워게임 連動保安을 위한 政策基盤의 객체 保安화 방법과 管理시스템 제안

유창원*, 이희조**
*고려대학교 컴퓨터정보통신대학원 소프트웨어공학과
** 고려대학교 컴퓨터정보통신대학원
e-mail : hunter07@korea.ac.kr

A Proposal Object Security Method and Management System by Policy Based for Interconnect Security

Chang-Won Yu*, Heel-Jo Lee**
*Dept. of Software Engineering, Korea University
** Dept. of Computer Science and Engineering, Korea University

요 약

본 논문은 국방 네트워크 환경측면에서 실 전략정보에 대한 접근/활용 범위가 확대되고, 정보의 신뢰성/가용성에 대한 중요도가 강조되고 있는 워게임 연동객체의 보안화 방안에 대해 기술한다. 연동객체는 HLA/RTI에서 시뮬레이션을 위한 페더레이터로 정의된다. RTI는 페더레이터간 정보교환, 접속 사양에 정의된 다양한 서비스를 제공하는 미들웨어이다. 정책을 기반으로 네트워크상에서 자원들에 대한 관리와 접근, 사용을 위한 다양한 기능과 안전하고 편리한 보안기능들이 널리 활용되고 있다. 본 논문에서는 RTI Security 인터페이스와 정책을 기반으로 한 자원접근 방법을 사용해서 페더레이터의 취약한 정보보호 기능을 강화하였다. RTI의 페더레이트 실 정보에 다계층 보안 수준을 적용하고 보안등급별로 필터링하여 연동객체 스스로가 정보를 보호(Self-protection)할 수 있도록 하는 환경을 구성하고 관리할 수 있는 시스템을 제안한다.

1. 서론

최근 국방 분야의 전략시뮬레이션 모델이 거의 정점에 와있지만, 각 군 단위로만 활용하고 있으며 연합사나 합참 차원에서 워 게임을 전군 통합전장 전략 시뮬레이션으로 활성화하는데 있어 다음과 같은 이유로 상당히 미흡한 실정이다.

① 워게임 모델간 또는 타 체계 이 기종간의 연동이 급속히 확대되고 있는 반면에 연동객체가 비 암호화된 상태로 운용되고 있다.
② 정보등급별로 일관성 있는 보안정책 적용과 전반적인 보안관리 시스템이 취약한 상태여서 대규모 네트웍이나 분산시스템에 무방비로 노출되고 있다.
③ 기존 RTI 제품의 보안 기능은 미약하여 보안 영역에 따라 각각 다른 보안 정책을 내부적으로 정의하여 사용하였다. 따라서 각기 다른 보안 영역의 통신 상대와 통신하거나 다른 보안 영역을 거쳐 통신하는 경우에 보안 영역간의 정책 요구사항이 다르고, 양방향의 통신이 같은 경로에서 같은 정책을 사용하는지를 보장할 수 없었다.

여기에는 여러 가지 이유가 있겠지만, 특히 전략 시뮬레이션에 적용하는 논리적인 도메인들의 규모가 확대됨에 따라 객체들간 Security Association 설정이 복잡해지고, 다양한 특성을 갖는 도메인들의 구성요소와 환경 등의 요인 때문에 각 시스템에 대한 보안정책 설정 및 제어가 어려운 문제로 등장하고 있다.

이를 해결하기 위해서는 보안 정책에 따라 다르게 정의된 정책 정보들에 대한 중앙 집중적인 관리와 협상을 용이하게 하는 HLA/RTI 기반의 연동객체 보안 관리 모델이 정의되어야 하는데, 본 논문에서는 정책기반에 RTI를 이용한 객체 보안화 방법과 연동객체 보안관리 시스템의 프로토타입을 제안한다. [3][4].

연구의 구성은 다음과 같다. 2장에서는 정책기반 연동객체 보안관리 모델을 설계하기 위한 관련연구 자료로 연동 미들웨어 HLA/RTI와 정책정보모델 IETF에 대하여 기술하고, 3장에서는 정책기반의 연동객체 보안화 방법과 관리 시스템의 프로토타입을 제안하고, 4장에서는 프로토타입 평가 환경 및 결과를 기술하고, 마지막으로 결론과 향후 연구과제를 제시한다.

2. 관련연구

기존의 워게임 프레임워크에서는 모델간의 연동

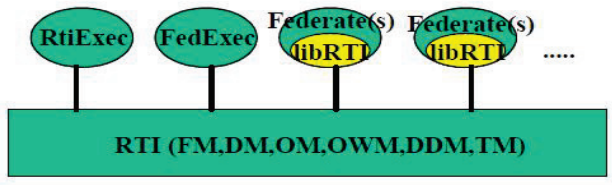
을 지원하기 위한 아키텍처로서 HLA 를 선정하였다. 모의 시뮬레이션 시스템의 재사용과 상호운용성을 보장하기 위해 하부구조로서 RTI를 채택하여 운용하고 2000년 이후 개발되는 모든 국방 분야 시뮬레이션을 RTI 기반에서 실행되도록 의무화하고 있다. 이에 따라 모의 시뮬레이션 상에서 연동되는 주요 정보들에 대한 보호방법을 강구하고 개발하는 것이 필요한 시점이다. 또한 기존의 단일모델의 보안담당자들은 확대되고 있는 연동환경에서 보안정책을 개발하고 적용하는 것에 익숙하지 않다. HLA 인터페이스 명세에 만족하는 보안정책 관리 시스템을 개발해야 하기 때문이다.

2.1 HLA/RTI(High Level Architecture/Run Time Infrastructure)

미국 국방성에서는 병렬/분산 시뮬레이션 개발의 효율 향상을 위한 공통 프레임워크로서 High-Level Architecture(HLA)[2,3]를 제안하였으며, 아래와 같은 세가지 구성요소로 이루어져 있다. : HLA 순응규칙(Compliance Rules); 객체 모델 템플리트(Object Model Template); HLA 하부 구조(Run-Time Infrastructure). HLA 순응규칙은 HLA 기반 시뮬레이션들이 지켜야 할 논리적 규범을 서술한 것이다.

HLA는 페더레이션 객체 모델(Federation Object Model : FOM)과 시뮬레이션 객체 모델(Simulation Object Model : SOM)의 이원화된 객체 모델을 사용하며, 객체 모델 템플리트는 FOM 및 SOM에 따라 정의된 객체들을 기술하는데 사용되는 객체 서술 도구이다.

마지막으로, HLA 하부구조(RTI)는 시뮬레이션 서비스들을 제공하는 네트워크 하부구조이며, RTI에서 제공될 서비스의 종류 및 기능은 HKA 접속 사양(Interface Specification)에 정의되어 있다. 그림 2 은 RTI의 구성 요소들을 나타낸다.



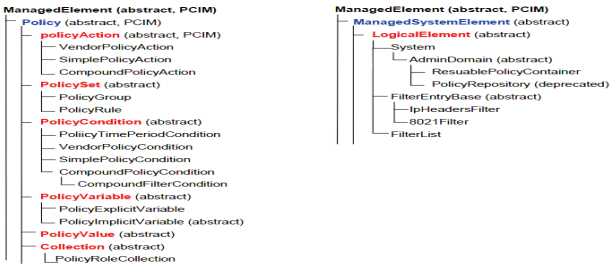
[그림 2.1]Components of RTI

RTIExec는 FedExec의 생성과 소멸을 담당한다. FedExec는 Federate들의 참가와 탈퇴를 담당한다. Fedetates은 libRTI를 통해서 RTI의 여섯 가지 서비스를 이용한다. 이들 서비스들은 Federation의 생성과 Federate의 참가, Class 선언과 객체 생성, Data Filtering, 시간 전진 등의 기능을 담당한다.

2.2 정책정보모델

정보모델은 DMTF(Desktop Management Task Force)의 CIM(Common Information Model)이 있으며, IETF(The Internet Engineering Task Force)의 정책 프레임워크(Policy Framework) 워킹 그룹에서는 정책에 대한 정보 모델인 PCIM(Policy Core Information Model)을 정의하여 RFC3060 으로 채택하였고, PCIM 을 확장한 PCIMe(Policy Core Information Model extensions)의 연구가 진행 중이다.

IETF 에서는 규칙기반 정책 표현을 선택하여 표준화를 진행하였다. 정책 정보를 표현하기 위한 방법으로는 IETF 와 DMTF(Desktop Management Task Force)에서 제시된 PCIM 을 사용한다. PCIM 은 정책 정보 모델을 표현하기 위한 객체 지향 정보 모델이다[7]. 정책 정보는 정책의 제어와 정책 정보를 표현하는 구조 클래스와 구조 클래스의 상호 연관성을 나타내는 연관 클래스를 사용하여 정의된다. 정책은 정책 규칙들의 집합을 사용하여 적용되고, 각 정책 규칙은 조건들의 집합과 반응들의 집합으로 구성된다. 여러 정책 규칙들은 정책 그룹들과 결합되고, 이러한 그룹들은 또 다른 그룹을 구성 할 수 있다. 그림 2.2 는 PCIMe (PCIM extensions)의 구조 클래스의 상속 계층을 나타낸다[8].



[그림 2.2] PCIMe의 구조 클래스 상속도

위에서 RTI에 대해서 간략히 소개하였는데, 기존의 RTI 제품은 보안을 지원하는 부분이 미약하여 네트워크상에서 시뮬레이션에 사용되는 실 데이터를 보호하는데 취약성을 드러냈다.

이로 인하여 연합훈련이나 전략 시뮬레이션 연동시 중요한 정보들이 외부로 해킹될 수도 있고, 또한 이기종간의 대규모 통신이 필요한 환경하에서 보안수준이 적용되지 못해 정보접근 권한이 낮은 사용자도 기밀정보들을 볼 수 있다는 심각한 문제점이 있었다.

따라서, 보안정책 모델을 통한 정보보호 기술은 절대적으로 필요하다. 이것을 해결하기 위해 본 논문에서는 실 데이터를 포함하고 있는 연동객체에 대한 정보를 보호하기 위해 새로운 객체보안화 방법과 관리시스템에 대한 프로토타입을 제안한다.

3. 정책기반의 연동객체 보안화 방법과 관리시스템 프로토타입 제안

시스템적인 네트웍 보안도 중요하지만, 연동되는 정보자체에 대한 보호는 더욱 중요하다. 보안 정책을 기반으로 RTI를 이용하여 연동객체인 Federate들 간의 정보 보호 수준을 강화하고 보안등급이 같은 객체만이 정보를 공유할 수 있도록 필터링을 적용하였다.또한, 연동 객체의 보호 수준과 효율적인 보안정책관리를 위하여 연동객체 관리시스템을 설계하였다.

3.1 연동객체 보안화 방법

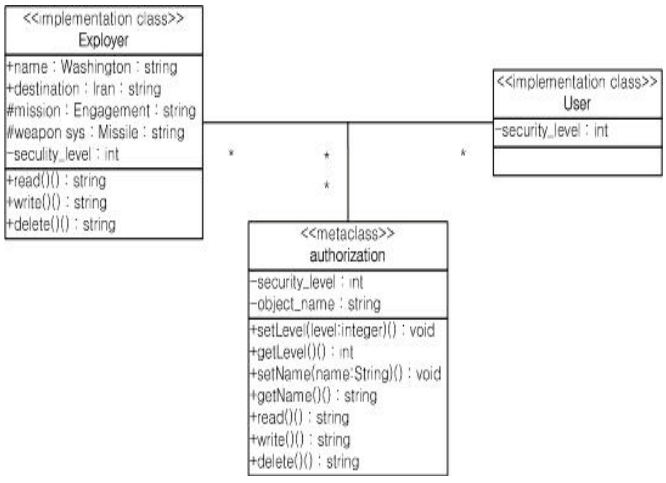
그림 3.1은 연동객체에 대한 객체보안화 방법을 표현하기 위하여 객체 지향 시스템 모델링의 표준화 기법인 UML의 클래스 다이어그램을 이용하여 보안객체를 표현하고 OMT 표기법을 이용하여 연동객체를 설계하였다.

Federate의 실 데이터를 보호하기 위해 다계층 보안 가드를 사용하였고 보안객체를 효과적으로 제어하기 위해 채널을 3개로 나누었다. [3]

1)RTIA와 RTIG 사이, Federate와 Ambassador 사이에 상호작용을 담당하고 다른 Federate 또는 RTIA[5]와는 분리하였다.

2)전송할 때 권한부여 또는 제약조건에 대한 RTI 정보를 공유하기 위해 신뢰할 수 있는 정책기반에 보안수준을 정의하기 쉽도록 하였다. 하지만, 일반 조직에서는 자신들의 정보에 보안수준을 적용하지 않고 있다. 이것은 신뢰도를 고려하지 않은 비공식적인 정책을 가지고 있기 때문이다. 그래서 본 논문에서는 어떤 조직이나 Federate에서 조직의 정보를 보호할 수 있게 RTI 서비스에서 따로 분리시켰다.

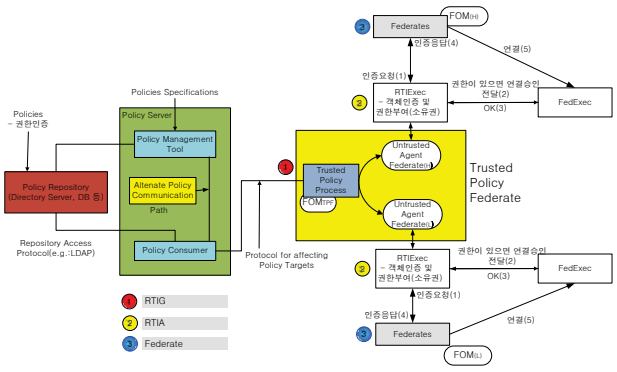
3)객체간에 연관성 있는 정보들을 신뢰하기 위해 RTI에서 Federates이 다른 Federates의 속성에 대한 지식을 획득할 수 있도록 했는데, 이것은 Federate내에 Metaclass의 속성으로 표현할 수 있다. 여기에 보안 레벨을 나타내는 Seculity_level과 이름을 나타내는 Name 이라는 속성을 가지고 속성값을 획득하고 설정하는 메소드를 오퍼레이션 형태로 제공하므로서 가능하다. 이때 어떤 Federate 정보는 반드시 다른 조직이나 다른 컴포넌트로부터 분리되어 있어야 한다.



[그림 3.1] 연동객체 보안화 방법

3.2 연동객체 보안관리시스템 프로토타입

RTI를 이용한 연동객체 보안관리 시스템의 프레임워크는 IETF의 정책 프레임워크를 참조하였으며 그 구성요소는 객체를 관리하는 객체 관리 도구(Object Management Tool)와 객체보안 정책을 저장하는 정책 저장소(Policy Repository)[6], 정책을 결정하는 서버 (PDS : Policy Decision Server), 정책을 적용하는 페더레이션 (PEF : Policy Enforcement Federation)으로 이루어져 있다.



[그림 3.2] 연동객체 보안관리시스템 프로토타입

보안관리시템 프로토타입에서는 다양한 객체간의 연관성 관계와 시스템 객체의 내부 상태 및 객체간의 연관성을 객체의 애트리뷰트와 객체간의 오프레이션 호출관계를 손쉽게 변경할 수 있도록 하였으며, 보안정책을 자체적으로 분석하고 필터링을 통해 보안정책간의 상호작용을 검증하는 방법을 적용하였다.

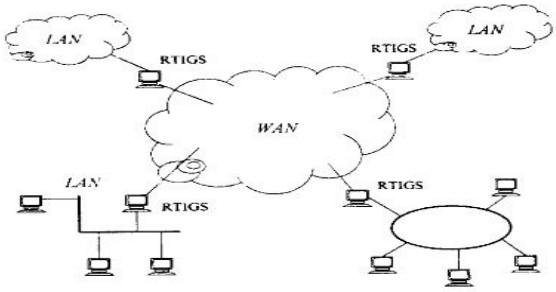
그림 3.2는 RTI의 연동 인터페이스에 보안정책 서비스를 적용하여 구조화 한 것으로 Federate가 네트워크상에서 동일한 수준의 보안정책이 적용된 Federate 하고만 정보를 공유할 수 있도록 프로토타입을 설계하였다. 이러한 구조에서는 보안정책을 적용하는 관리시스템과 적용시스템이 분리되므로 보안정책을 쉽게 변경 할 수 있어 관리가 간단하며 유사한 시스템에 동일한 정책을 재사용할 수 있다는 장점을 제공한다.

4. 프로토타입 환경 및 평가

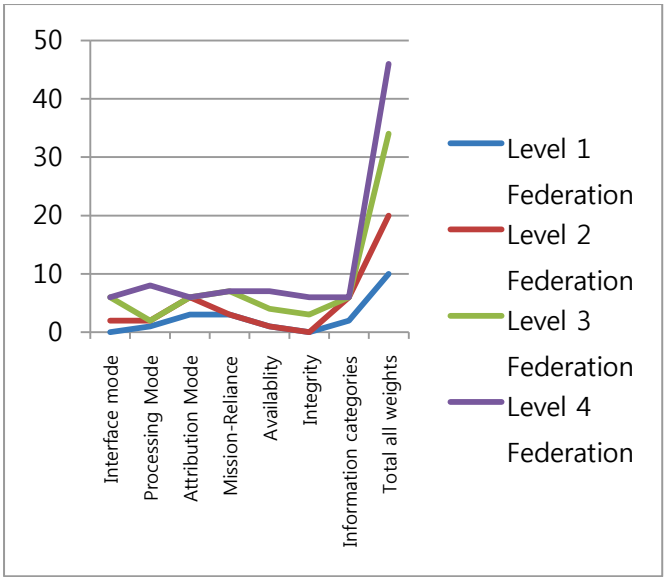
본 시스템은 국방 망으로 연결된 서로 다른 네트워크상의 컴퓨터들을 단위 노드로 갖는 시뮬레이션 시스템 구축이 가능하도록 하기 위하여 네트워크 환경을 WAN 과 LAN 으로 구분하여 이중적으로 관리[4]하며, LAN 에서는 UDP 브로드캐스트를 기본 통신으로 하고 WAN 은 UDP 유니캐스트를 기본 통신 방식으로 사용한다.

또한, WAN 과 LAN 사이를 오가는 메시지들에 대한 프로토콜 변환 및 메시지 필터링을 위하여 RTIGS(RTI Gateway Server)을 둔다. RTIGS 는 이외에도 메시지 전송 순서를 보장해주고, 메시지 흐름 제어 및 네트워크 오류 검출 등의 기능을 담당한다.

그림 4 은 워게임 시스템의 네트워크 환경을 잘 예시하고 있으며, 동일한 환경을 조성하여 프로토타입을 통해 연동객체를 식별하고 정보보호 수준을 필터링하는 보안클래스와 매핑하여 실 정보를 가지고 있는 연동객체 Federate 에 대한 보안인증수준을 평가하였다.



[그림 4] 워게임 시스템의 네트워크 환경



[그림 5] 연동객체의 자체보안화 능력평가

그림 5에서 보는 바와 같이 Federation의 모든 특성별로 가중치를 적용하여 연동객체에 대한 보안 인증 수준을 측정해본 결과 가중치 값들이 상당한 차이가 있음을 알 수 있다. 결과적으로 본 연구를 통해 연동객체가 보유 하고 있는 정보의 중요도에 따라 보호 수준을 높이면 해당 정보들에 대한 신뢰성, 가용성, 무결성이 높아져 네트워크상에서 객체 자체적으로 정보를 보호하는 능력이 커진다는 것을 입증 하였다.

5. 결론 및 향후 과제

본 논문에서는 정책기반에 RTI를 이용하여 연동객체 보안화 방법에 대한 구조와 속성 및 상호 작용에 대해 서술하고, 이를 보다 효율적으로 관리하기 위해 RTI의 프레임워크에 기존의 보안레벨들을 세분화하여, 세분화된 영역을 조직단위로 한 다중레벨 보안화 방법을 제시하였다.

그리고 정보의 중요도에 따라 보안수준을 차별화 할 수 있도록 보안 가드를 모든 Federate에 적용할 수 있는 일관성을 제공하기 위해 정책기반에 연동객체 보안관리 시스템에 대한 프로토타입을 설계하였고, 또한, 페더레이트간에 정보의 전송과 신뢰할 수 있는 정보 수준을 제공하기 위하여 보안계층별로 정보를 교환해주는 정책 페더레이트를 배치함으로써 자원의 낭비와 일관적인 정책을 적용하는데 소요되는 오버헤드를 감소시키는 유연성을 제공했으며, 보안수준에 따라 정보 전달 레벨을 원천적으로 달리 적용하므로서 연동객체가 네트워크상의 위해 요소로부터 자체적인 방어(Self Protecting) 기능을 갖도록 하였다.

결론적으로 이 방식을 적용한 연동객체는 국방체계들 중에서 가용성, 신뢰성, 무결성 및 기밀성이 반드시 요구되는 워게임체계(Wargame System)의 합동훈련 시 발생하는 군사기밀이나 시뮬레이션 자료들의 실제 값 들이 그대로 노출되고 있는 취약점을 보완할 수 있으며, 폐쇄적인 국방망에서 물리적인 보안조치만 가지고 외부의 해킹과 자료의 변조 등에 대응하기 어렵기 때문에 객체들 각각이 모두 보안 체계를 갖추고 있는 환경을 조성할 수 있다. 따라서, 워게임을 통한 실질적인 훈련 시 보안을 요하는 데이터를 효과적으로 보호 할 수 있고, 일관된 보안정책 적용 및 통제 효과를 기대할 수 있다.

하지만, 이 모델을 현실화하기 위해서는 연동 객체 보안관리 시스템이 수행하는 기능에 대한 세부적인 구현과 객체를 보안화하는데 있어서 필요한 계층별 제어 필드들에 대한 추가적인 연구가 요구된다. 더 나아가 정책 협상에 따른 연동 메커니즘 설계와 보안 관련기술 구현도 필요하다. 따라서, 향후에는 DRM 관련기술인 컨텐츠 식별자 DOI(Digital Object Identifier), 연동에 필요한 데이터를 기록하는 인덱스(INDECS), 불법복제와 변조방지를 위한 워터마킹 기술 등을 응용하여 향후에는 국방 연동분야의 객체들에 대해 적용해볼 계획이다.

6. 참고문헌

[1] J. Filsinger, Jarrellann, HLA Secure Combined Architecture, December 1996 (Available online:www.dmso.mil/)
[2] DMSO, “High Level Architecture Federation Security Process”Version 1.2, February 16, 2001
[3] Defense Information System Agency (DISA), Message Guard Assessment, Technical Memorandum, DoD Multilevel Security Program, June 1994.
[4] Fiorino, T et al, Lessons Learned During the Life Cycle of an MLS Guard Deployed at Multiple Sites, Eleventh Annual Computer Security Applications Conference, IEEE, December 1995, New Orleans.
[5] HLA Management Object Model, Version 0.2, 17 October 1996 (Available online:www.dmso.mil/)
[6] Wang ChangKun, "Policy-based Network Management", Communication Technology Proceeding, 2000.
[7] Department of Defense, “High Level Architecture Interface Specification, Version 1.3 Draft 7”, January 1998
[8] B. Moore, et al., “Policy Core Information Model-Version 1 Specification,” IETF RFC 3060, 2000.
[9] B. Moore, et al., “Policy Core Information Model (PCIM) Extensions,” IETF RFC 3460, 2003.