그리드에서 SPKI 인증서를 이용한 권한 위임에 관한 연구

이성현* · 이재승* · 문기영* · 이재광**

A Study on Delegation used SPKI Certificate in Grid

Seoung-Hyeon Lee* · Jae-Seung Lee* · Ki-Young Moon* · Jae-Kwang Lee**

요 약

그리드에서 인증과 위임 서비스를 제공하기 위해서 일반적으로 이용하고 있는 것이 X.509 인증서이다. 인증 서비스는 X.509 사용자 인증서를 이용하여 제공하고, 위임 서비스는 X.509 프록시 인증서를 이용하여 제공한다. 하지만, X.509 프록시 인증서를 이용한 위임 서비스는 제한 위임과 다중 위임과 같은 그리드 보안 요구사항을 충분히 수용할 수 없으며, 검증을 위한 인증서 신뢰 체인의 형성과 같은 오버헤드를 가질 수 있다. 본 논문에서는 기존 X.509 프록시 인증서를 이용한 위임 서비스가 지원하지 못했던 제한 위임 및 다중 위임을 지원하기 위하여 SPKI 인증서를 이용한 경량화 된 위임 방법을 제안하고, 이에 대한 그리드 적용의 이점을 제시하였다.

ABSTRACT

It is X.509 certificate that use to offer authentication and delegation service in grid. Authentication service offers by X.509 user certificate, and delegation service offers by X.509 proxy certificate. However, in case of provide delegation service using X.509 proxy certificate, can not fulfill complicated delegation requirement of grid. In this paper, proposed delegation mechanism that is done restricted delegation, multiple delegation and light weight that delegation service that use existent X.509 proxy certificate does not have. In this paper, delegation service that proposed used SPKI certificate.

키워드

그리드 보안, 프록시 인증서, SPKI 인증서, 위임 서비스

Ⅰ. 서 론

그리드 컴퓨팅 환경(grid computing environ- ment; 이하 그리드라 칭함)은 1990년대 미국 시카고 대학의 이안 포스터 교수에 의해 제안된 가상의 슈퍼컴퓨터를 개발 연구로부터 시작되었으며, IT 기반의 응용과학(e-science) 및 전자거래(e-commerce), 슈퍼컴퓨팅 등의 다양한 기술에 기반 기술로 적용되고 있다[1][2]. 하지만 그리드가 가지는 엄청난 효과에도 불구하고 일반적인 응용으로의 그리드 확산은 더디게 진행되는데, 이에 대한 문제점으로 꼽히는 것 중의 하나가 보안 문제이다. 그리드에서 제공하는 보안 서비스는 현존하는 다양한 보안 메커니즘을 그리드에 적합하도록 수정하고, 메커니즘간의 결합을 통해서 제공하게 된다. 하지만 그리드는 다음과 같은 보안 문제를 가지고 있다. 첫째, 보안 메커니즘의 수정과 결합으로 인하여 그리드에 기반을 두는 보안 문제

* 한국전자통신연구원 바이오인식기술연구팀
** 한남대학교 컴퓨터공학과

접수일자 : 2006. 8. 8

뿐만 아니라, 보안 메커니즘들이 자체적으로 가지고 있는 보안 문제를 함께 가질 수 있다. 둘째, 그리드는 기존의 분산시스템에 비해서 복잡한 보안 취약 구조를 가지게 되는데, 이를 고려한 새로운 보안 메커니즘을 제시하지 못하고 있으며, 모든 보안 문제를 해결할 수 있는 통합된 보안 메커니즘이 제시되지 않았다. 이와 같은 보안 문제의 미해결은 그리드 확산에 큰 걸림돌로 작용하고 있기 때문에, 그리드를 구성하는 다양한 시스템 자원, 프로토콜과 응용 프로그램 등과 관계없이 그리드가 요구하는 보안 서비스를 충족시킬 수 있는 보안 프레임워크의 정립이 요구된다.

본 논문에서는 그리드에서 제공하는 보안 서비스 중에서 위임(delegation) 서비스에 대한 연구를 수행하였으며, 다음과 같이 구성되었다. 2장에서는 그리드에서 제공하는 위임 서비스 개요 및 동작 과정을 살펴보고, 본 논문에서 적용하게 되는 SPKI(Simple Public Key Infrastructure) 인증서에 대한 개념을 살펴본다. 3장에서는 기존 위임 방법이 가지고 있는 문제점을 지적한 후, 이를 해결하기 위해 제안된 SPKI 인증서를 이용한 위임 방법에 대해서 설명하고, 4장에서 제안한 방법의 타당성을 입증한다. 마지막으로 5장에서 결론을 맺고, 향후 연구 방향을 제시한다.

II. 관련 연구

2.1. 그리드에서의 위임 개요

위임이란 분산 환경에서 사용자가 가진 권한을 시스템에게 전달하여, 사용자 요청 작업에 대한 수행 중 발생하는 외부 자원의 접근을 허락하는 과정이다. 분산 환경에서는, 요청 작업을 수행하기 위해서 필요한 자원이 사용자가 로그인 한 시스템에 있는 경우가 드물기 때문에 위임이 자주 발생한다. 특히, 그리드의 경우 사용자 요청 작업의 수행은 서로 다른 시스템의 유휴 자원을 묶어 하나의 작업 환경처럼 제공받기 때문에, 요청 작업의 수행을 위해서는 프로세스에 의한 위임이 각 시스템 사이에서 빈번하게 발생하게 된다. 그림 1은 그리드에서 프로세스가 획득한 권한을 다른 자원 사이트의 프로세스에게 위임하는 과정을 도식화한 것이다.

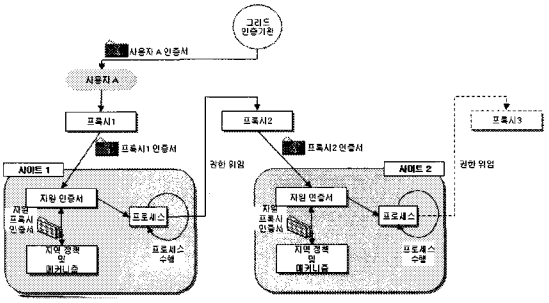

그림 1. 프로세스간 위임 과정
Fig. 1. The delegation process between process in grid

2.2 기존의 그리드 위임 방법

기존의 그리드 위임 방법에서는 사용자가 인증(authentication)/인가(authorization) 과정에서 획득한 권한을 위임하기 위해서 X.509 프록시 인증서(X.509 proxy certificate)를 이용한다.

X.509 프록시 인증서에 의한 위임은 새로운 공개키 쌍을 생성하고, 생성된 공개키에 대한 인증서(사용자 인증서와 동일하거나, 일부 수정된 인증서)를 발행하고, 사용자가 처음으로 접근한 자원 사이트의 프록시에 의한 서명으로 이루어진다.

그리드에서 사용자가 요청한 작업에 대한 수행 시 다른 자원 사이트로의 위임이 요구되는 동안 이전 사이트에서 생성한 프록시 인증서를 이용한 새로운 프록시 인증서의 발행과 이에 대한 서명이 계속되고, 신뢰 관계는 이들 프록시 인증서 체인(proxy certificate chain)에 의해서 결정된다[3][4][5][6]. 그림 2는 프록시 인증서를 이용한 기존의 그리드 위임 방법을 도식화한 것이다.

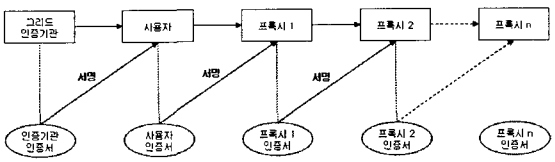

그림 2. 프록시 인증서 재발행을 통한 위임 방법
Fig. 2. The delegation method using proxy certificate reissue

2.3 SPKI 인증서

SPKI는 Non-X.509 인증 방법을 대표하는 프로토콜로, X.509 인증서가 익명성을 제공하지 못하며, 관리가 복잡하다는 문제점을 개선하기 위해서 최소한의 정보로 구성된 인증서를 만드는 것을 목표로 제안되었다.

SPKI는 PGP와 같이 개인 사용자 간에 인증을 해주는 방법을 사용함으로써, X.509에 비해서 간단한 구조를 가지고 있으며, 인증서를 ID가 아닌 공개키와 바인딩(binding)하기 때문에 익명성을 유지할 수 있다. 또한, 인증서 내에 권한 부여 정보를 추가할 수 있는 방법을 제공하고 있어, 인터넷 상에서의 접근 제어에 효과적으로 사용할 수 있다. 이와 같은 특징을 가지고 있기 때문에 SPKI 인증서는 다른 말로 '권한 인증서(authorization certificate)'라고도 부른다[7][8][9].

이와 같은 특징을 가지고 있는 SPKI 인증서를 사용한 위임 방법은 다음과 같은 장점을 가진다[8, 9].

첫째, SPKI 인증서는 서버가 발행한 인증서를 사용자가 소유하고 있다가 위임 요구가 발생할 경우 발급받은 SPKI 인증서를 제출하고, 권한의 위임은 서버가 지정한 규칙에 따라 제한적으로 이루어진다. 둘째, SPKI 인증서의 발급 시 사용자 ID(또는 SubjectDN)가 아닌 공개키나 공개키의 해시값을 사용하여 발행자와 소유자를 표시하기 때문에 사용자에 대한 익명성을 유지할 수 있다. 셋째, SPKI 인증서의 수정 없이 발급 받은 인증서를 다른 사용자에게 쉽게 위임할 수 있다. 넷째, 특정 서비스에 대해 독립적이며, SPKI 인증서 발행과 관리가 용이하므로 유지/보수 가격이 저렴하다.

Ⅲ. 위임 방법 제안

3.1 기존 방법의 문제점

프록시 인증서의 재발행을 이용한 기존의 위임 방법은 단순하고 일반적인 방법이며, 사용자 신원과 권한을 그리드 자원 사이트에 변경 없이 전달할 수 있다는 장점을 가지고 있지만, 다음과 같은 문제점을 가지고 있다.

첫째, 프록시 인증서에 대한 신뢰는 계층적인 CA 구조와 동일하게 계층적 인증서 체인을 가지게 되며, 위임이 지속될수록 신뢰된 인증서 체인이 길어지고 복잡하게 된다. 이에 따라 신뢰 검증의 어려움이 발생하고, 지속적인 위임이 어렵다. 둘째, 프록시 인증서의 재발행은 사용자 신원과 권한을 변경 없이 전달하며, 위임된 사이트에서 권한을 받기 위한 계정이 요구된다. 따라서 모든 위임 가능한 사이트는 동일한 계정과 접근 권한 정보가 정의되어야 한다. 셋째, 프록시 인증서에 제한 위임을 위한 권한 정보 등을 포함하는 경우 인증서의 확장필드에 포함되는 데이터 구성이 복잡해지고, 이를 처리하기 위한 별도의 방안이 마련되어야 한다.

위와 같은 문제점을 해결하기 위해 본 논문에서는 SPKI 인증서를 이용한 그리드 위임 방법을 제안한다.

3.2 SPKI 인증서를 이용한 위임 방법

3.2.1 SPKI 인증서를 이용한 위임 개요

SPKI 인증서를 이용한 위임 방법은 그림 3과 같이 구성된다.

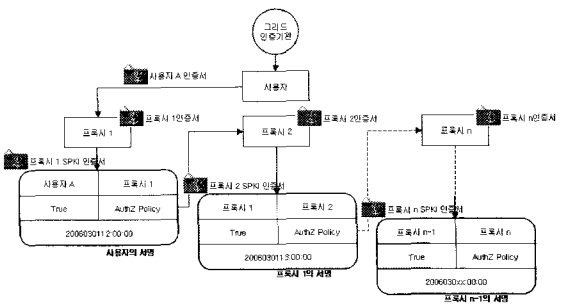

그림 3. SPKI 인증서를 이용한 권한 위임 과정
Fig. 3. The delegation process using SPKI certificate

그림 3에서 AuthZ Policy는 사용자가 프록시에 접근할 때 게이트키퍼(gatekeeper)를 통해 부여 받은 접근 권한에 대한 정책이다. 본 논문에서 그리드를 구성하는 모든 프록시는 SPKI 인증서를 발행할 수 있다고 가정한다. 실제, 그리드를 구성하는 프록시들은 OpenSSL을 이용한 공개키 쌍의 생성과 인증서 발행을 지원한다. 제안 방법에서 사용되는 SPKI 인증서의 유효 기간은 사용자가 자원에 접속하여 프로세스를 수행하는 동안으로 제한하고, 다시 접근할 경우 재발행 받는 것으로 한다. 또한, 위임이 지속됨에 따라 길어진 신뢰 체인은 5단계가 넘어갈 경우, 정리(reduction) 절차를 거쳐, 위임을 종료하고 Proxy 1에 의해서 새롭게 생성한 SPKI 인증서를 발행 받는다.

3.2.2 제안된 위임 방법의 SPKI 인증서 발행

본 논문에서 제안된 위임 방법의 SPKI 인증서 발행 절차는 표 1과 같은 표기법을 사용하며, 모든 프록시는 그리드 CA로부터 인증서를 발행 받았다고 가정한다.

표 1. SPKI 인증서의 표기법
Table 1. SPKI certificate notation

표기	설명
proxy	SPKI 인증서를 발행하고, 사이트 자원에 대한 접근을 관리
id	proxy의 식별자
Sig_p	서명값
U_{pub}, U_{pri}	사용자 공개키 및 개인키
$P(id)_{pub}$, $P(id)_{pri}$	프록시(id) 공개키 및 개인키
True, False	위임 여부
$AuthZ_p$	위임할 권한
Val_{Date}	SPKI 인증서 유효 기간

① 사용자 -> 프록시 1

사용자가 로그인을 거쳐, 프록시 1에게 SPKI 인증서를 발행하는 단계로, 초기 SPKI 인증서는 다음과 같이 발행된다.

$<U_{pub}, P_{pub}, True, AuthZ_P, Val_{Date}>U_{pri}$

② 프록시 1 -> 프록시 2

사이트 1에서 프로세스를 수행 중에 발생하는 1차 위임으로 프록시 2에게 SPKI 인증서를 발행하는 단계이다.

$<P1_{pub}, P2_{pub}, True, AuthZ_P, Val_{Date}>P1_{pri}$

③ 위임이 5단계 이상 진행 후

위임이 5 단계 이상 진행되면, 프록시 1로부터 새로운 SPKI 인증서를 발행받는 reduction을 수행한다.

$<U_{pub}, P4_{pub}, True, AuthZ_P, Val_{Date}>U_{pri}$

제안 방법에서 프로세스를 수행하기 위해서 권한을 위임받는 모든 프록시들은 위와 같은 단계를 거치면서 SPKI 인증서를 발행하고, 정의된 인가 정책에 의해서 정의된 접근 권한을 부여 받는다.

3.2.3 SPKI 인증서의 구성

SPKI 인증서는 위임 여부만 지정하고, 권한을 포함할 수 없는 4-tuple SPKI 인증서와 위임 권한(동등 또는 제한)을 지정할 5-tuple SPKI 인증서가 있다. 본 논문에서 제안된 위임 방법은 그림 4와 같은 5-tuple 인증서를 이용한다.

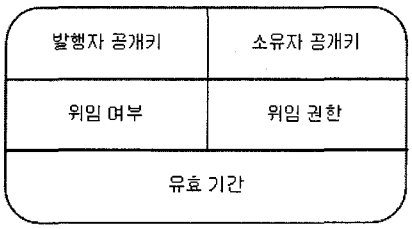

그림 4. SPKI 인증서 형식(5-tuple)
Fig. 4. SPKI certficate format(5-tuple)

- 발행자 공개키(issuer public key): SPKI 인증서를 발행하는 프록시의 공개키 또는 공개키 해시값
- 소유자 공개키(subject pubic key): SPKI 인증서를 발행받는 프로세스의 공개키 또는 공개키 해시값
- 위임 여부(delegation): 프로세스에 대한 인증서 원 소유자의 위임 여부로 True/False로 표현. True로 설정될 경우 권한을 위임할 수 있으며, 프로세스는 이에 대한 재위임이 가능. 단 위임되는 권한은 동일한 권한이거나 적은 권한
- 위임 권한(authorization): 프로세스를 생성한 사용자가 'user role level' 등의 위임 정책을 통해서 부여받은 정책 값으로, 실제 소유할 수 있는 권한을 지정
- 유효기간(validity): SPKI 인증서의 유효 기간으로 보안 대응을 위해서 프로세스의 생명주기로 지정

3.2.4 위임 동작 과정

본 논문에서는 제안한 SPKI 인증서를 이용한 위임 방법의 동작 과정은 그림 5와 같다.

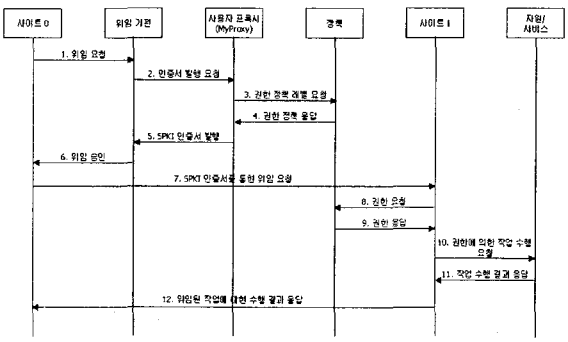

그림 5. 제안한 위임 방법의 동작 과정
Fig. 5. The operation process of delegation method to be proposed

제안하는 위임 방법은 SPKI 인증서와 SPKI 인증서 체인을 통해서 이루어진다. SPKI 인증서는 다음 프로세스에 대한 위임 여부를 결정하는 필드와 위임되는 권한을 표시하는 필드로 구성되는 5-tuple SPKI 인증서를 이용한다. SPKI 인증서를 이용한 위임에서 인증서의 신뢰 경로는 '5' 단계까지로 제한하며, 이후의 위임에 대해서는 인증서 reduction을 통해서 사용자 인증서로부터 새로운 SPKI 인증서를 생성할 수 있도록 한다. '위임 권한'에 기술되는 권한은 사용자 인증 및 인가 절차에서 RBAC을 이용하여 결정된 권한을 표시하며, 경우에 따라서는 부여 받은 권한을 축소 또는 확대한 새로운 권한을 소유할 수 있다. 이에 대한 절차는 인가와 동일하다.

Ⅳ. SPKI 인증서를 이용한 위임 능력 분석

SPKI 인증서를 이용한 위임 방법은 다음과 같은 이점을 가지기 때문에 그리드 위임 서비스를 제공하기에 적합한 방법이다.

- 인증서 발행의 분산화: SPKI 인증서는 그리드 CA의 제한을 받지 않고 MyProxy 또는 위임 모듈에서 자유로이 생성할 수 있다. 이는 그리드에서 자원 및 사용자 구성과 자원 사이트간의 프로세스 생성 및 권한 위임을 자유롭게 한다.
- 인가된 권한의 위임: 사용자 인증 및 인가 과정을 통해서 획득한 권한을 위임할 수 있음으로써, 그리드를 훨씬 유연하게 만든다. 이 경우, SPKI 인증서의 신뢰 경로는 자원 사이트의 신뢰를 형성한다.
- 유연한 권한: 인가와 권한은 자유롭게 정의될 수 있으며, 미리 정의된 권한 집합에 제한되지 않는다.
- 검증: SPKI 인증서 발행자는 인증서의 유효 기간 또는 다른 상태를 지정할 수 있고, 이를 검증할 수 있다. 이것은 쉬운 접근 관리와 함께 위임을 위한 좀 더 세밀한 접근 제어를 제공하고, 잠재적인 위협을 최소화하기 위해서 사용될 수 있다.
- 이름에 의존하지 않는 바인딩: SPKI 인증서는 공개키에 바인딩 하기 때문에, 익명성을 확보하고 프라이버시에 더 좋은 보호를 제공한다[10].

위와 같은 이점은 SPKI 인증서가 ID/PW를 기반으로 하는 ACL과 X.509 프록시 인증서를 통한 위임을 대체하는 강력한 수단으로 활용될 수 있음을 증명할 수 있다. ACL 데이터베이스와 달리 인증서는 어떠한 암호화 없이도 공표될 수 있다[11].

특히, 그리드와 같은 대규모 분산 시스템에서 권한 위임과 관련하여 긴 인증서 체인을 형성할 지도 모르는 것에서는 기존의 X.509 프록시 인증서 체인을 통한 신뢰 경로의 형성 보다는 SPKI 인증서를 이용하는 것이 바람직하며, 각 시스템의 일부에 이의 발행을 위한 모듈을 가지고 있는 것이 바람직하다.

본 논문에서 제안한 SPKI 인증서를 이용한 위임 방법은 기존 방법과 비교하여 표 2와 같은 특징을 가진다.

표 2와 같이 제안된 위임 방법은 기존 위임 방법과 비교해 많은 장점을 가지고 있으며, 실제 그리드를 구축하기 위해 이용되는 미들웨어인 글로버스 툴킷(globus toolkit)에서 제공하는 위임 방법과 비교하여 다음과 같은 추가기능을 가진다.

표 2. 기존 위임 방법과의 비교
Table 2. Comparison with exist delegation method

비교 기준	X.509 프록시 인증서	ID/PW	제안된 방법
위임 토큰	X.509 프록시 인증서	ID	SPKI 인증서
위임 방법	인증서 체인	ID 건네기	인증서 발행
다중 권한 위임	지원하지 않음 (인증서 형식 재정의 후 일부 가능)	지원하지 않음	인증서 발행 목적 및 위임 대상 권한에 따라 자유로이 설정 가능
부분 권한 위임	지원하지 않음 (인증서 형식 재정의 후 일부 가능)	지원하지 않음	인증서 발생 목적 및 위임 대상 권한에 따라 자유로이 설정 가능
위임 거부	지원하지 않음 (인증서 형식 재정의 후 일부 가능)	지원하지 않음	SPKI 인증서의 필드에서 정의 가능
위임 검증	인증서 체인의 신뢰 경로 검증	Password 검증	인증서 유효성 검증 (유효기간 및 상태)
위임 대상	MyProxy 및 프로세스	사용자	MyProxy 및 프로세스

첫째, 위임 시 단일 위임뿐만 다중 위임 기능을 제공한다. 즉, 위임자에게 위임 받은 권한을 자신이 수행하거나 또는 위임자가 허용한다면 권한을 위임받은 피 위임자가 다시 위임받는 권한을 제 3자에게 위임할 수 있다. 둘째, 위임 받은 모든 권한이 아닌 권한의 부분 집합을 위임할 수 있도록 하여 과도한 권한이 위임되는 것을 막을 수 있다. 셋째, 위임 받은 권한을 제 3자가 수행하고, 이에 대한 권한을 다른 피 위임자에게 위임하지 않을 수 있다. X.509 프록시 인증서를 이용한 방법에서 이에 대한 것은 인증서의 신뢰 경로를 형성하지 않는 것이지만, SPKI 인증서를 이용한 방법에서는 신뢰 경로를 형성(즉, SPKI 인증서의 발행)하고도 위임 권한을 주지 않을 수 있다.

V. 결 론

본 논문에서는 프록시 인증서를 이용한 기존 위임 방법을 개선하기 위해 SPKI 인증서를 이용한 위임 방법을 제안하고, 기존 위임 방법과의 비교 분석을 통하여 그리드 적용에 대한 우수성을 입증하였다.

본 논문에서 제안된 위임 방법은 MyProxy와 SPKI 인증서를 이용하여 기존의 위임 방법을 대체하기 위한 것이다. 제안된 위임 방법은 기존의위임 방법과 비교하여 복잡한 권한 부여 절차를 간소화하고, SPKI 인증서의 reduction을 통해 신뢰 체인의 재배치를 통해 신뢰 검증 오버헤드를 최소화하였다. 또한, 위임되는 권한의 범위와 위임 여부를 결정할 수 있음으로서, 제한 및 다중 위임 도입의 가능성을 검토하였다.

향후, 본 논문에서 제안된 그리드 위임 프레임워크를 기반으로 그리드에서의 안전한 보안 서비스를 제공하기 위한 방안에 대해 연구를 진행하며, 웹서비스 기반의 그리드 보안 프레임워크 구성을 위한 연구의 기초로 활용한다.

참고문헌

[1] 허의남, "글로벌 신경망, 그리드(GRID) 기술", 오라클 매거진, 2004

[2] 윤훈주, "유비쿼터스와 그리드컴퓨팅", 유비유넷 리포트, 제2호, 2006년 2월

[3] http://www.globus.org/toolkit/security/

[4] The Economic Impact of Role Based Access Control. Research Triangle Institute. NIST Planning Report 02-01. 2002.

[5] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, "Proposed NIST Standard for RoleBased Access Control", ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001.

[6] Ferraiolo D., Kuhn R., "Role-based access control", In Proceedings of the NIST-NSA National(USA) Computer Security Conference, 1992.

[7] C. Ellison외 5명, "SPKI Certificate Theory. Request for Comments", RBC 2693, September 1999.

[8] 신정화외 2명, "P2P 환경에서 SPKI 인증서를 이용한 접근 제어", 정보처리학회 논문지 C, 제10-C권, 제6호, 2003년 10월

[9] 이영록외 4명, "역할기반 접근제어 및 비밀통신을 지원하는 SPKI/SDSI HTTP 보안 서버", 정보보호학회 논문지, 제12권, 제6호, 2002년 12월

[10] Li Gong, and R. Schemers, "Implementing Protection Domains in the Java Development Kit 1.2", Proc. of the Network and Distributed System Security Symposium, Internet Society, 1998

[11] EGEE, "Gobal Security Architecture", EGEE Standard, 2004

저자소개

이 성 현(Seoung-Hyeon Lee)

2003년 한남대학교 컴퓨터공학 (공학석사)
2006년 한남대학교 컴퓨터공학 (공학박사)
2006년~ 한국전자통신연구원 바이오인식기술연구팀 Post-Doc
※관심분야 : 웹서비스 및 그리드 정보보호

이 재 승(Jae-Seung Lee)

1997년 포항공과대학교 정보통신학 (공학석사)
1997년~1999년 데이콤 정보통신 연구소 연구원
1999년~ 한국전자통신연구원 과제책임자/선임연구원
※관심분야 : 웹서비스 및 유비쿼터스 정보보호

문 기 영(Ki-Young Moon)

1986년 경북대학교 전산학 (이학석사)
2004년 충남대학교 전산학 (공학박사)
1994년~2001년 한국전자통신연구원 선임연구원
2001년~ 한국전자통신연구원 팀장
※관심분야 : 웹서비스 정보보호, 생체정보 인식

이 재 광(Jae-Kwang Lee)

1986년 광운대학교 전자계산학 (이학석사)
1993년 광운대학교 전자계산학 (이학박사)
1993년~ 한남대학교 컴퓨터공학 교수
※관심분야 : 네트워크 및 웹서비스 정보보호, 그리드