ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

OAuth 기반의 대리 인증서 위임 서비스

OAuth based Proxy Delegation Service

허 대 영[1] 황 선 태[1*]
Daeyoung Heo Suntae Hwang

요 약

그리드 환경에서 그리드 서비스를 웹 인터페이스 및 웹 서비스로 제공하기 위해 웹 표준 기술에 기반을 둔 그리드-웹 애플리케이션이 증가하고 있다. 그러나 웹 표준 보안 구조에서 위임 인증 방법의 부재로 웹 애플리케이션에 그리드 보안 시스템 GSI를 통합하는 것은 매우 어렵다. 이를 해결하기 위해서는 온라인 자격증명 저장 서비스를 이용하여 웹 애플리케이션에서 그리드 자격증명을 사용할 수 있도록 해야 한다. 본 논문에서는 그리드-웹 애플리케이션과 사용자 간의 상호 신뢰를 전제로 하는 온라인 자격증명 저장 서비스인 MyProxy를 사용하는 방법의 문제점을 분석하고, 상호 신뢰를 바탕으로 하지 않는 그리드 자격증명 위임 서비스를 제안한다. 이 서비스의 자격증명 교환 프로토콜은 OAuth에 X.509 인증 위임 절차를 추가한 것이다. 이 위임 서비스는 그리드-웹 애플리케이션에게 단일 로그온을 제공하고, 하나 이상의 그리드 자격증명을 위임하고 획득할 수 있는 보안 방법을 제공한다.

☞ 주제어 : X.509 위임 인증, 그리드 보안, 공개인증

ABSTRACT

Grid web applications by standard Web technology are increasingly used to provide grid service to users as normal Web user interface and service. It is however difficult to integrate a grid security system such as Grid Security Infrastructure (GSI) into Web applications because the delegation way of standard Web security is not the same as the one of Grid security. This can be solved by allowing Web applications to get a Grid credential by using an online credential repository system such as MyProxy. In this paper, we investigate the problem that occurs when MyProxy, which assumes mutual trust between a user and Grid web application, is adapted for achieving security integration between Web and Grid, and we propose a new Grid proxy delegation service to delegate a Grid credential to the Web without assuming mutual trust. In the service, the X.509 proxy delegation process is added to OAuth protocol for credential exchange, and authentication can be done by an external service such as OpenID. So, users can login onto the Grid web application in a single sign-on manner, and are allowed to securely delegate and retrieve multiple credentials for one or more Virtual Organizations.

☞ keyword : X.509 Proxy Delegation, Grid Security, OAuth

1. 서 론

인터넷의 성장과 인터넷 기술의 발달로 일반 웹 브라우저에서 멀티미디어나 엔터테인먼트 같은 복잡한 기능들을 처리할 수 있게 되었다. 이에 따라, 그리드 애플리케이션을 일반 웹 브라우저를 통해 사용할 수 있도록 하는 웹 애플리케이션과 그리드[1] 애플리케이션을 통합한 그리드-웹 애플리케이션이 증가하고 있다.

대부분의 그리드-웹 애플리케이션은 사용자가 서버에 사용자 대신 활동할 수 있는 권한을 위임하는 것이 필요하다. 그러나 웹 표준 보안과 그리드 보안에서 위임 방법이 서로 다르기 때문에 웹 애플리케이션에 그리드 보안 시스템 GSI[2]를 통합하는 것은 매우 어렵다.

본 논문에서는 사용자와 그리드-웹 애플리케이션에서 상호 신뢰를 배제한 환경에서 그리드 자격증명을 웹에 위임하는 새로운 온라인 자격증명 저장 서비스의 설계와 구현에 대해서 설명한다.

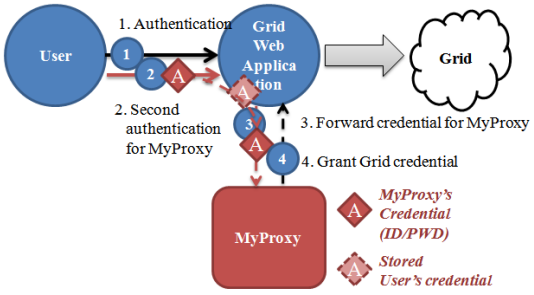
2. 웹 애플리케이션과 그리드의 통합 문제

이 장에서는 MyProxy[3,4]를 사용하여 그리드와 웹 애플리케이션의 통합에서 발생하는 문제점을 설명하고, 이를 해결할 수 있는 새로운 보안 모델을 제시한다.

1 Department of Computer Science, Kookmin University, 136-702, Korea
* Corresponding author (sthwang@cs.kookmin.ac.kr)
[Received 27 April 2012, Reviewed 9 May 2012(R2 16 August), Accepted 18 October 2012]
☆ 본 연구는 2011년 국민대학교 연구비지원으로 이루어졌습니다.

2.1 MyProxy의 한계

MyProxy는 사용자와 그리드-웹 애플리케이션간의 상호신뢰를 전제로 한다. 상호신뢰를 배제할 경우, MyProxy를 사용한 통합은 두 가지 문제점이 있다. 첫 번째, MyProxy와 웹 애플리케이션은 독립적인 인증 시스템을 가지고 있기 때문에 사용자는 웹 애플리케이션과 MyProxy로 2회 인증을 수행해야 한다. 뿐만 아니라, (그림 1)에서 보는 것과 같이 그리드-웹 애플리케이션이 MyProxy에서 직접 사용자의 그리드 자격증명을 획득해야 하기 때문에 사용자의 자격증명 정보(사용자 이름 및 비밀번호)가 그리드-웹 애플리케이션에 저장될 수 있다.



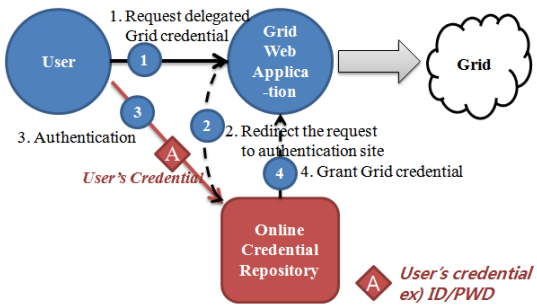
(Figure 1) Getting Grid credential from MyProxy via Web application

MyProxy의 두 번째 문제점은 한 사용자에게 하나의 그리드 자격증명만 위임할 수 있다. 그리드 컴퓨팅에서 자원 공유 협의체인 가상 조직이 다수 존재할 수 있다. 각 그리드 가상 조직은 독립적인 그리드 자격증명을 사용한다. 따라서 사용자는 다수의 가상 조직에 속하여 하나 이상의 그리드 자격증명을 가질 수 있다. MyProxy를 이용하는 그리드-웹 애플리케이션은 사용자가 특정 그리드 가상조직에 종속하도록 제약한다.

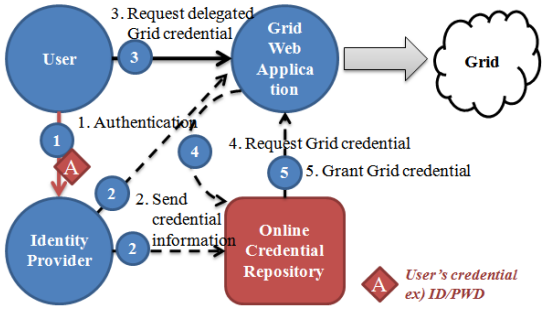
2.2 보안 모델의 개선

MyProxy의사용자 자격증명 정보가 웹 애플리케이션에 저장되지 않게 하려면, (그림 2)와 같이 사용자가 온라인 자격증명 저장소 서비스에 직접 인증을 수행해야 한다.

그러나 여전히 사용자는 그리드-웹 애플리케이션과 온라인 자격증명 저장 서비스에 각각 인증해야 한다. 즉, 사용자는 2회의 인증을 해야 한다. 이를 해결하기 위해서



(Figure 2) Direct to online credential repository



(Figure 3) Using external authentication

는 (그림 3)과 같이 별도의 신원 확인 서비스를 두는 방법으로 해결할 수 있다.

MyProxy는 사용자 이름에 단 하나의 그리드 자격증명서를 사상하도록 설계되어있다. 다수의 가상조직을 지원하도록 하기 위해서는 식별된 사용자와 위임된 대리 인증서를 1:n 관계로 사상하여 해결할 수 있다.

단, 대리 인증서가 다수의 사용자에 속하는 것은 다수의 사용자가 하나의 인증서를 공유하는 형태로 PKI 환경에서 허용하지 않는다. 따라서 사용자는 다수의 대리 인증서와 1:n 관계를 갖고, 다수의 대리 인증서는 사용자와 1:1 관계를 가져야 한다.

3. 대리 인증서 위임 서비스의 제안

이 장에서는 2장에서 언급한 보안 모델에 따라 설계하고 개발한 서비스에 대해 설명한다. 이 서비스의 중요한 특징은 다음과 같다.

- 단일 로그온: 사용자는 여러 번 인증 할 필요 없이 한 번의 인증으로 여러 자원을 사용할 수 있어야 한다.

- 인증 위임: 사용자는 중간 서비스가 사용자를 대신할 수 있도록 인증을 위임할 수 있어야 한다.
- 다중 가상 조직: 사용자는 하나의 계정으로 여러 개의 자격증명을 사용할 수 있어야 한다.
- 유연성 및 확장성: 인증 시스템은 기존 방식의 시스템을 적용하거나 다른 사용자 식별 방식을 쉽게 적용할 수 있어야 한다.
- 인증 중계 방지: 사용자의 인증 정보가 중간 서비스에게 위임 절차 없이 중계되는 것은 금지해야 한다.
- 추적성(traceability): 사용자는 위임된 인증이 사용되는 것을 추적할 수 있어야 한다.

3.1 인증

위임 서비스에서 인증은 두 가지 목표를 갖는다. 첫 번째, 그리드-웹 애플리케이션에게 단일 로그온을 지원하는 것이다. 위임 서비스를 이용하여 그리드 보안을 통합하는 여러 그리드-웹 애플리케이션들이 위임 서비스를 중심으로 통합할 수 있도록 한다. 단일 로그온을 지원하기 위해서 위임 서비스에서 인증은 외부 사용자 신원 공급자와 연동할 수 있다. 외부 사용자 신원 공급자는 OpenSSO[5], OpenID[6]와 같은 웹 기반 인증을 지원해야 한다.

두 번째, 위임 서비스의 저장소에 저장되어 있는 그리드 자격증명을 그리드-웹 애플리케이션이 사용할 수 있도록 허가하는 것이다. 그리드-웹 애플리케이션이 사용자의 그리드 자격증명을 사용할 수 있게 허가하는 것은 사용자의 책임이다.

3.2 자격증명(Credential) 관리

위임 서비스는 사용자로부터 그리드 자격증명을 위임받아서 사용자가 허가한 그리드-웹 애플리케이션에 그리드 자격증명을 위임해야 하는 서비스를 제공한다. 따라서 위임 서비스는 위임 받은 그리드 자격증명을 안전하게 관리해야 하는 책임이 있다.

위임 서비스에서 그리드 자격증명을 관리하기 위해서 그리드 자격증명이 갖는 요소를 이용한다. 그리드 자격증명은 PKI 환경에 기반하고 있다. 따라서, PKI 기반의 위임된 그리드 자격증명은 다음과 같은 요소를 갖는다.

- 인증서 고유 이름: 모든 인증서는 디렉토리 시스템에서 사용하는 고유 식별자와 같은 방식의 이름을 가진다.
- 인증서 만료 시간: 인증서는 발급자가 인증서 효력을 보장하는 유효 시간이 있다. 유효시간은 인증서 효력이 개시되는 시간과 만료되는 시간으로 표현한다.
- 인증서 사슬: PKI 시스템은 발급자가 발급하지 않은 인증서 이름을 사용하여 위조하는 등의 인증서 위조 방지를 위한 체계를 가진다.
- 다중 그리드 자격증명을 지원하기 위해서 그리드 자격증명을 고유 이름과 인증된 사용자 신원과 연관하여 저장소에 저장한다. 사용자가 고유 이름이 같은 그리드 자격증명을 다시 위임하는 경우, 저장소에서 기존의 그리드 자격증명을 폐기하고 새로운 그리드 자격증명을 저장한다. 저장된 그리드 자격증명은 만료 시간을 주기적으로 검사하여 자동적으로 저장소에서 제거된다.

마지막으로 그리드 자격증명이 가지는 인증서 사슬은 그리드 자격증명의 유효성을 검증하는 데 사용한다. 그리드 자격증명의 유효성은 3.3절에서 기술되는 정책에 따라서 검증된다.

3.3 정책

위임 서비스는 그리드 자격증명을 요청하는 웹 애플리케이션의 접속에 대한 제어와 위임된 그리드 자격증명의 유효성 보장에 대한 정책을 제공한다. 접속 제어 정책은 웹 애플리케이션이 사용자가 위임한 그리드 자격증명에 대한 접근을 제어하는 것이다. 만약 사용자가 허가하지 않는 경우, 위임 서비스는 해당 사용자의 그리드 자격증명에 대한 접근을 거절한다.

인증 유효성 보장은 PKI 기반의 그리드 자격증명을 위임 서비스에서 검증하여, 클라이언트에게 유효성을 보장하는 것이다. 위임 서비스는 인증의 유효성 보장에 대한 가능/불가에 대한 것과 보장을 해야 하는 경우 검증 정책을 수립할 수 있다.

인증서 사슬의 유효성 검증을 위해서 위임 서비스는 화이트 리스트와 블랙 리스트 방식의 발급 기관의 인증서를 관리 정책과 관리자와 사용자 수준의 감독을 나누어 정책을 수립한다.

- 화이트 리스트 정책: 이 정책은 화이트 리스트에 등록된 발급 기관의 인증서만 유효한 것으로 본다. 화이트 리스트에 등록되지 않은 발급 기관의 인증서는 인증서 사슬의 유효성과 관계없이 거절한다.

- 블랙 리스트 정책: 이 정책은 화이트 리스트와 반대로 블랙 리스트에 등록된 발급 기관의 인증서만 거절한다. 즉, 블랙 리스트에 없는 발급 기관의 인증서는 모두 유효한 것으로 보고 인증서 사슬 유효성을 검사한다.
- 검증 없음 정책: 이 정책은 인증서 사슬 유효성 검증을 위임 서비스에서 수행하지 않는 것이다.

관리자는 위임 서비스를 위의 3가지 방식 중 한가지로 운영할 수 있다. 각 기본 정책에 따라 사용자가 위임하는 인증서의 유효성을 검사한다.

사용자는 위임 서비스의 관리 정책 내에서 사용자 수준의 정책을 수립할 수 있다. 사용자 수준 정책은 화이트 리스트 사용자 수준 정책과 블랙 리스트 수준 정책 두 가지만 지원한다. 사용자 수준의 정책은 관리자가 수립한 정책의 범위 안에서 더욱 강하게 적용하기 위해서 사용된다. 즉, 화이트 리스트 정책일 경우, 관리자에 의해 인가된 발급 기관의 목록의 크기를 줄이기 위한 블랙 리스트 사용자 수준 정책을 지정할 수 있다. 반대로 블랙 리스트 정책일 경우에는 블랙 리스트에 포함되지 않은 모든 발급 기관 중에서 사용자가 허가할 화이트 리스트 사용자 수준 정책을 지정할 수 있다. 마지막으로 검증 없음 정책일 경우, 사용자는 사용자 수준 정책을 적용할 수 없다.

3.4 감사

위임 서비스는 서비스에서 발생하는 모든 보안 사건을 기록해야 한다. 따라서 사용자가 그리드 자격증명을 위임하거나, 그리드-웹 애플리케이션이 그리드 자격증명을 요청하는 것을 감지하고 기록할 수 있어야 한다. 기록된 감사 결과는 보안 정책이 명시된 접근 제어나 인증 정책을 준수하고 있는지 점검하는 데 사용될 수 있다.

본 논문에서 제안하는 위임 서비스는 다음과 같은 보안 사건을 다룬다.

- 사용자 인증: 사용자 신원 확인, 접근 시도한 Username, 사용자 IP, 사용 단말기 정보(웹 브라우저, 운영체제 등), 접근 시간 및 성공/실패 여부가 기록된다.
- OAuth 자원 접근: OAuth[7] 인증을 통한 접근. 토큰, 접근 IP, 접근 시간과 성공/실패 여부가 기록된다.
- 인증서 위임: 원본 인증서 고유 이름, 원본 인증서 만료 시간, 위임 만료 시간 및 위임 시간 및 위임 성공/실패 여부가 기록된다.
- 대리 인증서 발급: 원본 인증서 고유 이름, 원본 인증서 만료 시간, 대리 인증서 고유 번호, 대리 인증서 만료 시간, 발급 시간과 발급 성공/실패 여부가 기록된다.
- 인증서 유효성 감사: 인증서 유효성 감사는 인증서 위임 시에 발생한다. 3.3절에 설명한 정책에 따른 유효성 감사 결과와 감사 시간이 기록된다.

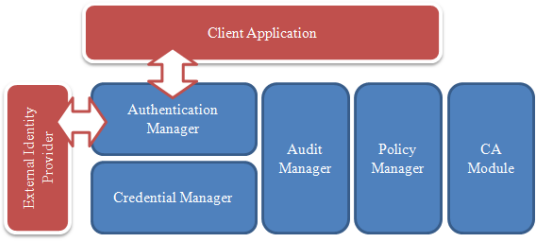
3.5 Certificate Authority (CA) 모듈

본 논문에서 제안하는 위임 서비스는 대리 인증서를 위해서 인증서 발급 기관(CA)의 일부 기능을 제공한다. 첫 번째 대리 인증서를 발급할 수 있는 기능을 가진다. 두 번째, 발급한 대리 인증서의 유효성을 검증할 수 있는 CRL (Certificate Revocation List)를 제공한다. CRL은 폐기된 인증서 목록으로, 인증서 유효성을 확인하는 타 서비스 혹은 애플리케이션이 사용한다. 위임 서비스는 사용자의 대리 인증서 단위의 별도의 CRL 배포 지점과 전체 인증서에 대한 CRL 배포 지점을 모두 제공하여 유효성을 검증하는 단말 서비스/애플리케이션에 호환성을 제공한다.

4. 구 현

4.1 주요 구성요소

위임 서비스는 (그림 4)에서 보여주는 것과 같이 5개의 컴포넌트 구성된다. 사용자인증(Authenti- cation) 관리자는 4.2절에서 설명하는 새로운 자격증명 교환 프로토콜을 사용하여 사용자 인증 및 그리드 자격증명의 위임을 수행한다. 인증(Credential) 관리자는 사용자 관리자를 통해서 OAuth 인증에 사용되는 애플리케이션 키와 접근 토큰을 관리한다. 또한 사용자가 위임한 그리드 자격증명인 대리 인증서를 암호화하여 저장한다. 인증 관리자는 위임 받은 대리 인증서가 만료되거나 폐기 되면 저장소에서 삭제하고 인증서 모듈(CA)를 사용하여 새로운 인증서 폐기 목록을 배포하는 일을 수행한다. 감사 관리자는 다른 모든 컴포넌트의 활동과 보안 감사와 관련된 사건이나 활동이 발생할 때 마다 기록될 수 있도록 모든 컴포넌트에서 호출된다. 정책 관리자는 그리드 자격증명 위임이나 획득과 같은 인증서와 관련된 행위를 수행하기 전에 감사를 수행한다.



(Figure 4) Software Architecture of proposed service

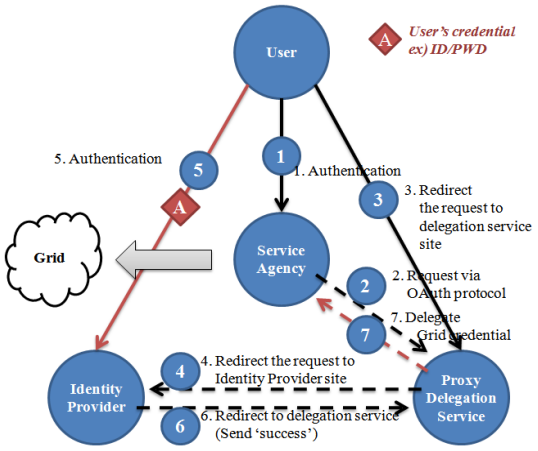
마지막으로 인증서 모듈(CA)은 그리드 자격증명을 위임할 때에, 대리 인증서를 서명하는 일과 사용자의 그리드 자격증명서의 유효성 검증, 발급한 대리 인증서의 유효성을 보장하기 위한 인증서 폐기 목록을 처리하는 기능을 제공한다.

4.2 자격증명 교환 프로토콜

2.1절에서 언급한 MyProxy를 이용한 그리드 자격증명 교환에서 사용자 신원 및 암호문이 제 3 자에게 저장될 수 있는 한계점을 본 논문에서 제안하는 인증 서비스는 극복해야 한다. 위임 서비스는 사용자 인증을 제 3 자 서비스에게 중간 인증 경유 없이 그리드 자격증명으로 교환할 수 있는 프로토콜이 필요하다. 그래서 제 3 자에게 접근 권한을 부여하는 OAuth에 그리드 자격증명을 위한 X.509 인증 위임 표준 절차를 추가한 프로토콜[8]을 사용한다. 이 프로토콜은 OAuth의 공유 토큰 교환 방법을 사용하여 온라인 자격증명 저장소에서 중간 경유 없이 제 3 자 서비스에게 그리드 자격증명을 위임할 수 있다.

(그림 5)는 인증 정보를 그리드 자격증명으로 교환하는 프로토콜을 간략하게 보여준다. (그림 5)의 2~6단계는 외부 사용자 신원 공급자를 사용하여 사용자를 식별하는 과정을 보여준다. 사용자는 외부 사용자 신원 공급자를 통해서 OAuth, OpenID와 같은 웹 인증 프로토콜을 통해서 식별된다. (그림 5)의 7단계에서는 발급된 공유 토큰을 사용하여 그리드 자격증명을 획득하거나 위임한다.

자격증명 교환 프로토콜에서 그리드 자격증명을 교환하기 위해 (그림 6)과 (그림 7)에서 보여주는 것과 같이 대리 인증서의 서명 요청과 서명 응답을 OAuth의 공유 토큰 교환 요청과 응답 패킷을 확장한다. 2개의 HTTP 헤더 xoauth_proxy_request 와 xoauth_public_certificate가 추가되었고, 대리 인증서 서명 요청서 혹은 서명된 대리 인증서는 첨부파일 형태로 전달된다.



(Figure 5) Credential exchange protocol

```
HTTP/1.1 200 OK
(HTTP headers…)
xoauth_proxy_request=request.csr
Content-type: multipart/x-mixed-replace, boundary="Boundary"
--Boundary
Content-Type: application/x-www-form-urlencoded
<OAuth response content>
--Boundary
Content-Type: text/plain
Content-disposition: attachment; filename="request.csr"
<Content of proxy certificate signing request>
```

(Figure 6) Packet for requesting proxy credential

```
POST /token HTTP/1.1
(HTTP headers…)
xoauth_public_certificate=proxy.pem
Content-type: multipart/x-mixed-replace, boundary="Boundary"
--Boundary
Content-Type: application/x-www-form-urlencoded
<OAuth request contents>
--Boundary
Content-Type: text/plain
Content-disposition: attachment; filename="proxy.pem"
<Content of Proxy certificate>
```

(Figure 7) Packet for response

위임 서비스로 그리드 자격증명을 위임할 때는, 위임 서비스가 OAuth의 사용자 인증 완료 후에 (그림 6)와 같이 헤더를 확장하여 응답한다. 클라이언트는 대리 인증서를 서명하여 (그림 7)와 같이 헤더를 확장하여 위임 서비스에 접근 토큰을 요청함으로써 위임이 이루어진다.

위임 서비스에서 인증서를 획득할 때는, 그리드-웹 애플리케이션은 위임 서비스로 OAuth 접근 토큰 요청 시

(그림 6)처럼 인증서 요청 서명을 위한 헤더를 확장하여 요청한다. 위임 서비스는 사용자 인증 단계에서 사용자가 선택한 그리드 자격증명을 사용하여 대리 인증서를 서명하여 (그림 7)처럼 헤더를 확장하여 응답한다.

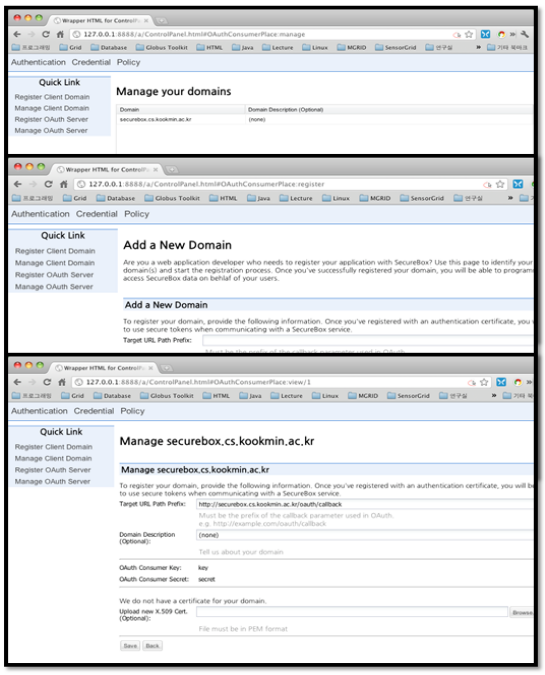
4.3 인증

위임 서비스는 사용자 식별을 위해서 OAuth, OpenID와 같은 웹 인증 기술을 제공하는 외부 사용자 신원 공급자를 지원한다. 따라서 사용자의 신원 정보를 제공하지 않는 서비스의 경우 사용할 수 없다.

본 논문에서 구현한 위임 서비스에서 사용자인증(Authentication) 관리자는 Email을 사용자 이름으로 사용하도록 구현되었다. 따라서 외부 사용자 신원공급자는 다음과 같은 사항을 만족해야 한다.

1. OAuth/OpenID와 같은 웹 인증을 제공
2. 인증 후에 신원 공급자로부터 사용자의 Email을 얻을 수 있어야 한다.

(그림 8)은 외부 인증 서비스를 관리하는 화면을 보여준다.



(Figure 8) External IdP Management

5. 관련연구

많은 연구자들이 MyProxy와 같은 온라인 자격증명 저장 서비스를 이용하여 X.509 위임방법을 사용하는 그리드와 웹의 보안을 통합하기 위한 연구를 하였다.

CredEx[9]는 비밀번호 기반 웹 서비스와 GSI 기반 그리드 서비스간의 자격증명 교환 시스템이다. CredEx는 사용자 인증을 위해서 인증서의 식별에 중점을 두고, WS-Security[10]와 WS-Trsut[11] 표준을 기반으로 개발되었다. CredEx는 반복적인 자격증명 교환 호출을 위해서 별칭을 사용한다. 자격증명 교환에 사용하는 별칭과 사용자 인증 정보를 연결하는 것은 사용자 책임이다. 또한 사용자는 자격증명 교환을 위해서 별칭을 알고 있어야만 한다.

SafeBox[12]는 InterGrid 컴퓨팅 플랫폼을 위한 온라인 자격증명 관리 서비스 아키텍처이다. SafeBox는 MyProxy보다 긴 시간 동안의 대리 인증서 위임을 MyProxy 보다 안전하게 저장하고 획득하기 위한 방법과 한 개 이상의 그리드 가상 조직간에 사용하는 방법을 고안하여 개발되었다. SafeBox는 한 개 이상의 그리드 자격증명을 저장할 수 있도록 보안 방법을 제공하고 있다. 대리 인증서 위임 및 획득을 위해서 사용자는 사용자 이름과 비밀번호 쌍을 통해서 공유 토큰을 발급하고, 공유 토큰을 통해서 저장된 그리드 자격증명을 획득할 수 있다.

(표 1)은 온라인 자격증명 서비스들을 사용자 인증 및 인증방식과 그리드 인증으로 교환하는 방법, 그리드 인증을 사용하려고 하는 제 3자로부터 사용자 인증의 보호 여부, 단일 로그온 지원 여부 및 다중 인증서 지원 여부를 비교한 것이다. 우선, 사용자 인증 및 인증 방식에 있어 본 논문은 OpenID나 OAuth와 같은 웹에서 사용하는 외부 인증 방법을 이용하여 사용자 인증을 지원한다. 공인인증서 및 다른 여러 가지 인증을 도입 확장할 수 있는 유연성을 가진다. CredEx나 SafeBox는 사용자이름과 비밀번호 쌍의 자체 인증 방식을 사용한다.

제 3 서비스에게 그리드 인증을 교환 하는 방법에서는 CredEx는 제 3 서비스가 CredEx에 직접 요청을 해야 함으로 사용자 인증 정보가 제 3 서비스에 중계되어야 한다. 제 3 서비스에게 사용자 이름과 비밀번호가 노출된다. SafeBox는 제 3 서비스에게 발급받은 공유 토큰을 전달함으로써, 사용자 이름과 비밀번호가 노출되지 않도록 한다. 그러나 공유 토큰을 제 3 서비스에게 전달하는 과정이 제시 되지 않았다. 본 논문에서는 OAuth 방식으로 제 3 서비스에게 접근을 허가한다. 확장된 OAuth 프로토콜을 통해서 사용자 인증 정보가 노출되는 것을 막으면

(표 1) 온라인 자격증명 서비스 비교
(Table 1)

	본 논문	CredEx	SafeBox
인증방식	웹 기반 인증	사용자이름/비밀번호 쌍	
사용자인증	외부인증	자체 인증	
단일 로그온 (SSO)	O	X	O
다중 인증서	O	O	O
그리드 인증 교환방법 (사용자포함)	OAuth에 기반한 사용자 허가	WS-Trust +중계	공유 토큰 기반
제3자로부터 인증보호	OAuth에 의존적	X	공유토큰에 의존적
인증중계 방지	OAuth를 통해 해결	X	공유 토큰의 전달 방법이 제시 되지 않음

서 그리드 인증을 교환하는 것을 지원한다.

6. 결 론

본 논문에서는 그리드 서비스를 지원하는 웹 애플리케이션이 표준 웹 환경의 인증 방식에서 그리드 자격증명을 지원하기 위한 온라인 자격증명 저장 위임 서비스를 제안하였다. 위임 서비스는 그리드 자격증명 위임을 위해서 OAuth에 X.509 위임 인증 절차를 추가한 자격증명 교환 프로토콜을 사용하여서, 사용자 인증 정보를 그리드-웹 애플리케이션을 통해 중계하지 않고, 하나 이상의 그리드 자격증명을 위임하거나 획득할 수 있는 안전한 방법을 제공한다.

제안한 위임 서비스의 주요 이점은 중계 애플리케이션(그리드 포털)에게 위임 서비스를 위한 인증 정보를 전달하지 않고, 그리드 자격증명에 대한 접근을 허가할 수 있는 것과 외부 신원 공급자를 통해서 그리드-웹 애플리케이션과 위임 서비스의 단일 로그온 지원이 가능한 것, 다중 인증서 지원으로 그리드-웹 애플리케이션이 쉽게 여러 가상 조직에 속한 그리드를 지원할 수 있는 것이다.

참 고 문 헌(Reference)

[1] I. Foster, C. Kesselman and S. Tuecke, “The anatomy of the grid” in International Journal of High Performance Computing Applications, Mar. 2001.

[2] V. Welch, I. Foster, C. Kesselman, O. Mulmo, L. Pearlman, S. Tuecke, J. Gawor, S. Meder and F. Siebenlist, “X.509 Proxy Certificates for Dynamic Delegation”, In 3rd Annual PKI R&D Workshop, 2004.

[3] J. Novotny, S. Tuecke and V. Welch, ″An Online Credential Repository for the Grid: MyProxy″ in Proc. of the Tenth International Symposium on High Performance Distributed Computing (HPDC- 10), IEEE Press, Aug. 2001.

[4] J. Basney, M. Humphrey and V. Welch, “The MyProxy online credential repository” in Software Practice and Experience, vol.35, pp. 801-816, 2005,

[5] CollabNet: OpenSSO. Online available at https://opensso.dev.java.net/.

[6] OpenID Authenticatioin 2.0, OpenID Foundation, 2007; http://openid.net/specopenid-authentication-2_0.html

[7] E. Hammer-Lahav, “RFC5849; The OAuth 1.0 Protocol”. IETF, Apr. 2010

[8] 허대영, 황선태, 정갑주 “X.509 대리 인증서 위임을 위해 확장된 OAuth 프로토콜”, 정보과학회논문지, 시스템 및 이론, 제 38권, 제 5호, pp.257-262, 2011.10

[9] D. D. Veccio, M. Humphrey, J. Basney and N. Nagaratnam, “CredEx: user-centric credential management for grid and Web services” in Proc. Of the IEEE International Conf. on Web Services p.149-156, Jul. 2005

[10] A. Nadalin, et al., Eds. Web Services Security 1.0 (WS-Security). OASIS Standard 200401, March 2004; http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

[11] A. Nadalin, M. Goodner, M. Gudgin, A. Barbir, and H. Granqvist. WS-Trust 1.3; http://docs-oasis-open.org/wssx/ws-trust/v1.3/ws-trust.pdf, 2007. OASIS Standard

[12] J. H. Abawajy, “An online credential management service for InterGrid computing” in IEEE Asia-Pacific Services Computting

◐ 저 자 소 개 ◑

허 대 영

2004년 국민대학교 컴퓨터과학과(이학사)
2006년 국민대학교 대학원 전산과학과(이학석사)
2006년~현재 국민대학 대학원 전산과학과 박사과정
관심분야 : 그리드 컴퓨팅, 클라우드 컴퓨팅, 시스템 아키텍쳐
E-mail : dyheo@cs.kookmin.ac.kr

황 선 태

1985년 서울대학교 컴퓨터공학과(공학사)
1987년 서울대학교 대학원 컴퓨터공학과(공학석사)
1996년 Manchester University, Computer Science(공학박사)
1997년~현재 국민대학 컴퓨터공학부 교수
관심분야 : e-Science, 사이버인프라스트럭쳐, 그리드 컴퓨팅, 클라우드 컴퓨팅, 공개소프트웨어
E-mail : sthwang@cs.kookmin.ac.kr