 상태관리 객체가 보안 메커니즘과의 인터페이스 역할을 수행하도록 하고 대리자 객체는 서버 중복을 통한 적응 메커니즘과의 상호작용을 표현한다. 분산 시스템의 보안성을 보장하기 위하여 코바 보안 모델은 미들웨어상에서 정책 객체를 사용하여 보안성을 보장하고 있는[1] 반면 제안한 응용 보안 모델은 침입감내 기능을 갖는 보안계층을 추가하여 정보의 가용성과 서비스의 지속성을 유지한다[11].

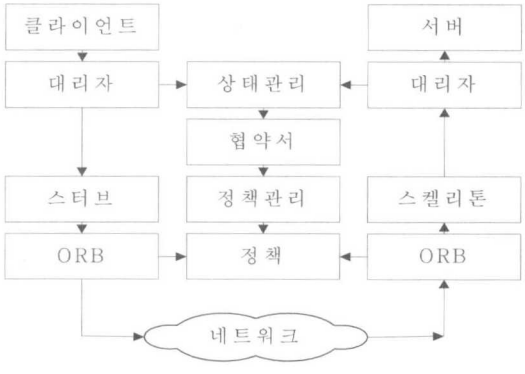


그림 5. 침입감내시스템의 응용 모델

### 3.2 침입감내시스템의 응용아키텍쳐

분산 보안 시스템의 침입감내 응용 모델의 구현은 모델의 타당성을 검증하고 미들웨어 계층에서 다양한 보안 메커니즘의 통합 방법과 적응 메커니즘의 활용 방법을 제시하는데 있다. 이를 위한 시스템 아키텍쳐는 그림 6과 같다. 상태관리 객체는 침입차단 및 침입탐지 시스템과 같은 보안 시스템과의 인터페이스를 수행하는 보안 메커니즘을 실현하고 대리자 객체는 동일한 서비스를 제공하는 중복되어 있는 서버와의 상호작용을 통해 침입을 당한 경우에도 필수 서비스가 지속될 수 있도록 적응 메커니즘을 적용하여 구현한다. 협약서 객체는 침입감내를 위한 요구사항을 기술하는 객체로 서비스 품질 요구사항과 지속성 요구사항을 표현한다.

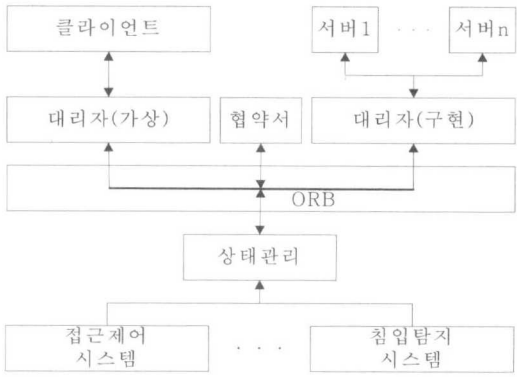


그림 6. 침입감내시스템의 응용아키텍쳐

제안시스템은 침입감내 응용을 위한 프레임웍을 제공하는데 목적을 두고 있다. 이를 위하여 접근제어 시스템과 침입탐지시스템 그리고 지연감시시스템와 같은 보안 시스템은 제안시스템의 통합된 부분이 아니다. 따라서 응용 아키텍쳐를 구성하는 보안 메커니즘은 침입감내기능에 따라 선별적으로 통합하여 사용할 필요가 있다.

### 3.3 침입감내 시스템의 응용컴포넌트

협약서 객체가 관리하는 QoS(Quality of Service) 매핑 구조는 그림 7과 같다. 이는 침입감내 서비스의 수준을 설정하는 역할을 한다. 협약서 객체는 시스템의 상태를 나타내는 모드와 유의한 범주의 상태값을 매핑하고 있는 리스트를 유지관리하는 객체로 상태관리객체로부터 상태값을 획득하여 침입감내 수준을 결정하는 기능을 수행한다. 협약서 객체는 QoS매핑 구조의 상태모드 필드값으로 정상모드, 지연모드, 위험모드, 침입모드를 설정할 수 있고 상태범주 필드는 상태값의 범위를 표현한다.

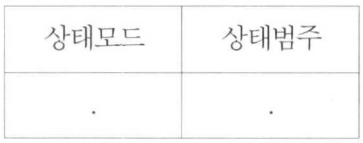


그림 7. 협약서 객체의 구조

상태관리객체의 구조는 그림 8과 같고 보안 시스템과의 인터페이스를 위하여 IDL로 구현한 래퍼(Wrapper)객체를 사용하여 시스템의 상태값을 얻는다. 래퍼 객체는 보안 시스템이 제공하는 서비스에 대한 인터페이스를 캡슐화하고 있는 객체로서 상태관리객체가 보안시스템의 서비스를 이용할 수 있게 한다.

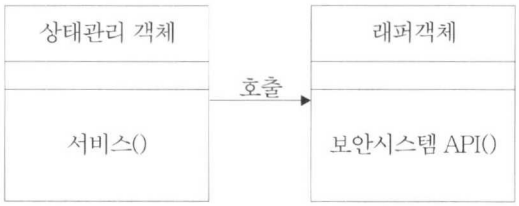


그림 8. 상태 관리 객체 모델

상태관리객체의 서비스 기능은 그림 9와 같고 보안시스템이 미리 필터하여 송신한 보안관련 데이터를 재필터링하여 침입감내의 조건에 부합되는 보안상태값을 생성하여 대리자객체에게 전송한다.

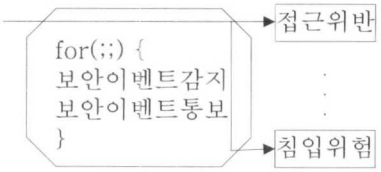


그림 9. 상태관리객체의 서비스 기능

대리자 객체의 모델은 그림 10과 같다. 대리자 객체는 시스템의 상태 모드에 따라 리다이렉트되는 서버를 선정하는 역할을 수행한다. 예를 들어 서비스품질수준이 정상 모드에 해당되는 경우와 지연 모드인 경우에는 인증기능이 없는 메인서버에게로 요청 메시지를 전달하여 처리하고 위반 모드와 침입 모드인 경우에는 인증기능을 수행하는 중복서버에게로 요청메시지를 전송하여 처리한다.

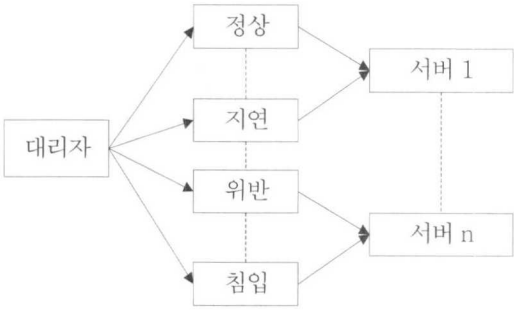


그림 10. 대리자 객체의 모델

대리자 객체의 서비스 기능은 그림 11과 같다. 대리자객체는 협약서 객체가 리턴해주는 침입감내수준에 따라 서비스 품질을 유지할 수 있고 동일서비스를 제공하는 서버에게로 연결을 설정해주는 역할을 한다.

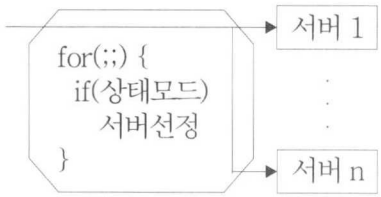


그림 11. 대리자 객체의 서비스 기능

## Ⅳ. 응용 시스템의 설계 및 모델의 검증

### 4.1 응용시스템과 통합 구조

침입감내모델을 적용한 응용시스템의 사례로서 공기업 정보공개시스템의 개발에 관한 연구시스템

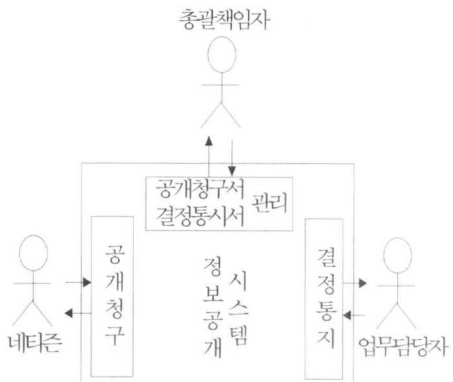


그림 12. 공개정보시스템의 아키텍처

[12]을 선정하였다. 공기업 정보공개시스템의 기본 구조는 그림 12와 같다. 네티즌이 정보공개를 청구하면 총괄책임자의 역할을 수행하는 정보시스템 관리자가 이를 접수받아 각 해당 업무 담당자에게 정보공개청구서를 배부하면 업무담당자는 공개여부를 결정하여 결정내용을 데이터베이스에 등록하여 청구인이 이를 열람할 수 있는 형태로 운영되고 있다.

그림 13은 정보공개시스템과 분산객체시스템의 통합을 위하여 미들웨어계층에서 객체포장 모델을 사용하여 구성한 응용시스템구조이다. 포장객체시스템은 공개정보시스템의 API를 호출하는 모든 메서드를 캡슐화하고 있다[11]. 클라이언트 객체가 공개정보시스템의 기능을 필요로 하는 경우 포장객체시스템에게 메시지를 보내면 포장객체시스템은 공개정보시스템의 API를 호출함으로써 공개정보서비스를 제공받는다. 또한 기존 서비스를 확장하고 있는 구현객체를 개발하여 이를 이용할 수 있다. 즉 포장객체는 기존 시스템의 모든 서비스를 포장하는 대신 유용한 서비스만을 선별하여 포장하는 메커니즘을 사용할 수 있다.

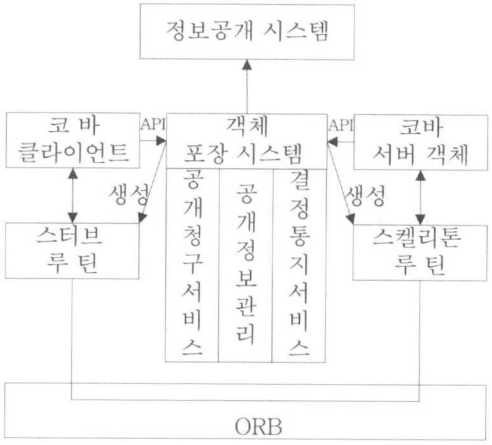


그림 13. 코바 응용시스템으로의 통합 구조

### 4.2 침입감내응용시스템의 구조

정보공개시스템의 서비스를 코바 서버객체로 캡슐화하여 구현한 응용시스템을 침입감내 기능을 갖도록 변경한 침입감내응용시스템의 구성도는 그림 14와 같다. 침입감내응용모델은 침입감내기능의 구현을 비즈니스와 보안 구현으로부터 분리함으로써 애플리케이션과 보안 그리고 침입감내 기능의 개발에 대한 역할을 분담하여 개발 작업을 효율적으로 수행할 수 있고 다양한 침입감내 모듈을 코바에 플러그인하여 사용될 수 있는 유연성을 제공한다. 또한 침입감내기능의 분리구현은 침입감내를 위한 자동화도구를 개발하여 소프트웨어의 생산성을 증가시킬 수 있는 이점을 제공한다.

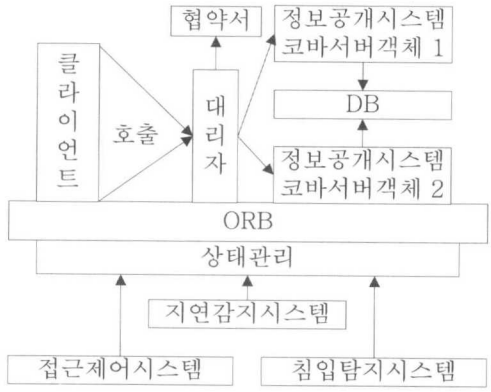


그림 14. 침입감내응용시스템

그림 15는 침입감내시스템을 구성하는 협약서 객체와 상태관리객체 그리고 대리자 객체사이의 인터페이스를 위하여 공통적으로 사용되는 데이타구조를 보여주고 있다. 데이타구조는 지연시간과 액세스 위반, 침입탐지에 대한 상태값을 탑재할 수 있도록 정의되어 있다. 상태관리객체는 보안 시스템과의 상호작용을 통하여 인터페이스 데이터구조에 시스템의 상태값을 설정하고 협약서 객체는 이를 이용하여 QoS매핑구조 데이터를 참조하여 침입감내수준을 결정한다. 대리자 객체는 협약서 객체가 리턴해주는 침입감내수준에 따라 클라이언트와 연결할 서버를 선정하는 역할을 수행한다.

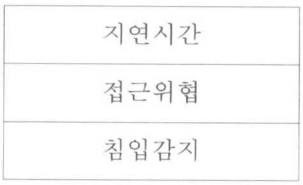


그림 15. 인터페이스 데이터구조

### 4.3 침입감내 응용 모델의 검증

침입감내 응용 모델의 실용성을 확인하기 위한 검증방식은 침입감내 응용 모델을 적용한시스템을 코바시스템를 구성하는 분산 보안 인터페이스의 상위계층으로 구현하는 방법과 코바시스템에서 직접

구현하는 방식을 비교 분석하였다. 그림 16은 침입감내응용모델에 대한 실용성 평가 모델을 보여주고 있다. 보안 인터페이스를 이용한 구현 방식은 침입감내기능을 코바 보안의 통합 모델인 인터셉터를 상속하여 구현하였고 코바 미들웨어를 이용한 구현 방식은 침입감내 응용모델을 POA(Portable Object Adapter)의 구현 클래스로부터 직접 상속을 받도록 선언하여 구현하였다[9].

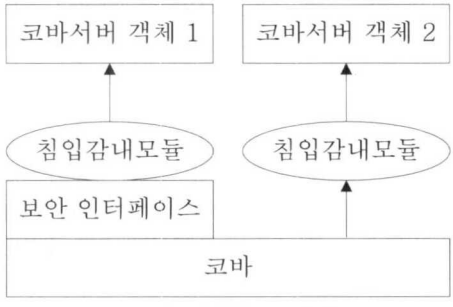


그림 16. 실용성 평가 모델

침입 감내 응용 모델의 실용성을 확인하기 위한 모의실험은 셀러론 850MHz와 윈도우즈 2000 운영체제 환경하에서 표 1과 같이 상태값을 상이하게 하여 응답 메시지를 얻는데 소요되는 시간을 측정하여 실험하였다. 상태모드는 정상, 지연, 위반, 침입으로 구별하고 표 2와 같이 정상과 지연 모드인 경우에는 정보공개시스템이 제공하는 서비스를 캡슐화하고 있는 코바서버객체 1로 표현된 메인 서버 객체를 통하여 서비스를 제공하고 위반과 침입모드인 경우에는 코바서버객체 2로 묘사된 동일 서비스를 제공하는 인증기능을 갖는 중복 서버를 사용하여 서비스를 제공받도록 구현하여 모의실험을 행하였다.

표 1. 입력 상태값

| 지연시간 | 접근위반 | 침입유무 |
|---|---|---|
| 200 | 0 | 0 |
| 300 | 5 | 1 |
| . | . | . |
| . | . | . |

표 2. 서버의 선정과 상태모드

| 상태모드 | 연결서버 |
|---|---|
| 정 상 | 메인서버 |
| 지 연 | |
| 위 반 | 중복서버 |
| 침 입 | |

모의실험을 통한 결과값은 표 3과 같고 코바의 보안 인터페이스를 상속받아 구현한 침입감내 응용모듈을 코바 시스템에 플러그인하여 구현한 침입감내응용시스템이 POA를 사용하여 침입감내모델을 구현한 응용시스템보다 응답 메시지를 제공 받는데 소요되는 시간이 약간 느리다는 것을 알 수 있다.

이는 보안 인터페이스 방식의 경우에는 초기화 작업의 수행 후에 침입감내 모듈의 인스턴스 과정이 수행되는 반면 미들웨어 접근 방식의 경우에는 직접 객체의 인스턴스 과정이 수행되기 때문에 수행 속도의 면에서 미들웨어 접근방식의 결과치가 약간 우수하게 나왔음을 확인 수 있다. 또한 침입감내기능을 갖는 분산 보안 시스템은 코바시스템을 통하여 코바의 보안시스템 및 응용시스템과 분리되는 형태로 구현하여 통합하고 있다.

표 3. 서비스요청 응답 소요시간

| 상태모드 | 보안인터페이스방식 | 미들웨어방식 |
|---|---|---|
| 정 상 | 0.35 | 0.32 |
| 지 연 | 0.45 | 0.41 |
| 위 반 | 0.53 | 0.52 |
| 침 입 | 0.56 | 0.54 |

## V. 결 론

오늘날 정보에 대한 비밀성 보다는 정보의 가용성과 서비스의 지속성이 중요한 관심사가 되고 있다. 이는 개인과 기업이 점차 분산 시스템에 의존해서 중요 서비스에 액세스하고 핵심적인 업무를 처리하기 때문이다. 따라서 보안 취약점에 대한 공격이 발생하더라도 서비스를 지속적으로 제공할 수 있는 시스템의 능력이 요구된다. 이의 해결책으로 다양한 보안 메커니즘과 적응 메커니즘을 사용하는 적응형 침입감내기술이 제시될 수 있다. 이러한 침입감내기술은 다양한 보안 메커니즘과 적응 메커니즘을 사용하여 실현할 수 있다.

보안 메커니즘은 시스템의 공격으로부터 애플리케이션을 보호함으로서 서비스를 지속적으로 제공할 수 있는 반면 침입감내 메커니즘은 시스템에 대한 악의적 공격이 발생하여도 공격으로 인한 변화에

애플리케이션을 적응시킴으로써 중요한 서비스를 지속적으로 제공하는 것이다.

본 논문에서 제안하고 있는 침입감내 응용 모델은 코바 보안 모델로부터 분리 확장되는 형태로 침입감내 기능을 제공함으로써 개발구조를 개선하고 침입감내 모듈의 재사용을 향상시킬 수 있다. 또한 급속하게 늘어가고 있는 침해사고에서 애플리케이션이 생존할 수 있도록 함으로써 시스템의 신뢰성과 안정성을 높여 줄 수 있을 것으로 기대된다. 향후 QoS로 표현되는 침입감내 서비스의 수준과 서비스 요구사항 그리고 보안 시스템으로부터 얻으려는 상태 정보를 명세화할 수 있는 자동화 도구에 대한 연구가 필요하다.

## 참 고 문 헌


[1] Blakley, B., R. Blakley and Soley, R.M., CORBA Security: An Introduction to Safe Computing with Objects, Addison-Wesley, 2000.

[2] Randell, B, "Dependability - Unifying Concept", Computer Security, Dependability & Assurance: From Needs to Solutions, 1998.

[3] Ebert, C., "Dealing with Nonfunctional Requirements in Large Software Systems," Annals of Software Engineering, Volume 3, pp. 367-395 September 1997,

[4] Ellison, R.J., et. al., "Survivable Systems: An Emerging Discipline," Procedings of the 11th Canadian Information Technology Security Symposium(CITSS), Ottawa, Ontario Canada, pp.10-14, May, 1999.

[5] Feiyi Wang, et. al., "SITAR: A Scalable Intrusion-Tolerant Architecture for Distributed Services", Proc. of 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, NY, pp87-97, June 2001.

[6] Fisher, D. A. and H.F. Lipson, "Emergent Algorithms-A New Method for Enhancing Survivability in Unbounded Systems," Proceedings of the 32nd Annual Hawaii International Conference on System Sciences, Maui, Hawaii, (HICSS-32), IEEE Compuer Society, pp.5-8, January, 1999.

[7] Just, J., et.al., "Intrusion Tolerance through Forensics-based Attack Learning", Proc. of the ICDSN 2002 Supplementary Volume, pp.35-43. June 2002.

[8] Orfali, R. and D. Harkey, Client/Server Programming with JAVA and CORBA, John Wiley & Sons, 1998.

[9] Rugaber, S. and J. White. Restoring a legacy: Lessons learned. IEEE Software,15(4): pp.28-33, July-Aug, 1998.

[10] Webber, et. al.. Defense-enabled applications". In Proceedings of the 2nd DARPA Information Survivability Conference and Exposition, 2001.

[11] 김영수, 최흥식 "보안 인터페이스의 통합을 위한 객체포장 모델 및 응용" ,한국통신학회논문지, 제 29권 제 2호, pp. 333-341, 2004년.

[12] 김영수, "한국통신 홈페이지 KT 정보공개시스템 개발에 관한 연구", 한국통신연구보고서, 2000.



김 영 수(Young Soo Kim) 정회원

1989년 2월:전북대학교 회계학과 졸업(경영학 학사)
1992년 2월:경희대학교 경영학과 졸업(경영학 석사)
2003년 8월:국민대학교 정보관리학과 졸업 (정보관리학박사)
<주관심분야> 전자상거래, 인터넷 응용, 분산정보시스템, 정보보안

최 흥 식(Heung Sik Choi) 정회원

1983년 2월 : 한양대학교 산업공학과 졸업
1985년 2월 : 한국과학기술원 경영과학과 석사
1991년 2월 : University of Rochester, 경영학 석사
1995년 2월:University of Rochester, Computers and Information Systems, 경영학박사
1985년 3월: 1988년 6월 : 데이콤정보통신연구소 연구원
1995년 3월~ 현재 : 국민대학교 비즈니스IT학부 교수
<주관심분야> 통신경영, 통신정책전략, 네트워크 설계