유비쿼터스 환경에서 업무시 컴퓨터 보안에 대한 연구

이명희* · 유재언**

1. 서 론

유비쿼터스 환경에서의 보안정책은 "민감한 정보를 관리하고, 보호하고, 구분하는 체계를 현실적인 조정과 법률과 관습을 통해서 설정하는 것"이라고 할 수 있다[1]. 기업들의 보안 정책은 그들의 정보의 민감성이나 가치 등을 포함하는 다양한 요인들에 의해 좌우되며 또한 그 정보의 손실이나 잘못된 사용도 영향을 미치고 있다. 또한 기업들은 개인의 사생활과 정보시스템에서 나타나는 정보의 보호를 위해 특정한 보안 절차의 채택을 법적으로 요구 받고 있는 상황이다.

필수적으로 알아야 할 사항(the need to know)은 사용자(user)가 접근할 수 있는 정보의 양을 최소화되게 결정하는 것이다. 이러한 원칙은 보안 연구에서 때때로 언급되지만 추상적이고 철학적인 개념과 같을 수 있다. 하지만 이러한 개념으로 받아들여야 할 것이다. 예를 들면 Saltzer와 Schroeder는 "완벽한 직무를 위해 필연적인 것"이라고 얘기하고 있지만 직무(job)의 정의[2]에 대해서는 언급을 하지 않고 있다. Summers는 사람은 정보에 접근하기 위해 필수적으로 알아야 할 사항을 갖고 있어야 하지만 그 필수적으로 알아야할 사항을 어떻게 결정하느냐에 대해서는 상세히 설명하고 있지 않다[3].

필수적으로 해야 할 업무(task)를 이행해야 하는 운영상의 문제와 반드시 관련이 있게 된다. 운영상의 다양한 유형이 필수적으로 알아야 할 사항에 의해 가정되는 동안 운영상 특성을 만들며 운영상의 "필수적으로 해야 할 행동"과 같은 양상을 보이게 된다. 필수적으로 해야 할 행동(the need to do)은 필수적으로 알아야할 사항에 의해 요청된 정보를 통한 최소한의 운영으로 정의된다.

임의의 보안상의 접근은 사용자(user)가 강제적인 접근과 같이 동일하고 공식적인 보안인증으로 정보에 접근할 때 얻을 수 있는 정보에 대한 유연성이 필요하다.

몇 몇의 연구결과는 필수적으로 알아야 할 사항에 대한 정책을 기본으로 하는 역할을 정의내리고 있다[4]. 특정한 사용자(user)에게 독점적으로 접근(Access)을 승인을 하지 않지만 일반적인 업무 환경[5,6], 교육[7], 보증[8]과 같은 조직체계의 어플리케이션을 위해 각 역할에 기본이 되는 권한

※ 교신저자(Corresponding Author) : 이명희, 주소 : 서울시 강남구 삼성동 167번지 한국전력거래소 (135-791), 전화 : 02-3456-1741, FAX : 02-3456-6599,
E-mail : yi3253@kpx.or.kr
* 한국전력거래소
** 서울벤처정보대학원대학교 정보경영학과 교수
(E-mail : 6230yu@suv.ac.kr)

을 승인해주게 된다. 그러나 관리자(manager)나 사무원(clerk)과 같은 역할은 보다 넓은 범위로 실체(entity)로 정의되며, 필수적으로 알아야 할 사항에 대한 세부적 명세(specification)에 대해서는 정의하지 않는다.

Biskup[9]은 개인적인 사항과 사용자(user)가 자신의 정보에 접근하는 사람을 결정하는 권리와 같이 필수적으로 알아야 할 사항에 대한 확인을 해야 한다고 한다. 그러나 사적인 내용의 접근과 같은 어플리케이션에서 사용자(user)가 자신의 정보에 접근하는 인원을 결정하는 사항에 대해서는 상호 협의에 의한 몇 몇의 user만을 제외하고는 제한하게 된다.

1.1 과정

본 논문에서는 사용자(user)가 업무(task)를 이행하기 위해 필수적으로 알아야 할 사항과 필수적으로 해야 할 사항에 대해 제안하게 된다. 업무(task)는 이미 존재하고 사용자(user)(task이 할당된 인원)와 정보(task를 완료하기 위해 요구되는 사항) 양쪽에 직접적으로 관계가 있는 일반적인 실체이다. 본 논문에서는 더욱 명확한 세부 업무(task)로 나누게 되는 업무(task)의 간결한 구조에 대해 정의하게 될 것이다.

유비쿼터스 환경에서 GSM(Group Security Model)으로 불리는, 사용자(user)가 시스템의 정보에 접근하기 위해 필수적으로 알아야 할 사항과 그 정보를 갖고 지정된 업무(task)를 완료하기 위해 정보를 수정해야하는 필수적인 사항을 제한하는 보안모델을 정의하게 된다.

2장에서는 UGSM에서 인증을 기초로 선택된 업무(task)의 기술과 정당성을 나타내고, 3장에서는 결론을 도출한다.

1.2 연구

조직의 목표와 목적에 의해 나타나는 "존재 이유"는 직무의 정의와 지시와 그 직무를 성취하는 것으로 정의된다. 이것은 조직이나 기업에서 가장 기본적인 개념의 업무(task)로 나타나며 유비쿼터스 환경에서 보안모델을 기본으로 적절하게 초점이 맞춰져 있다.

어떻게, 어떤 원리를 갖고, 조직에서 내린 정의를 기본으로 어떤 업무(task)를 어떻게 할당하는 문제는 조직의 관리와 운영상의 사상에 영향을 받게 된다. 계층적 구조를 갖는 조직에서 업무(task)는 가장 상위 수준의 업무(task)가 결정됨에 따라 그 영향으로 하부임무(subtask)가 결정되고 있다.

조직의 각 수준에서 고용인은 자신의 업무(task)를 더욱 세부적으로 하기 위해 다듬어지며 다음 하위 수준에서 고용인의 하부업무(subtask)를 지정하게 된다. 단체로 조직된 환경에서 업무(task)의 생성과 세분화는 조직 내의 각 개인사이의 논의와 타협으로 이루어지게 된다.

업무(task)를 완료해야하는 책임이 주어지는 개인이나 집단과 관계되는 업무(task)가 있다면 몇 몇의 사람들은 업무(task)를 관리하는 특정한 역할이 주어지게 된다. 예를 들면, 만일 업무(task)가 개개인이 모여 있는 단체에 주어지게 된다면 그 중 한사람은 업무(task)를 완료하기 위해 통솔력이나 관리상의 책임이 주어지게 될 것이다.

이런 업무(task)에 대한 사용자(user)의 지정은 각 지정된 업무(task)의 기본적인 권한으로 이루어진다. 더욱 일반적으로 얘기하면, 사용자(user)는 그 업무(task)를 정의하는 사람이나 리더와 같이 특정한 역할을 갖고 있는 사람에 의해서 그 업무(task)를 할당받게 된다. 각 개인은 조직 구조에서 자신보다 하위수준에 있는 사람이나 업무

(task)의 감독을 하는 사람들에게 업무(task)를 할당 받기도 한다.

단지 사용자(user)가 업무(task)와 관계를 갖고 있다면 정보는 업무(task)와 관계를 갖게 된다. 각 업무(task)는 업무(task)의 성취를 요구하는 어떤 정보와 관계를 갖고 있어야 한다. 사용자(user)에게 업무(task)를 할당하는 것은 일반적으로 조직의 구성과 정책, 요구사항에 의해 결정되어는 것에 반하여 사용자(user)가 어떤 업무(task)를 성취해야만 얻게 되는 정보를 결정하는 것은 그 업무(task)를 만드는 사람에게 있게 된다. 그러나 사용자(user) 또한 업무(task)를 완료하기 위해 그들이 요구하는 정보가 무엇인지 알게 된다.

현재의 논쟁은 어떻게 정보가 업무(task)와 관련 있게 되나?, 요구사항에 대해 어떻게 업무(task)를 이행하거나 생성해 내는가?, 그리고 요구한 정보에 대해 어떻게 접근을 받아들이는가? 업무(task)에 의해 요구되어서 실행한 정보를 어떻게 보증하나?, 그리고 얻은 정보를 업무(task)의 완료를 위해서만 어떻게 사용을 하나? 등이 있다.

정보는 임의로 접근할 수 없게 되어야 하며, 비록 특정 업무(task)를 이행하기 위해 요구된 정보와 같은 요구가 있다고 하더라도 강제적인 보안 모델에서 정보는 사용자(user)의 보안 수준과 요구된 정보의 보안 수준에 따라 접근하게 되며, 정보에 접근하는 인원 이외에 이러한 접근에 대해서 알 필요가 없게 된다. 특히 상업적인 환경에서는 보안 모델은 독자적인 모델로 나타나게 된다.

임의의 보안의 접근을 통해 요구된 정보의 소유자는 그 정보를 요청한 사람에게 접근 승인과 같은 평가를 허가하여야 한다. 만일 정보의 소유자는 요청된 정보가 합당하다고 하다면 그 정보가 요구된 업무(task)를 위해 사용되도록 해야 할 것이다. 만일 정보의 소유자가 업무(task)통해 요청된 정보의 접근을 승인하지 않는다면, 그 정보를 사용하여 업무(task)를 이행하게 되는 집단 리더(leader)는 다른 방법으로 정보를 구해야 할 것이다. 접근허가에 대한 권한은 그 정보의 소유자에게 있게 된다. (만일 모든 사람들이 그들이 원하는 모든 정보에 접근할 수 있다면, 모든 사용자(user)들은 그들의 신뢰만으로 접근하게 되며 컴퓨터 보안에 대한 필요성은 없게 될 것이다.)

개별적으로 정보의 접근을 요구하는 것은 누가 하는 것이 아니고 무엇에 의한 것도 아닌 각 업무(task)에 따라 개별적으로 할당된 업무(task)에 의해 요청되어야 한다. 업무(task)가 완료 된다면, 업무(task)를 통해 특정 정보를 요청하는 것은 더 이상 할 수 없게 된다. 개개인은 시스템에서 어떠한 정보도 더 이상 접근할 수 없게 될 뿐 아니라 현재 할당된 업무(task)의 완료와 그 책임을 져야 한다.

사용자(user)는 같은 시간에 몇 몇의 지정된 업무(task)의 완료를 해야 한다. 반드시 고려되어야 할 문제는, 사용자(user)는 자신의 업무(task)에 필요한 모든 정보에 접근할 수 있는 권한이 있어야만 하는 것이다. 이것은 실제 상황에서는 보편적인 방법일 것이다. 예를 들면 주어진 몇 개의 업무(task)를 정상적으로 완료하지 못한 개인은 상이한 업무(task)로부터 종료되지 못한 업무(task)의 정보 보호가 요구되며, 어느 특정시점에서 업무상으로 한 가지 정보로만 업무(task)를 이행하여야 할 것이다. 그러나 실제적인 생활에서 같은 시간대에 개개인은 자신에게 지정된 모든 정보에 대해 알고 있다.

그러나 이것은 필요하지 않을뿐더러 바람직한 사항도 아니다. 다양한 업무(task)에 대한 많은 정보의 조합으로부터 필요하지 않은 기회를 만들어 사용되거나 결과를 끌어내게 된다. 사용자(user)는 지정된 순간에 하나의 업무(task)와 관련된 정

보의 접근만을 할 수 있어야 한다. 업무(task)를 이행하기 위해 요구되는 모든 정보는 그 업무(task)와 관련이 있어야 한다. 같은 시간대에 여러 업무(task)에 대한 정보의 접근은 그 정보를 알아야 할 필요가 있는 어떤 법칙 하에서 이루어 져야 한다. 만일 사용자(user)가 몇 가지 업무(task)와 연관되어 있는 정보로부터 어떤 결론을 도출해내야 한다면 업무(task)는 그 자체만으로 필수적인 정보가 되며, 그 정보와 연관성을 갖게 된다.

특히 몇 몇의 사용자(user)가 중요한 object에 접근을 하게 된다면 업무(task)는 그 사용자(user)를 효과적으로 묶게 되는 실체가 된다. 많은 사용자(user) 대신에, 그 사용자(user)와 관계가 있는 업무(task)로 정보에 접근을 하게 되면 업무(task)와 관계를 맺고 있는 사용자(user)들은 그 정보에 접근을 승인받게 된다. 이와 유사하게 업무(task)는 정보를 그룹화 해서 그 정보그룹에 대해 승인을 하게 된다. 그러므로 사용자(user)는 많은 정보와 연결되어있는 업무(task)에 연결되어 있는 것이 필요하다.

필수적으로 알아야 할 사항을 기본으로 하는 업무(task)를 사용하는 것에는 많은 이익이 있다. 하위 업무(task)가 완료되면 그 상위 업무(task)를 완료시킬 수 있다. 비록 원형이라고 하더라도 만일 그 업무(task) 조직이 목표나 목적이 변하지 않는다면 최초 수준의 업무(task)는 결코 완료되지 않게 될 것이다.

어떤 업무(task)를 통해 정보에 접근을 하게 될 때 정보에 대한 접근 승인은 각자 역할[4,6,9]에 따른 정보 접근을 승인하는 제한된 장점을 갖게 된다. 역할보다도 업무(task)들은 더 작은 하위 개념의 개체들이며 기본적인 정보의 요구사항들에 대해 일시적 framework를 가지고 있다, 예를 들면, 한 관리자의 역할이 진행 중 일 때, 많은 특정한 시작부분과 끝부분에 관련해서 다른 관리자들이 수행하는 다양한 업무들이 존재한다. 또한 업무(task)는 유연성을 갖고 있으며, 통계적인 정의로 나타나는 역할과 비교 할 수 있는 동적인 속성을 갖고 있다.

2. 유비쿼터스 환경에서의 보안 모델

USGM(Ubiquitous Group Security Model)의 목적은 할당된 업무(task)를 완료하기 위해 각 사용자(user)가 정보에 접근할 때 필수적으로 알아야 하는 것과 운영상 사용자(user)가 필수적으로 해야 할 사항들을 제공하는 것이다.

USGM은 사용자(user), 역할(role), 업무(task), 접근유형(access type), 오브젝트(object) 다섯 가지 요소로 구성되어있다. (그림 1) 사용자(user)는 정보시스템의 접근 시 승인을 받을 때 각기 다른 독립적인 실체로 표시된다. 업무(task)는 조직에서 수행하는 활동영역이나 할당된 몫으로 표시된다. 오브젝트(object)는 시스템 상에서 정보의 실체로 표시된다. 역할(role)은 사용자(user)가 업무(task)를 하기 위해 갖는 관계로 표시되는 사용자(user)와 업무(task)사이에 관련된 연결을 뜻한다. 리더와 구성원, 접근유형(access type)은 사용자(user)가 오브젝트(object)에 읽기, 쓰기 등을 실행 하는 것과 같은 운영으로 나타나는 업무(task)와 오브젝트(object) 간의 연결을 뜻한다.

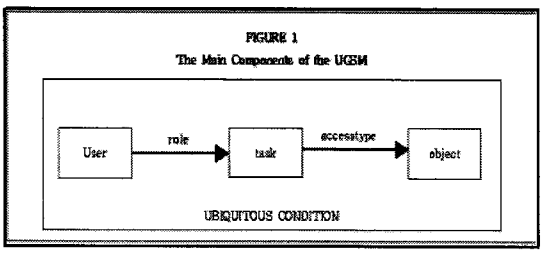


그림 1. UGSM의 구성

사용자(user)는 역할(role)을 통해 오브젝트(object)를 할당 받게 된다. 정보는 접근유형(access type)에 따라 업무(task)와 연결된다. 사용자(user)는 할당받은 업무(task)와 관련되고 조건으로 지정된 접근 유형에 의해서만 정보에 접근할 수 있게 된다. 만일 정보가 필수적으로 알아야할 사항과 필수적으로 해야 할 정책과 관련된 업무(task)라면 사용자(user)는 필수적으로 접근해야 하는 정보와 할당받은 업무(task)를 완료하기위해 필수적으로 해야 하는 운영을 제한받게 된다.

UGSM은 업무(task)를 이행하기 위해 정보 소유자의 판단으로 정보의 접근을 승인하게 되는 임의적인 보안모델이다. 정보를 소유하고 있는 사용자(user)의 필수적으로 해야 할 행동중의 하나는 정보의 접근을 요구하는 사람들에 대해서 접근을 부여하는 책무가 있다.

UGSM은 임의적인 보안 모델에서 전형적인 구성요소가 없는 강제적인 보안 요소를 포함하고 있다. 오브젝트(object)의 소유자는 자신의 정보에 접근의 승인을 부여할 수도 있으며(임의로 하지는 않음) 업무(task)의 인원에 제한을 두기도 한다. 또한, 업무(task)를 할당 받은 모든 사용자(user)가 정보를 받게 해서 안 된다. 리더의 역할을 하게 되는 사용자(user)만이 다른 업무(task)에 대한 정보를 받을 수 있게 하여야 한다.

완전한 UGSM은 Telos[10] graphical standards를 사용하는 그림 2와 같이 표시된다. 비록 UGSM이 Telos언어로 정의되었다고 하지만 보안모델은 모든 정보시스템에 적용할 수 있다. 우리가 오브젝트(object)라고 부르는 것은 데이터 모델에 의해 가용한 정보의 어떤 개체라도 될 수 있다. UGSM에서 기술한 사항은 모든 특정데이터 모델을 가정하는 것은 아니다.

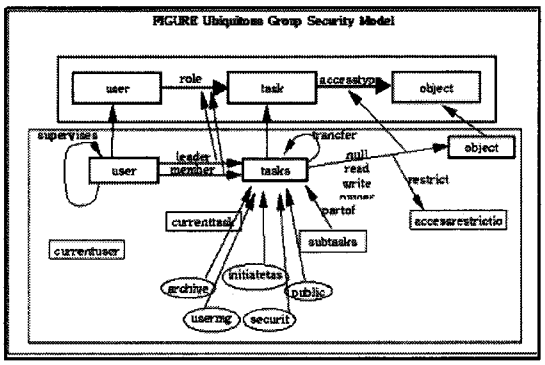


그림 2. Ubiquitous Group Security Model

그림 2의 위쪽절반 부분은 다섯 개의 기본적인 구성요소인 사용자(user), 역할(role), 업무(task), 접근유형(access type), 오브젝트(object)를 표시하고 있다. 아래쪽 절반은 조건으로 지정된 역할(role), 업무(task), 접근유형(access type)과 같은 기본 구성요소사이의 관계를 보여주고 있다. 다음의 단락들은 UGSM의 5대 구성요소의 간략한 설명을 보여준다.

2.1 사용자(Object user)

Object user는 시스템에서 정보에 접근을 하는 각기 다른 사람으로 표시된다. 사용자(user) 사이의 관계는 superviser link에 의해 지정되어있다. 사용자(user)는 역할(role) link에 의해 하나 이상의 업무(task)를 할당 받게 된다. 현재 등급의 사용자(user)는 일반적으로 정보시스템에 접근하는 사용자(user)를 등급의 한 예로 정의한 것이다.

2.2 관계(Role Link)

관계(role link)는 사용자(user)와 업무(task)사이의 관계로 정의된다. UGSM에서는 리더(leader)와 멤버(member)라는 두 종류의 역할로 정의한다. 업무(task)와 연결되어있는 멤버(member)

로서의 사용자(user)는 업무(task)에서 부여된 접근유형(access type)에 의해 시스템에서 오브젝트(object)에 접근할 수 있다. 업무(task)와 연결되어있는 리더(leader)로서의 사용자(user)는 하위업무(subtask)를 생성할 수 있으며, 다른 업무(task)에 대해 정보의 접근 인가를 승인할 수 있는 책임과 특권을 갖고 있다. 한 업무(task)에 대해서는 한명 이상의 리더(leader)를 갖을 수 있다.

2.3 업무표현(Task Represent)

오브젝트 업무(Object task)는 실행하기 위한 활동이나 할당으로 표시된다. 사용자(user)들은 업무(task)를 실행하기 위해 주어진 관계(role link)에 지정된다. 업무(task)를 완료해야 하는 시스템의 오브젝트(object)는 접근유형(access type)에 따른 업무(task)와 관련이 있다. 사용자(user)는 자기에게 할당된 업무(task)와 관련된 정보만 접근해야 한다.

더욱 세부적인 업무(task)의 기술(description)과 지정을 하기 위해서 업무(task)는 등급에 따른 하위업무(subtask)로 나누어져야 한다. link의 일부분은 하위업무(subtask)와 상위업무(parent task) 간을 연결한다. 전달 link는 이 업무(task)에 해당하는 오브젝트(object)들이 (다른)어떤 업무(task)로 전달되어야 하는지(전달 될 수 있는지) 자세히 설명해 준다.

현재 업무(task) 등급에서는 어떤 순간에서라도 정보시스템의 일반적인 접근을 위해 어떤 하나의 예를 갖고 있어야 한다.

아카이브(archive), 보안(security), 초기업무(initiate task)는 UGSM의 관리를 위해 요구되는 특정한 public 이다. 사용업무(task)는 사용자(user)를 만들거나 삭제할 수 있는 기능을 갖고 있다. 공용업무(pubic task)는 모든 사용자(user)가 접근할 수 있는 정보로 구성되어있다. 아카이브 업무(archive task)는 그 업무(task)의 이력을 소유하게 된다. 보안업무(security task)는 다양한 보안 해석 활동을 수행할 수 있다. 초기화업무(initiate task)는 최초 수준(초기상태)의 업무(task)를 만들 수 있다.

접근유형(access type)은 업무(task)와 사용자(user)가 지정된 오브젝트(object)에 의해서 수행하는 운영으로 표시되는 오브젝트(object)간의 link이다. UGSM에서 정의한 접근유형(access type)은 데이터 모델(data model)과 정보시스템에서 정의된 operation에 의해 정해진다.

일반적인 접근유형(access type)은 read, write, owner를 포함하고 있다. 접근유형(access type)들 중에서 접근 제한의 속성은 접근유형(access type) link의 응용성과 타당성에 관한 추가적인 특성에 의해 정의되는 정보의 owner에 의해 결정된다.

2.4 데이터 모델(Data Model)

데이터 모델(data model)에 의해 결정되는 오브젝트(object)는 시스템에서 정보의 실체로 표시된다. 오브젝트(object)기반의 추론적(rational)인 데이터(data)는 file, view, relation, record, field임에 반하여 연역적(deductive)인 객체 기반의 object는 atomic, composite object, class, attribute, rule, object의 제약유형(constraint type)을 나타낸다.

업무(task)를 이행하기 위해 요구되는 오브젝트(object)는 업무(task)와 접근유형(access type)의 사이에 반드시 연관이 있어야 한다. 조직의 보안정책과 데이터 모델(data model)에서 효과적인 오브젝트 유형(object type)을 결정하기 위해서는

오브젝트(object)에 접근은 오브젝트(object)와 관련된 접근을 포함하여야 한다.

2.5 유비쿼터스 경영환경에서 보안 모델 (UGSM Ubiquitous Group Security Model)

UGSM은 정보시스템에서 인터페이스와 같이 권한을 갖게 된다. 정보는 오직 UGSM을 통하여 접근할 수 있게 된다. UGSM은 그 자체만으로 정보 시스템의 한 부분으로 인식된다. 시스템에서 다른 오브젝트(object)와 유사한 UGSM을 포함하는 오브젝트(object)는 적절한 접근 승인 권한을 갖고 있는 사용자(user)에 의해서만 정보에 접근하고 그 정보를 수정할 수 있는 자격을 갖게 된다. UGSM과 정보시스템 간의 관계는 fig3)과 같이 나타낼 수 있다. 정보시스템에 접근을 요청하는 것은 UGSM을 통해서 하게 된다. 만일 현재 사용자(user)와 업무(task)를 위한 접근 승인이 인가되면 정보 시스템에서 나온 데이터(data)는 조건으로 지정된 접근유형(access type)에 의해서 제공 되고 수정할 수 있게 된다.

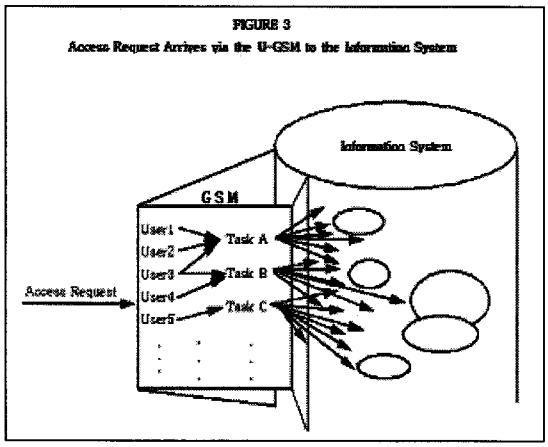


그림 3. Access Request Arrives via the U-GSM to the Information System

업무(task)는 GSM의 충주적인 구성요소이다. 업무(task)를 실행하기 위한 과정에서 활동이나 지정으로 표시되며 시스템에서 정보 접근을 요구하게 된다. 사용자(user)는 사용자(user)가 업무(task)에서 갖는 역할(role)과 관련이 있다. 오브젝트(object)는 업무(task)가 완료되는 과정동안 오브젝트(object)가 승인하게 되는 운영(operation)으로 표시되는 접근유형(access type)과 연결된 업무(task)와 관련이 있다. 그래서 업무(task)에서 역할(role)을 갖는 사용자(user)는 접근유형(access type)의 연결을 통해 업무(task)와 관련된 오브젝트(object)에 접근 하게 된다.

업무(task)에는 업무(task), 하위 업무(subtask) 두 개의 class가 있다. 최초 수준(first level) 업무(task)는 상위 업무(parent task)가 없는 업무(task)로 표시되는 업무(task)의 등급의 예로 설명할 수 있다.

link의 한 부분을 통해서 상위 업무(parent task)와 하위 업무(subtask)에 대해서 알 수가 있게 된다. 업무(task)는 계층적 구조나 계승적인 특성을 갖지는 않는다. 이것은 첫째로 실질적인 업무(task)는 논리적인 핵심이나 특징을 갖고 있으며 오브젝트(object)의 등급으로 구성된 것이 아니며, 둘째로는 업무(task)의 특성을 갖는 사용자(user)가 상위 업무(parent task)의 특성을 갖고 있는 업무(task)와 관계된 경우는 일반적인 경우가 아니라는 점이다. 또한 오브젝트(object)는 업무(task)가 하위 업무(subtask)에 의해 특성을 자동적으로 받지 않는 것을 요구하게 된다.

업무(task)는 source task가 정보에 접근을 승인하는 destination task 부여함으로써 표시되는 전달 특성을 갖게 된다.

class task와 같은 예를 생성할 수 있는 능력이 최초수준의 업무(task)에서 가능하다. 초기업무

(initiate task)라고 불리는 administrative task는 이러한 접근의 인가로 정의된다. 이러한 접근의 인가는 아래와 같이 지정된다. 하위 업무(subtask)의 생성을 인가하는 것은 업무(task)의 리더(leader)에게 그 권한이 주어진다.

보통 오브젝트(object)를 갖고 있는 업무(task)는 다른 업무(task)에게 자신의 오브젝트(object)에 접근할 수 있는 권한을 부여한다. 다른 방법으로는 오브젝트(object)에 접근의 인가를 받는 것이 있다. 즉 상위 업무(parent task)를 통해서 인가를 받는다. UGSM은 업무(task)의 leader에게 leader가 갖고 있는 업무(task)의 접근인가를 복제하여 하위업무(subtask)의 접근을 인가할 수 있게 하고 있다.

업무(task)와 관련된 정보가 그 업무(task)에 할당된 모든 사용자(user)가 접근할 수 있게 된다면, 사용자(user)가 업무(task)의 다른 책임으로 요구된 정보에 접근 할 수 있는 동안 사용자(user)는 필요 이상 정보에 접근을 할 수 있게 된다. 업무(task)의 상이한 측면을 실행하고 있는 사용자(user)를 갖고 있는 업무(task)의 리더(leader)는 더욱 세부적이고 명확하게 하위 업무(subtask)로 나눠야 한다. 그런 다음에 다양한 사용자(user)는 업무(task)에 지정하게 되며 하나의 상위 업무(parent task)가 아닌 확실히 구분된 하위 업무(subtask)로 지정된다. 그런 이후 모든 오브젝트(object)와 관련된 상위 업무(parent task)의 접근권한 대신에 하위 업무(subtask)와 연관된 오브젝트(object)에 대한 접근권한만을 부여하게 된다.

하위 업무(subtask)를 실행하기 위한 요구사항의 집합은 상위 업무(parent task)의 실행을 위해 요구사항의 부분집합으로 나타난다. 이와 유사하게 하위 업무(subtask)에 접근하기 위해 필요한 오브젝트(object) 그룹은 상위 업무(parent task)가 요구하는 오브젝트(object)의 부분집합이다. 만일 상위 업무(parent task)가 업무(task)를 수행하기 위해 요구되는 모든 정보에 대해 접근인가를 갖고 있다면, 각 하위 업무(subtask)는 상위 업무(parent task)에 접근할 수 있는 정보에 대한 부분을 요구하게 된다. 업무(task)가 하위 업무(subtask)로 나누어진 경우 접근을 하기 위해 더 많거나 상이한 오브젝트(object)를 요구하지는 않게 된다. 정보를 얻기 위한 하위 업무(subtask)의 목적이 더욱 세분화되어서 정의되고 있으면, 하위 업무(subtask)를 실행하고 있는 동안 정보에 접근하기 위한 모든 목적은 같아지게 되며, 상위 업무(parent task)의 한 부분으로 실행하게 될 것이다.

상위 업무(parent task)에서 하위 업무(subtask)로 사용자(user)의 레벨을 고려하여 접근인가를 복제하는 과정을 승인하지 않기 위한 논의는 보안 모델(security model)에서 하게 된다. 상위 업무(parent task)는 하위 업무(subtask)와의 관계보다는 조직에서 상위 업무 리더(parent task leader)의 관리 하에서 더 높은 승인 레벨을 갖는 더 높은 수준의 고용인에게 책임을 부여한다. 정보의 소유자는 그 정보에 대한 목적이 동일할 지라도 그 정보가 접근 레벨이 낮은 고용인에게 자신의 정보가 채택되는 것을 동의하지 않을 것이다. 만일 정보의 접근이 사용자(user)의 레벨에 따라서 구분된다면, 그 사람의 업무(task)에서 사용되고 있는 필수적으로 알아야 할 사항이 레벨에 따라 차이가 나게 될 것이다. 이러한 사항은 GSM의 목적은 아니다. GSM은 사용자(user)의 레벨을 기본으로 승인 인가를 하는 것이 아닌 필수적으로 알아야 할 사항을 토대로 접근권한을 지정하게 된다.

UGSM은 정보의 용도가 커지게 되어 처음 부가되었던 정보의 용도를 벗어나기 때문에 상위

업무(parent task)의 접근 승인을 복제(copy)를 통해 접근 인가를 하는 능력을 허용하지 않는다.

임의의 보안 접근은 정보의 소유자에게 다른 사용자(user)가 자신의 오브젝트(object)에 접근할 수 있는 권한을 준다. UGSM은 이러한 권한을 업무(task)의 리더(leader)에게 부여하고 있다. 그러나 UGSM은 정보의 수용자와 정보의 소유자 사이의 전달 고리의 요구에 의한 정보의 소유자가 위임한 권리에 더욱 제한을 가하고 있다. 이러한 제한은 UGSM에서 강제적인 보안규정 한도로 제공된다. 전달 고리(Transfer link)는 정보가 어디로 흐르는지 표시하게 된다. 이러한 transfer link는 Biskup[11]의 privacy model에서 설명하는 subchannel과 유사하다.

Transfer link는 업무(task)와 업무(task)의 상위 업무(parent task)사이나 업무(task)와 하위 업무(subtask)사이에서는 필요하지 않다. transfer link는 업무(task)의 리더(leader)에 의해서 생성된다. 이것에 의해서 두 명의 리더(leader)가 정보의 전달에 필요로 하게 되어서 한 명은 transfer link를 제공하게 되며, 한명은 정보의 전달을 맡게 된다. (비록 두 개의 업무(task)의 리더(leader)는 반드시 다른 사람이 되어야 한다는 조건을 정하지는 않았지만 이러한 조건은 추가되어야 한다. 아니면 만일 상위 업무(parent task)의 리더(leader)가 하위 업무(subtask)의 리더(leader)와 같이 동일한 사용자(user)라면 transfer link의 생성은 감사 보고서를 통해서 나타내야 한다.) 만일 source task가 상위 업무(parent task)가 없는 최초 수준의 업무(task)라면 업무(task)의 리더(leader)는 다른 업무(task)와의 transfer link를 스스로 만들 수 있게 된다.

예를 들면 만일 업무(task)A가 업무(task)B에게 부여한 오브젝트(object)를 갖고 있다면 업무(task)A의 상위 업무(parent task)의 리더(leader)는 가장먼저 업무(task)A와 업무(task) B의 transfer link를 제공하여야 한다. 업무(task)A는 최우선 순위의 업무(task)로 실행하게 되며 그 이후에 업무(task)A의 리더(leader)는 업무(task)B로부터 transfer link를 만들게 된다. 조직(organization)은 transfer link를 생성하는 인원에게 더욱 나은 조건을 설정해 줘야 한다. 형편에 따라 최우선순위 업무(task)의 리더(leader)는 자신의 하위 업무(subtask)의 transfer link를 생성하게 된다. transfer link의 삭제 또한 상위 업무(parent task)의 리더(leader)나 업무(task)의 리더(leader)에 의해서 실행된다.

업무(task)는 바라던 결과를 이루거나, 업무(task)가 끝날 때 종료된다. 업무(task)가 종료되면 그 하위의 모든 하위 업무(subtask)도 종료된다. 일반적으로 사람들은 하위 업무(subtask)가 상위 업무(parent task)보다 먼저 종료되기를 원하게 된다. 업무(task)가 종료되면 사용자(user)는 더 이상 그 업무(task)와 관계된 정보시스템에 접근을 할 수 없게 된다.

업무(task)는 최우선순위의 업무(task)의 경우만 제외하고는 상위 업무(parent task)의 리더(leader)에 의해 종료된다. 초기 업무(Initial task)의 리더(leader)는 최우선순위 업무(task)가 상위 업무(parent task)를 갖지 못하는 동안에는 최우선순위 업무(task)를 삭제하는 능력을 갖게 된다.

업무(task)가 종료되기 전에 업무(task)의 리더(leader)는 자신의 업무(task)가 다른 업무(task)를 유일하게 소유하는 상위 업무(parent task)가 되기 위하여 정보의 소유권을 갖게 된다. 그렇지 않다면 시스템은 정보의 소유를 위해 아카이브 업무(archive task)를 만들게 될 것이고 이를 통해서 유일한 정보 소유자로 업무(task)를 종료하게

될 것이다. 시스템에서 모든 정보는 항상 업무(task)가 소유하고 있어야 한다.

아래의 절은 UGSM의 관리상의 목적으로 업무(task)가 요구하는 사항을 기술한 것이다.

공용 업무(public task)는 모든 업무(task)가 접근할 수 있는 정보와 관련된 업무(task)이다. 초기 업무(Initiate task)는 업무(task)의 리더가 최우선 순위 업무(task)를 종료하고(parent task가 없는 task)생성하는 것은 허가한다. 이 업무(task)는 class task와 같은 예에서 보듯이 생성하고 삭제할 수 있게 된다. 모든 업무(task)가 리더(leader)를 요구하게 되면 이 업무(task)는 하위 업무(subtask)를 생성 할 수 있는 리더(leader)를 부여하게 된다. 초기 업무(Initiate task)의 리더는 최우선순위의 업무(task)를 삭제할 수 있으며 삭제된 업무(task)로부터 leader를 제거할 수 있다. mgmt task 사용자(user)의 리더(leader)인 사용자(user)는 UGSM에서 사용자(user)와 super-vice link를 더하거나 삭제할 수 있다. 아카이브 업무(Archive task)는 소유자가 없는 모든 오브젝트(object)의 소유권자가 된다. 오브젝트(object)의 소유자는 오브젝트(object)의 접근을 인가에 대한 사항을 제공하게 된다. Current task는 하나의 예를 포함하는 업무(task)의 subclass로서 다시 말하면 현재 정보시스템에 접근하고 있는 업무(task)이다. 이러한 업무(task)는 처리(transac-tion)의 모든 요청이 시작할 때 설정되어진다. GSM의 명세에서 많은 규칙과 제약들은 current task에 명확화 되어있다.

어떤 특정한 정보를 알아야하는 업무(task), 즉 접근하는데 허가가 필요한 정보는 현재 (소유하고 있는) 접근 인가가 쓸모없게 만드는 (또 다른) 것을 요청하게 된다. 예를 들어, 읽는 것은 허가가 되지만 쓰는 것은 또다시 허가를 받게 하는 것이 있다.

GSM에서는 정보에 대한 요구사항이 업무(task)의 리더(leader)에 의해 만들지는 것과 같이 다른 업무(task)와 통신을 허용하는 것도 업무(task)의 리더(leader)에게 있다.

요청된 업무(task)는 올바른 정보를 소유한 사람에게 필수적인 지식이 아니기 때문에 이러한 요구사항은 시스템에 의해 처리되어진다. 요청되어진 정보가 존재 하건 하지 않건 간에 만일 정보가 존재하지 않는다면 메시지는 정보의 소유자에게 보내지지 않는다. 또한 시스템은 접근 인가 요청에 대한 회신은 하지 않게 된다. 그렇지 않고 회신을 하게 된다면 시스템에서 존재하거나 존재하지 않는 오브젝트(object)를 알아내는 방법으로 사용될 것이다. (그 시스템에 오브젝트(object)의 존재 유무에 대해서 알려져서는 안된다.)

만일 접근승인을 위한 오브젝트(object)가 존재 한다면 시스템은 요청에 대한 업무(task)(적절한 오브젝트(object)를 갖고 있는)를 보내게 될 것이다. 만일 하나이상의 업무(task)가 요청된 오브젝트(object)에 접근유형(access type)을 갖는 owner를 갖고 있다면 이러한 요청사항은 모든 업무(task)로 보내지게 된다.

요청된 정보를 갖고 있는 업무(task)의 리더(leader)는 그 요청사항에 대해 접근인가를 부여하거나, 거부하거나, 무시하는 과정을 반드시 결정해야 한다. 요청된 오브젝트(object)에 접근 인가는 요청된 업무(task)에게만 그 권한을 부여하게 된다. (접근 인가는 transfer link를 통해서 업무(task)에게 부여된다.) 요청사항에 대한 거부는 요청한 업무(task)에게 메시지를 보내게 되어 왜 접근 승인이 이루어지지 않았나에 대해 설명하게 된다. 또한 업무(task)는 접근 요청에 대한 회신으로 무시(ignore)를 부가항목으로 갖게 되며, 이

러한 회신을 통해서 요청된 정보가 존재하고 있다는 것을 알게 된다. 만일 이러한 회신이 없다면, 요청하는 정보가 오브젝트(object)에 대해 접근 승인이 거절되었거나, 아니면 시스템에 오브젝트(object)가 존재하는지에 대한 정보를 알 수 없게 된다.

3. 결 론

지금까지 유비쿼터스 환경에서 보안모델의 정보에 접근하는 관점에 대해 논의 하였다. 현재 존재하고 있는 이러한 업무(task)의 개념과 이해는 현재 사용되고 있는 대부분의 환경에서 많은 부분 사용되고 있으며 많은 유사부분을 갖고 있다. 몇몇의 업무(task)를 실행하는데 있어서 많은 부분 사용자(user)들은 이러한 개념을 사용하고 있다. 모든 정보에서 필요한 것은 업무(task)와 관련되어 있어야 한다. 업무(task)는 정보의 공유뿐만 아니라 정보에 접근인가를 받기 전이라도 통신과 협상을 위한 요구사항을 공유할 수 있는 구성요소 그룹을 포함하게 된다. 업무(task)는 종종 정보의 접근을 제한하기 위해 정보에 접근할 수 있는 시작시간과 종료시간이 존재하기도 한다. 지금까지 우리는 UGSM에서 사용자(user)의 업무(task)에 기본을 두고 있는 정보에 대한 접근의 명세(specification)에 대해서 기술해 왔다. 만일 사용자(user)가 업무(task)와 아무런 연관이 없다면, 사용자(user)는 정보 접근에 대해 요청을 할 수 없게 된다. 유비쿼터스 환경에서 몇몇의 보안 모델은 UGSM이 실제 생활에서 적용할 수 있는 보안모델이고, 정보 접근을 할 수 있는 업무(task)에 대한 보편적인 실체로 사용되는 것이 없는 접근통제를 하게 된다. 업무(task)의 이러한 개념은 Clark와 Wilson의 직무의 분리[12]를 위한 요구사항과 관련이 있다. UGSM에서 직무의 분리 이행은 업무(task)에 포함된 사용자(user)와 종속적이 된다.

UGSM은 업무(task)의 적절한 정의에 따라 그 형태를 갖게 되며, 사용자(user)가 접근 유형에 따라 필수적으로 알아야 할 최소한의 정확한 정보를 지정하게 된다. 만일 업무(task)가 과도한 범위에서 정의되고 필요한 정보 이상으로 접근이 이루어진다면 UGSM의 이점은 쉽게 없어질 것이다. 그렇게 때문에 업무(task)의 명세에서 사용자(user)를 돕기 위한 더욱 많은 연구와 업무(task)를 완료하기 위해 요구되는 정확한 정보와의 관계가 요구된다.

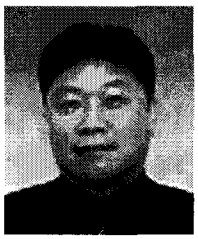
이러한 연구는 업무(task)의 명세와 특성에 의해서 이루어지게 된다. 예를 들면, 협력적인 업무(task)지향의 업무 모델은 Mahling, *et al.*[13]에 의해서 제안되었다. Steels[14]은 문제의 해석을 위해 필요한 것으로 업무(task)의 특성을 알기 위해 개념적인 해석과 실제적인 접근을 하였다. 업무(task)의 서로 다른 유형에 대한 특성(예를 들면, 진단법, 해석, 설계, 계획)은 정보의 요구사항에 대한 서로 다른 입력과 출력에 관계가 있다. 우리는 일반적인 업무(task)보다는 특정한 업무(task)와 그 업무(task)에 지정된 특정한 사용자(user)에 대해서 더 많은 고려를 하여야 한다.

참 고 문 헌

[1] Walker, S.T. "Setwork Security Overview," *Proceedings of the IEEE Symposium in Security and Privacy,* pp. 62-76, 1985.

[2] Sltzer, J.H. and M.D. Schrodeder. "The Protection of Information in ComputerSystems," *Proceedings of the IEEE,* 63:9, pp. 1278-1308, September 1975.

[3] Summer, R.C. "An Overview of Computer-Security," *IBM Systems Journal*, 23:4, 1984.
[4] Sandhu, R.S., E.J. Coyne, and H.L. Feinstein, "Role-based Access Control Models," *Computer*, 29:2, pp. 38-47, 1991.
[5] Harrison, M.A., W.L. Ruzzo, and J.D. Ullman." Protection in Operating Systems," *Communications of the ACM*, 19:8, pp. 461-471, August 1976.
[6] Lochovsay, F.H. and C.C. Woo. "Role-based-Security in Database Management Systems," in Landwehrm C.E. (Ed.), *Database Security: Status and prospects*, Elsevier, IFIP, pp. 209-222, 2000.
[7] Ting. T.C. "A User-Role Based Data Security-Approach," in Landwehr, C.E. (Ed.), *Database Security: Status and Prospects*, Elsevier, IFIP, pp. 187-208, 1988.
[8] Haigh, J.T. "Modeling Database Security-Requirements," in Landwehr, C. (Ed.).Database Security: Status and Prospects, Elsevier, IFIP, pp. 45-56, 1987.
[9] Biskup, J. "Privacy Respecting Permissionsand Rights," *Hildesheimer Informatik-Berichte*, Hochschule, Hildesheim, 2005.
[10] Mylopoulos, J., A. Borgida, M. Jarke, and Koubarakis. "Telos: Representing Knowledgea bout Information System," *ACM Transactions on Information Systems*, 8:4, pp. 325-326, October 1990.
[11] Biskup, J. "A General Framework for Data-baseSecurity," *European Symposium on Research in Computer Security*, ESORICS, Toulouse, France, 2004.
[12] Clark, D.D. and D.R. Wilson. "A Comparisionof Commercial and Military ComputerSecurity Policies," *Proceedings of the IEEESymposium on Security and Privacy*, pp. 184-194, 2000.
[13] Mahling, D.E., B.G. Coury, and W.B. Croft. "User Models in Cooperative Task-oriented-Environments," *Proceedings of the 23rd Annual Hawaii iEEE International Conferenceon System Sciences*, pp. 94-99, 1990.
[14] Steels, L. "Components of Expertise," *AI-Magazine*, pp. 28-49, Summer 1990.



이 명 희

- 1982년 홍익대학교 전자공학과 학사
- 1988년 홍익대학교 전자공학과 석사
- 2005년~서울벤처정보대학원대학교 정보경영학과 (박사과정 재학 중)
- 1985년~2001년 한국전력공사(영광원자력, 태안화력, 기술개발처, 내자처, 감사실, 연료처, 계통운영처)
- 2001년~현재 한국전력거래소 정보기술처 KEMS개발실 부장
- 주관심분야 : 유비쿼터스 기술, 컴퓨터 보안, 전력IT

유 재 언

- 1986년 고려대학교 경영대학 무역학과 졸업
- 1988년 영국 헐대학교 경영대학 경영시스템학과 석사
- 2001년 영국 링컨대학교 경영대학 경영학과 박사 (시스템이론 전공)
- 2001년 국제 시스템과학 학회 (ISSS) Applied Systems & Development 분과 부회장 (Deputy Chair)
- 2004년 서울벤처정보대학원대학교 정보경영학과 교수