협력시스템에서의 보안 프레임워크 설계

정연일[0] 이승룡
경희대학교 전자계산공학과
{zhung, sylee}@khu.ac.kr

Design of A Security Framework for Collaborative System

Yonil Zhung[0] Sungyoung Lee
Dept. of Computer Engineering, KyungHee University

요 약

협력 시스템은 분산 시스템 환경에서 호스트들이 네트워크를 통하여 상호 연결되어 있으며 다양한 사용자가 여러 자원들 공동으로 활용한다. 협력 시스템 발전 및 정보 보안의 중요성에 대한 인식 증가로 인하여, 개방형 분산 협력 시스템 환경에서도 정보 통신 시스템의 자원을 보호하기 위한 여러 가지의 보안 서비스에 대한 연구가 진행되고 있다. 하지만 기존의 일반적인 보안 서비스로는 협력 시스템에 특징과 구조에 맞는 서비스를 제공하기 어려운 점이 있다. 본 논문에서는 저자가 개발한 산업 디자인 협력 시스템에서의 보안 프레임워크를 제안한다. 제안된 프레임워크는 인증, 암호화 정책, 접근제어, 보안 정보 관리의 네 가지로 구분하며 각각의 서비스가 상호 보완적으로 구성되어 있다. 또한, 특정 협력 시스템에 맞도록 구성되었지만 다른 협력 시스템에도 응용할 수 있도록 표준화를 따랐으며, 사용자의 요구에 따라 다른 비밀성과 무결성을 지원하기 위한 QoP(Quality of Protection) 서비스도 고려하여 설계하였다. 제안된 보안 프레임워크는 접근제어 요소를 협력 시스템의 구성에 맞도록 재구성하여 기존 정책의 단점인 복합적인 상황에서 확실한 보안을 할 수 있었으며 접근 정의에 따라 다른 알고리즘을 사용함으로 보안 프레임워크가 포함된 후에도 빠른 협력 작업이 가능했다. 또한 디자인 협력 시스템의 동시성 제어 정책을 기반으로 접근 제어 정책을 결정하였기 때문에 시스템 성능에 향상을 가지고 왔다.

1. 서 론

정보 보안의 중요성은 정보 통신 기술의 발달로 인하여 정보 시스템 사용이 증가되며, 인터넷 등 개방형 정보 통신망과의 상호 접속으로 인한 정보의 유출, 파괴, 위·변조, 바이러스 유포 등 각종 해킹 및 컴퓨터 범죄가 증가하고 있는 현재에 특히 강조가 되고 있다[1]. 협력 시스템은 컴퓨터와 통신망을 이용하여 사람과 사람 사이의 공동 작업을 지원하는 시스템이다. 협력 시스템은 분산 시스템 환경에서 호스트들이 네트워크를 통하여 상호 연결되어 있으며 다양한 사용자가 자원을 공동으로 활용한다. 따라서 개방형 분산 협력 시스템 환경에서 정보 통신 시스템의 자원을 보호하기 위하여 여러 가지의 보안 서비스를 제공해야 한다. 그러나, 기존의 보안 서비스와는 달리 협력 시스템의 특징과 구조에 맞는 보안 서비스가 필요하다. 본 논문에서는 저자가 개발한 산업 디자인 협력 시스템을[2] 모델로 하여 협력 시스템에 필요한 보안 프레임워크에 대하여 논한다. 본 논문은 다음과 같이 구성되어 있다. 2장에서는 기존의 분산 환경에서의 보안 기술, 3장에서는 산업 디자인 협력 시스템 및 보안 프레임워크에 대하여 설명하고, 4장에서는 결론 및 향후 전망에 대하여 설명한다.

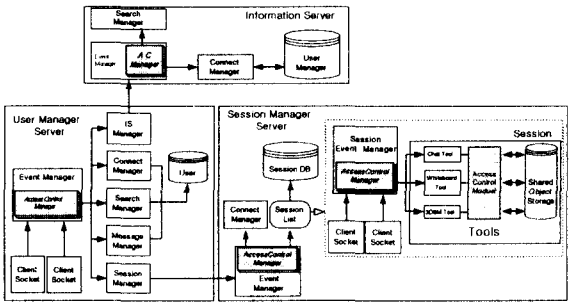
2. 관련 연구

현재, 협력 작업 환경을 지원하는 시스템은 많이 개발되었으며 또한, 개발 중에 있다. TeamWave Ltd.의 TeamWave는 Tcl/Tk로 사용자들간의 협력 작업 지원을 목표로 설계되었으며 클라이언트/서버 환경을 기반으로 한다. TeamWave의 경우 방화벽을 통한 보안 정책만을 채택하고 있다. 그리고, 런던 대학의 Mushroom는 자바 기반 프레임워크로서 분산 협력 작업, 그룹 형성과 자원 공유 등을 제공한다. Mushroom 또한, 접근제어 리스트를 이용한 보안만을 채택하고 있다. 그리고, North Carolina 대학의 Suite는 사용자 규칙, 협력 권한, 접근 제어 등에 대한 정의를 미리 정의해 두고 이를 이용하는 접근제어 정책만을 제공하고 있다. 하지만, 대부분의 협력 시스템들은 보안의 중요성을 인식하면서 협력 작업에 더 중점을 두고 개발 중에 있으며, 협력 시스템에서의 보안 정책은 기존 보안 정책의 일부분만을 채택하고 있을 뿐 전체적인 보안프레임을 구성하는 경우는 드물다.

3. 산업 디자인 협력 시스템에서의 보안 프레임워크

3.1 산업 디자인 협력 시스템 구조

본 논문에서 다루는 협력 시스템은 분산 객체 공유 모델을 바탕으로 클라이언트/서버 모델을 이며, 분산 객체는 이벤트에 의해 조작된다. 협력 시스템 서버 구조는 [그림 1]과 같다.



[그림 1] 산업 디자인 협력 시스템 서버 구조

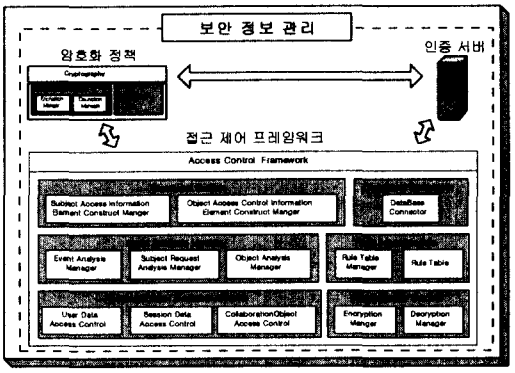
분산 객체 공유 모델을 바탕의 산업 디자인 협력 시스템은 사용자 접속 및 인증, 올바르지 않은 사용자의 접근 시도를 감시,

차별적인 사용자 정책에 따라 접근 제안, 사용자의 요구에 따라 세션을 관리한다.

협력 시스템 클라이언트는 분산 공유 객체를 공유하고 개발한 산업 디자인 프로세서를 지원하기 위한 환경을 제공하기 위하여 3D Studio Max, 원격회의 시스템, 화이트 보드 시스템, 의사 결정지원 시스템, 그리고 각 부서마다 협력 작업 일정 및 공지 사항을 제공하기 위한 게시판 및 작업 파일의 공유를 위한 자료실을 개발하였다.

3.2 협력 시스템의 보안 프레임워크 구조

산업 디자인 협력 시스템의 보안 프레임워크는 인증, 암호화 정책, 접근제어 프레임워크, 보안 정보 관리 서비스의 4가지로 구성이 된다[그림 2].



[그림 2] 보안 프레임워크 전체 구조

각각의 정책들은 독립적으로 구분이 가능하지만 어느 하나만으로 협력 시스템의 보안을 만족시킬 수 없으며 네 가지 정책이 서로 상호 보완적으로 협력 시스템의 보안 정책을 구성하고있다. 협력 시스템의 특징상 안정적인 시스템 운영과 원활한 협력 작업을 위해서는 협력 시스템의 접근 제어 정책이 가장 중요한 정책이다.

3.3 인증 정책

인터넷과 같은 개방형 분산 시스템 환경에서는 호스트들이 네트워크를 통하여 상호 연결되어 있으며 다양한 사용자가 자원을 공동으로 활용한다. 개방형 협력 시스템에서도 호스트들 사이에 분산된 여러 가지 자원들은 서버에 의하여 제공되는 네트워크 서비스 형태로 공유된다. 협력 시스템 환경에서 사용자는 원하는 자원에 접근하기 위하여 서버에게 서비스를 요청할 수 있다. 이렇게 사용자가 네트워크를 통하여 시스템에 접근할 때, 정보통신시스템 자원을 보호하기 위하여 정당한 사용자인지, 허용된 시스템에서 접근 요청을 하는지, 통신 대상이 되는 목적지 시스템에 대한 접근권한이 있는지를 검사하여 허용여부를 확인하는 절차가 필요하다. 본 시스템에서는 X.509를 이용하여 인증 서버를 구축하여 사용자가 인증서를 이용하여 협력 시스템을 사용할 수 있도록 하였다. 본 시스템에서 인증 서버의 특징은, 기존의 인증 서버의 경우 인증서 발급 및 관리만 가능하지만, 협력 시스템에서 사용할 인증 서버의 경우 인증서 관리뿐만 아니라 암호화 정책에서의 QoP를 지원하기 위한 작업 및 각종 암호화 알고리즘에서 사용하는 키 관리도 가능하도록 해야하기 때문에 QoP 지원 및 키 관리 기능까지 인증 서버에서 담당하도록 하였다.

3.4 암호화 정책

협력 시스템은 안전한 보안 정책과 빠른 협력 작업 사이에는 tradeoff가 존재한다. 한가지 암호화 정책을 가질 경우 이 두 가지를 만족시키는 것은 불가능하다. 따라서 협력 시스템의 경우 여러 가지의 암호화 정책을 갖는 것이 바람직하다. 본 시스템에서는 관용 암호방식과 공개키 암호 방식을 모두 사용한다. 초기 로그온 및 협력 작업 시, 협력 작업에는 관용 암호방식을 사용하며, 그 밖의 작업에서는 공개키 암호 방식을 이용한다. 협력 작업 시 사용하는 관용 암호 방식에 사용되는 키 관리를 해줘야 하는 작업이 필요하다. 이 작업은 인증서를 이용한 인증서버에서 같이 할 수 있도록 설계하였다.

본 시스템에서는 또한, 한가지 관용 암호 알고리즘을 사용하는 것이 아니라 여러 알고리즘을 사용하는데 이것은 보안 레벨이 낮고, 높은 협력 작업에 따라 각기 다른 암호 알고리즘을 사용하기 위해서이다. 이것은 원활한 협력작업을 위한 것으로 클라이언트간에 비밀성과 무결성을 보장하기 위한 QoP 서비스를 필요로 하고 있다. QoP란 보안 기능들의 집합이며 인증, 비밀성, 무결성, 부인거부등의 조합들로 구성되어 있다[4]. 기존 QoP의 경우는 통신 초기 설정, 실행, 완료, 암호 알고리즘 사용 정도의 서비스만을 제공하게 된다. 본 논문의 협력 시스템에서 클라이언트간의 QoP서비스는 응용레벨에서 요구하는 암호화 알고리즘 호환이 가능하도록 QoP 정보를 보안 문맥 객체에 추가하고, 추가된 정보를 관리하고 제어 할 수 있도록 하며, 클라이언트간의 공통 QoP 정보를 생성하여 동일한 QoP 정보를 갖도록 하였다.

3.5 접근제어 프레임워크

일반적으로 접근 제어라면 사용자, 프로그램, 시스템 등의 인가된 주체만이 정보시스템의 자원에 접근할 수 있도록 제한하는 것을 의미한다. 모델이 된 산업 디자인 협력 시스템에서 외부 접근제어는 주로 인증과 암호화 정책과 관련이 있으며, 내부 접근제어는 인가된 사용자에 한하여 정보의 중요도에 따라 접근을 제어하며 원활한 공동작업을 위해 신분이나 직무에 따른 제어를 할 목적으로 구성되어 있다.

접근제어의 각 모듈은 주체 및 객체의 접근 요소를 생성하는 모듈(Construct Module)과 주체 및 객체의 정보를 가져오기 위해 데이터베이스와 연결하는 모듈(DataBase Connector), 이벤트 요구 발생 처리, 주체의 요구 분석, 객체의 분석을 담당하는 모듈(Event Analysis Module), 규칙 테이블을 관리하는 모듈(Rule Table Module), 접근 제어 결정 모듈(Access Control Decision Module), 그리고 암호화와 복호화를 담당하는 모듈(Cryptograhpy Module)로 이루어져 있다. 제한된 접근 제어 정책에서 가장 중요한 부분은 접근 제어 결정 모듈이며 이 부분의 구조에 따라서 전체적인 성능에 대한 전혀 다른 결과를 가져올 수 있다. 객체 및 주체의 접근 제어 정보와 접근 정보는 다른 협력 시스템에서 구조와 특징에 맞게 변경 가능하면 이용 가능하게 확장성을 고려하였고, 정의 해둔 규칙 테이블의 경우 시스템을 사용하려는 사용자의 요구에 따라 구성하여 맞는 보안 정책을 펼칠 수 있도록 하였다. 접근 제어 결정 모듈의 각 접근 제어 정책은 다음과 같다.

3.5.1 사용자 정보 접근 제어

클라이언트의 사용자 정보에 대한 이벤트 요구가 들어왔을 때 이벤트 처리기내의 접근제어 모듈에서 사용자에 대해 접근 제어를 해주게 된다. [그림 3]에는 사용자에 관한 정보 데이터 접근 제어를 나타낸다. 일반적인 데이터의 경우 접근자의 신분, 직무, 소속 그룹과 규칙 테이블에 정의된 규칙과 비교를 하여 규칙에 따른 데이터에 접근 가능하게 하거나 보안을 많이 요구하는 데이터와 데이터를 변경하고자 할 시 접근자의 보안등급, 무결성 등급과 규칙테이블에 정의되어 있는 규칙과 비교하여

맞는 데이터까지 접근 및 변경을 가능하게 한다.

(M = 접근자, RT=규칙테이블, I=신분, R=직무, G=그룹,
S=보안 등급, IW=무결성 등급, O=소유권, P=허가권)

```
Permit_GeneralData_Access =
      TRUE :  if (M(I) >= RT(I))
                Access_Rule_All_data
                return
              if (M(R) = RT(R) and M(G) = RT(G))
                Access_RGRule_All_data
                return
              if (M(R) = RT(R))
                Access_RRule_data
                return
              if (M(G) = RT(G))
                Access_GRule_data
                return
      FALSE : otherwise
Permit_SecretData_Access =
      TRUE :  if (M(S) >= RT(S))
                find (M(S) = RT(S))
                  Access_Rule_data
      FALSE : otherwise
Permet_ModifyData_Access =
      TRUE :  if (M(IW) >= RT(IW))
                find (M(IW) = RT(IW))
                  Access_Rule_data
      FALSE : otherwise
```

[그림 3] 사용자 데이터 접근 제어 알고리즘

3.5.2 세션 객체 접근 제어

협력 작업에는 세션의 생성 및 관리는 중요한 부분이다. 불법적인 사용자에 의해 세션이 생성되고 관리되거나, 허가되지 않은 사용자에게 정당하게 생성된 세션이 파괴되거나 불법적인 사용에게 세션이 노출된다면 심각한 피해를 입을 수 있다. [그림 4]에는 세션의 생성과 참여, 관찰 그리고 업데이트를 하기 위해 접근자의 접근 정보와 규칙 테이블 안의 규칙 정보를 비교하여 정해진 규칙에 맞는 행동만을 하도록 한다.

```
Permit_SessionCreate_Access =
      TRUE :  if (M(I) >= RT(I)  or M(S) >= RT(S))
                Access_Create_Session
      FALSE : otherwise
Permit_SessionJoin_Access =
      TRUE :  if (M(R) = RT(R))
                Access_Join_Rule_Session
              if (M(G) = RT(G))
                Access_Join_Rule_Session
      FALSE : otherwise
Permit_SessionObserve_Access =
      TRUE :  if (M(S) >= RT(S))
                Access_Oberce_Session
      FALSE : otherwise
Permit_SessionUpdate_Access =
      TRUE :  if (M(IW) >= RT(IW)  or M(O) = RT(O))
                Access_Update_Rule_Session
              if (M(R) = RT(R)  or M(G) = RT(G))
                Access_Update_Rule_Session
      FALSE : otherwise
```

[그림 4] 세션 객체 접근 제어 알고리즘

3.5.3 공유 객체 접근 제어

사용자가 공유 객체를 많이 사용하는 협력 시스템의 경우 접근 제어 서비스 모듈은 보안 측면뿐 아니라 협력 작업에서도 필요한 부분이다. [그림 5]에서는 공유 객체를 다루는 부분에서 데이터의 생성 및 업데이트, 실행에 관해서 접근자의 소유권, 무결성 등급 등을 규칙 테이블의 정의된 규칙과 비교하여 행동을 제어하게 된다.

위에서 설명한 세 가지의 접근 제어에서 접근자는 신분, 직무, 보안등급 등의 기록이 있는 접근정보(Access Information)를 소유하고 있으며 접근하려는 정보에는 객체의 종류, 생성자, 보안 등급, 보안레이블, 소유권 등의 정보가 객체 생성 시 자동으로 접근 제어 정보(Access Control Information)에 포함되도록 하며, 미리 정의 해둔 규칙테이블에 의해 정의된 규칙에 맞는 접근의 여부와 접근 범위들을 허용하도록 하였다.

```
Permit_CreateData_Access =
      TRUE :  if (M(P) = RT(P))
                Access_Create_Data
      FALSE : otherwise
Permit_UpdateDate_Access =
      TRUE :  if (M(O) = RT(O)  and M(IW) >= RT(IW))
                Access_Update_Rule_Data
      FALSE : otherwise
Permit_ExcuteDate_Access =
      TRUE :  if (M(O) = RT(O)  and M(S) >= RT(S) or M(I) >=
RT(I))
                Access_Excute_Rule_Data
      FALSE : otherwise
```

[그림 5] 공유 데이터 접근 제어 알고리즘

3.6 보안 정보 관리 서비스

보안 정보 관리 서비스는 암호 알고리즘의 교체 및 접근 제어 테이블 수정 등 보안과 관련된 정보를 관리하는 서비스로 보안 정보 데이터베이스를 관리하는 보안 데이터베이스 관리자(Security Database Manager)이라는 관리자를 두어 보안 정보를 변경하거나 추가할 수 있도록 한다. 기존 시스템의 변화와 보안 정책의 변경 및 보안과 관련된 문제를 관리 할 수 있도록 서비스를 한다. 또한, 보안 사항을 모니터링 하여 상황을 알려주고 외부로부터의 침입과 보안에 위반되는 사항에 대해서도 내용을 저장하고 통보하는 역할까지 담당하도록 하였다.

4. 결론

최근 개방형 정보 통신망을 이용하는 협력 시스템에서의 작업이 급격히 증가하면서 보호해야 할 정보의 대상과 가치도 증가하였다. 그리고 이에 대한 적절한 대응도 필수적으로 되었다. 본 논문에서는 협력 시스템에 개입된 주체들 사이의 가장 심각한 위협요소인 불법적인 위·변조, 도청, 신분위장 및 재전송 등으로부터 시스템의 안정성을 확보하기 위하여 개발중인 협력 시스템에 맞는 보안 프레임워크에 대하여 논하였다. 보안 서비스는 인증 프레임워크, 암호화 서비스, 접근 제어 프레임워크, 보안 정보 관리 서비스의 네 가지 부분으로 나누어서 설계하였다. 또한 데이터 전송시 사용자의 요구에 따라 다른 비밀성과 무결성 지원하기 위한 QoP(Quality of Protection) 서비스를 포함하였으며, 다른 협력시스템에서 사용할 수 있도록 표준화 작업을 하였다. 제한된 보안 프레임워크는 여러 보안 요소를 정의하여 복합적인 상황에서 확실한 보안을 하였으며 상황에 따른 알고리즘과 보안 요소를 사용함으로 보안이 포함한 협력 작업에 빠른 속도 향상을 가져왔다. 또한 디자인 협력 시스템의 동시성 제어 정책을 기반으로 접근 제어 정책을 결정하였기 때문에 시스템 성능에 향상을 가지고 왔다.

향후 연구과제로는 모든 정보 보호 서비스를 고려하기 위한 보안 플랫폼 및 각 객체의 컴포넌트화에 관한 연구가 진행되어야 할 것이다.

5. 참고 문헌

[1] 기술본부기술응용팀, 개방형 통신망 환경에서의 인증 및 접근 통제 기술, 한국정보보호센터, pp 1, 1998.4

[2] 양진모, 이승룡, 확장성을 지원하는 산업디자인 협력 시스템 개발, '99 한국 정보처리학회 추계 학술발표 논문집, 1999년 10월, pp 223-228.

[3] CORBA Security Service Specification, page 2-1~2-168 , 2000.5

[4] J. Linn, Generic Security Application Program Interface (GSS-API), RFC-1508, 1993.9

[5] Vijay Varadharajan, Chris Crall, Issues in the Design of Secure Authorization Service for Distributed Applications, Proceedings of the Globecom '98 Volume 2, 874-879, 1998.11