협력 시스템에서의 접근 제어 프레임워크 설계

정연일[U] 이승룡
경 희 대 학 교 전 자 계 산 공 학 과
{zhung, sylee}@oslab.kyunghee.ac.kr

The Design of Access Control Framework f or Collaborative System

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

요 약

협력 시스템은 컴퓨터의 성능 향상과 네트워크 기술의 발전으로 인하여 분산 환경에서 다수의 사람들이 프로젝트나 어떤 작업을 동시에 수행이 가능하도록 하는 기술이다. 분산 환경과 개방형 정보 통신망을 이용하는 협력 시스템은 정보의 신뢰성이 보장되고 안전한 서비스를 제공해야 한다. 또한, 협력 시스템은 공유 객체 기술을 기반으로 함에 따라 공유 객체에 대한 보안 기술의 개발은 절대적으로 필요하다. 특히, 협력 시스템의 보안은 기존의 보안 정책을 그대로 적용하기보다는 각각의 협력 시스템의 특성에 맞게 새롭게 구성되어져야 한다. 본 논문은 실시간 산업 디자인 협력 시스템에서의 보안 프레임워크 중 접근 제어 프레임워크 부분에 대하여 논하고자 한다. 접근 제어는 사용자 정보, 세션 정보, 공유 객체 정보에 대한 접근 제어로 구성되며 사용자 정보 접근제어와 세션의 접근제어는 접근자의 접근 정보에 의해 정의된 규칙에 따른 정보에 접근을 제어하며 공유 객체 접근 제어는 공동 작업을 원활히 하기 위해 주체와 객체사이의 정보를 이용하여 제어하는 특징이 있다.

1. 서론

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[2]. 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 현재 진행중인 협력 시스템을 모델로 하여 협력 시스템에 필요한 보안 정책들 중 접근 제어 프레임워크에 대하여 논한다. 본 논문은 다음과 같이 구성되어 있다. 2장에서는 기존 접근제어 기술과 관련된 내용, 3장에서는 현재 모델로 택한 협력 시스템에 대한 설명, 4장에서는 접근 제어 프레임워크에 대하여 설명하고, 5장에서는 결론 및 향후 전망에 대하여 설명한다.

2. 관련 연구

접근 통제(Access Control)는 사용자가 네트워크를 통하여 시스템에 접근할 때, 허용된 시스템에서 접근 요청을 하는지, 통신 대상이 되는 목적지 시스템에 대한 접근 권한이 있는지를 검사하여 허용 여부를 결정한다. 따라서 네트워크의 특정자원에 대해서 접근권한이 있는지를 검사한 후 접근 여부를 결정하므로 불법 침입자에 의한 불법적인 자원 접근 및 파괴를 방지 할 수 있다. [3][4][5]. OSI(Open Systems Interconnect) 보안 구조에서의 접근 제어 정책은 다음과 같다. 신분 기반 정책은 주체나 그들이 속해있는 그룹들의 신분에 근거하여 객체에 대한 접근을 제한할 뿐 접근되는 객체 정보의 중요성에는 아무런 지식을 가지고 있지 않고 있다. 규칙 기반 정책은 주체와 객체들간의 관계를 정의하고, 정보의 흐름이 일어났을 때 정보가 소유한 제한 규칙을 상속하며, 각 주체와 객체에 대해서 규칙 기반 정책이 일정하다. 직무 기반 정책은 신분 기반 정책과 규칙 기반 정책의 특성을 모두 가진 상업용 환경에 적합한 정책으로 개별적 신분이 아닌 자신의 직무에 따라 접근 할 수 있는 정보가 결정되고, 사용할 수 있는 정보의 한계가 정해진다[6].

3. Collaborative System

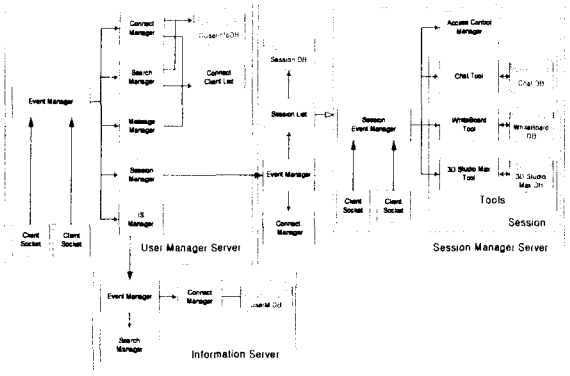
3.1 협력 시스템 구조

분산 객체 공유 모델의 설계는 전체 협력 시스템의 프레

임워크를 결정짓는 중요한 요소로 작용한다. 협력 시스템은 분산 객체 공유 모델을 바탕으로 협력 시스템 클라이언트/서버 모델을 제안한다. 분산 객체는 이벤트에 의해 조작된다. 클라이언트/서버 환경은 모든 이벤트들이 서버에 집중되어 분산 객체의 관리가 용이하다[2].

3.2 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[그림 1].



[그림 1] 산업 디자인 협력 시스템 서버 구조

3.3 협력 시스템 클라이언트 구조

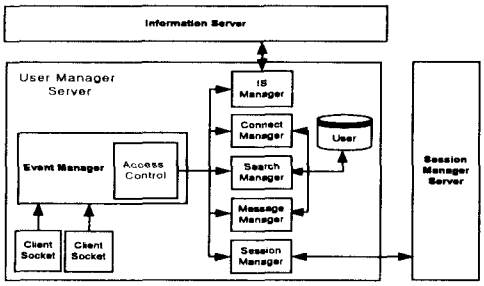
클라이언트는 분산 공유 객체를 공유하고 개발한 산업 디자인 프로세서를 지원하기 위한 환경을 제공하여야 한다. 이를 지원하기 위하여 3D Studio Max, 원격회의 시스템, 화이트 보드 시스템, 의사 결정지원 시스템, 그리고 각 부서마다 협력 작업 일정 및 공지 사항을 제공하기 위한 게시판 및 작업 파일의 공유를 위한 자료실을 개발하였다.

4. 접근 제어 프레임워크

본 논문에서 모델로 삼은 협력 시스템의 보안 프레임워크는 크게 인증, 암호화, 접근제어, 그리고 보안정보의 관리 등으로 나눌 수 있는데 어느 한가지만으로 보안 프레임워크를 구성할 수는 없으며 네 가지 정책이 서로 상호 보완적으로 구성되도록 하였다. 일반적으로 접근 제어라면 사용자, 프로그램, 시스템 등의 인가된 주체만이 정보시스템의 자원에 접근할 수 있도록 제한하는 것을 의미한다. 모델이 된 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. 본 논문에서는 접근제어는 시스템 내부에서의 접근 제어만을 논하고자 한다.

4.1 사용자 정보 접근 제어

[그림 2]에서처럼 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.



[그림 2] 사용자 정보 접근 제어

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.

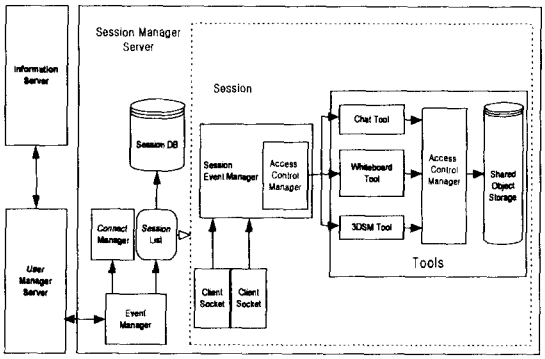
(M = 접근자, RT=규칙테이블, I=신분, R=직무, G=그룹, S=보안 등급, IW=무결성 등급, O=소유권, P=허가권)

```
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

4.2 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] 세션 객체 접근 제어

[그림 4]와 같이 세션 이벤트 매니저(Session Event Manager)안에 접근 제어 매니저(Access Control Manager)를 사용하게 된다. [그림 5]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 5] 세션 객체 접근 제어 알고리즘

4.3 공유 객체 접근 제어

사용자가 공유 객체를 많이 사용하는 협력 시스템의 경우 접근 제어 서비스 모듈은 보안 측면뿐 아니라 협력 작업에서도 필요한 부분이다. [그림 6]에서는 공유 객체를 다루는 부분에서 데이터의 생성 및 업데이트, 실행에 관해서 접근자의 소유권, 무결성 등급 등을 규칙 테이블의 정의된 규칙과 비교하여 행동을 제어하게 된다.

```
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 6] 공유 데이터 접근 제어 알고리즘

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.

5. 결론

최근 개방형 정보 통신망을 이용하는 협력 시스템에서의 작업이 급격히 증가하면서 보호해야 할 정보의 가치와 대상도 증가하며, 또 이에 대한 적절한 대응도 필수적으로 되었다. 본 논문에서는 협력 시스템에 개입된 주체들 사이의 가장 심각한 위협요소로부터 시스템의 안정성을 확보하기 위한 핵심 부분인 접근 제어부분만을 다루었다. 그리고 현재 개발중인 시스템을 모델로 하여 협력 시스템에 맞는 보안 서비스 개발에 대하여 논하였다. 향후 연구 과제로는 데이터 전송시 사용자의 요구에 따라 다른 비밀성과 무결성을 지원하기 위한 QoP(Quality of Protection) 서비스를 고려하고 있으며 보안 환경의 변화에 적응할 수 있도록 보안 정보 관리 프레임워크를 강화 할 필요가 있다.

6. 참고 문헌

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

[2] 양진모 외, 산업 디자인 협력 시스템에 대한 연구, 정보처리학회, 1999.4

[3] 강창구 외, 통합정보 모델을 이용한 접근제어 메커니즘 설계 및 구현, 한국정보처리학회, 1997.9

[4] Shari Lawrence Pfleeger, A Framework for Security Requirements, Computer & Security Vol.10, 1991

[6] Warwick Ford, Computer Communications Security-Principles, Standard Protocols and Techniques, 1994