서비스 기반 구조의 그리드를 위한 통합 인증 및 권한 위임 방법

김상완, 박형우, 김종°
한국과학기술정보연구원 슈퍼컴퓨팅센터 그리드연구실, 포항공과대학교 컴퓨터공학과°
{sangwan, hwpark}@kisti.re.kr, jkim@postech.ac.kr°

A Single Sign-On Authentication and Delegation Mechanism for Service Oriented Architecture Grid

Sangwan Kim, Hyoungwoo Park, Jong Kim°
KISTI Supercomputing Center Grid Technology Research Department,
POSTECH(Pohang University of Science and Technology) Computer Engineering Department°

요 약

그리드 미들웨어는 다양한 종류의 수많은 그리드 자원을 일관된 방법으로 이용하고 제어할 수 있는 수단을 사용자에게 제공해 준다. 많은 수의 그리드 자원을 한번의 인증으로 이용할 수 있게 하는 통합인증과 사용자의 권한을 다른 서비스로 위임할 수 있는 권한 위임은 그리드 미들웨어에서 해결해야할 중요한 문제이다. 본 연구에서는 사용자 통합인증과 권한 위임 구조로 쉽게 확장이 가능한 사용자 인증 시스템 구조를 제시한다.

1. 서 론

그리드 컴퓨팅은 네트웍으로 연결되어 있는 다양한 종류의 컴퓨팅 자원을 통합하여 보다 효율적으로 사용하기 위한 컴퓨팅 방식이다. 지역적으로 분산되어 있거나 서로 다른 관리도메인에 속한 컴퓨팅 자원을 서로 공유함으로써 국가적으로 컴퓨팅 자원에 대한 중복투자를 줄일 수 있으며, 사용자 입장에서는 동시에 많은 수의 컴퓨팅 자원에 접근할 수 있으므로 갑자기 많은 양의 컴퓨팅 자원이 필요한 경우에도 쉽게 대처가 가능하다.

그리드 환경에서 사용자는 절절한 그리드 자원을 이용하기 위해서 먼저 사용자는 자신이 해당 그리드 자원을 이용할 수 있는 정당한 사용자임을 증명하는 사용자 인증 과정을 거치게 된다. 사용자가 많은 수의 그리드 자원을 동시에 또는 연속적으로 이용하기 위해서는 각 자원에 대한 사용자 인증 과정을 하나로 통합할 수 있는 방안이 요구된다. 또한 그리드 환경에서는 PSE (Problem Solving Environment)와 같이 사용자를 대신하여 작업을 실행시키고 진행상황을 관리하는 에이전트(혹은 그와 유사한 것)가 필요할 수도 있으며, 이 경우 해당 에이전트가 사용자의 권한 일부를 위임 받아 사용자 대신 그리드 자원에 접근해야 해야 하는 상황이 발생한다.

본 연구에서는 서비스 기반의 그리드 컴퓨팅 환경에서 사용자 통합 인증 및 권한 위임을 가능하게 하는 보안 구조를 제시한다. 본 논문의 제2절에서는 기존의 그리드 보안 구조로써 글로버스에서 개발된 GSI에 대한 설명과 장단점을 논의한다. 제3절에서는 본연구에서 제시하고자 하는 기본 인증구조를 설명하고, 제4절에서는 통합인증을 위해 확장된 구조를, 제5절에서는 권한 위임을 위해 확장된 모델을 제시한다.

2. 기존 연구

글로버스[1]에서 이용하고 있는 GSI(Grid Security Infrastructure)[2][3] 보안 구조의 핵심은 PKI와 X.509 공개키 인증서 및 사용자 프록시 인증서이다. GSI에서 인증기관(Certificate Authority)은 모든 보안 객체(사용자 및 그리드 자원)에 대하여 X.509 형식을 따르는 고유의 공개키 인증서를 발급한다. 사용자 프록시 인증서는 사용자의 권한을 동적인 엔터티에게 동적으로 위임 할수 있게 하고, 반복적인 사용자 인증과정을 사용자 개입 없이 한번에 수행할 수 있도록 한다.

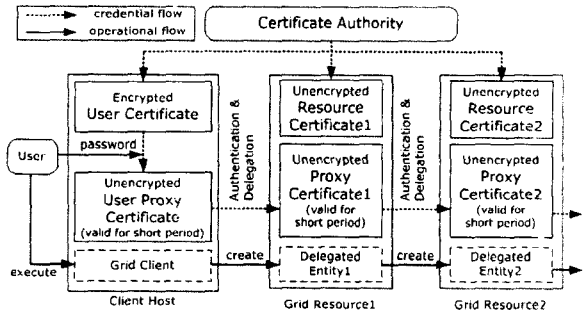


그림1. GSI 구조도 및 동작 원리

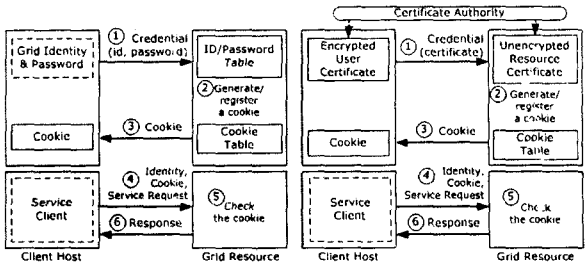
그림1은 GSI의 구조 및 동작 원리를 설명하고 있다. 사용자는 자신의 로컬 호스트에 CA로부터 발급받은 사용자 인증서를 보관하고 있다. 사용자 인증서(user certificate)는 파일의 형태로 존재하여 다른 사람들에 의한 오남용을 방지하기 위해 사용자의 비밀번호로 암호화 되어 있다. 따라서 사용자 인증서를 이용하여 사용자 프록시 인증서(user proxy certificate)를 생성하는 단계에서 비밀번호를 입력하여야만 한다. 사용자 프록시 인증서는 암호화 되어 있지는 않으나 인증서 유효기간이 일정 시간으로(기본 12시간) 설정되어 있다. 사용자 프록시 인증서 역시 파일 형태로 존재하며, 사용자가 실행한 클라이언트 프로그램에 의해 이용되어 그리드 자원에 사

용자를 인증하는데 이용된다. 그리드 자원에서는 클라이언트의 요청에 의해 새로운 프록시 인증서가 생성되고, 이것을 이용하여 또 다른 그리드 자원에 연속적으로 그리드 자원에 인증 과정을 거치게 된다.

그러나, GSI는 다음과 같은 단점들을 가지고 있다. 첫째, 프록시 인증서의 오남용에 대한 가능성이 존재한다. 그림1에서 보여 주고 있는 신뢰 사슬(trusted chain)은 파일 시스템 상에 암호화 되지 않은 인증서에 의해서 형성되며, 신뢰 사슬의 어느 한 단계에서 인증서가 공격자에게 노출 될 경우 사용자의 권한이 남용될 소지가 있다. 이러한 공격의 피해를 줄이기 위해 위임 단계에서 인증서의 유효기간을 설정하고 인증서에 사용자 권한을 명시적으로 제한하여 남용될 가능성을 줄이는 방법이 있을 수 있으나, 인증서에 모든 권한을 기술하는 것이 쉽지 않을 뿐더러, 인증서에 명시된 권한 내에서는 권한이 남용될 수 있으므로 완전한 해결책이라고 할 수 없다. 두 번째, 신뢰 사슬에서 상위 인증서에 대한 유효성을 점검하기가 어렵다. 그리드 자원의 입장에서 사용자 인증단계에서 받아들이는 것은 프록시 인증서이며, 이 프록시 인증서의 유효성을 점검하기 위해서는 신뢰 사슬의 상위 인증서에 대한 모든 유효성을 검사하여야만 한다. 이것은 상당히 복잡한 과정이며, 단순히 인증서의 서명을 단계적으로 확인하는 것으로는 충분하지 않을 수 있다. 공격자가 사용자 프록시 인증서를 오남용 하고 있다는 사실을 사용자가 발견하고, 해당 프록시 인증서를 무효화 시킬 경우 해당 인증서를 이용하여 생성된 모든 프록시 인증서를 추적하여 폐기 하거나, 인증 과정에서 일일이 상위 인증서에 대한 유효성을 온라인상으로 조회하는 과정이 필요한데, 이것은 현실적으로 매우 어렵다. 셋째로, GSI는 공개키 기반 구조에서 사용되는 수학적인 알고리즘을 이용하므로 사용자 인증과정이 복잡하고, 필요에 따라 보안 레벨을 낮추거나 높일 수 없다. 그리드는 다양한 종류의 자원의 통합을 목표로 하고 있으며, 이것은 단순히 컴퓨터뿐만 아니라, 소형 휴대용 장치, 특수 하드웨어 장비 등을 모두 포함한다. 공개키 알고리즘과 같은 복잡한 인증절차는 이와 같은 그리드 자원에 하드웨어적으로 구현하기 어려울 뿐만 아니라, 상대적으로 낮은 정도의 보안을 수준을 요구하는 경우에도 일률적으로 적용되어야 하므로 성능저하나 사용자 불편을 초래할 수 있다.

3. 기본 모델

본 연구에서 제시하고자 하는 사용자 인증 메커니즘의 가장 간단한 형태를 그림2에 나타내었다. 그리드 자원은 서비스 형태로 외부에 공개 되어 있으며, 이 서비스를 이용하는 과정은 서비스에 대한 요청(request)과 그에 대한 응답(response)으로 이루어진다고 가정하였다. 본 연구의 모델에서는 클라이언트가 그리드 서비스를 이용하는 과정에 있어서 사용자 인증단계와 서비스를 이용하는 단계를 분리시킴으로써 같은 서비스에 대하여 다양한 인증 방법을 적용시킬 수 있도록 하였다. 그림2 (a)와 (b)에서 인증정보를 전달하는 과정(①)과 그것을 확인하고(②), 쿠키를 전달하는 단계(③)가 사용자 인증단계에 해당하고, 나머지 ④-⑥단계는 서비스를 이용하는 단계



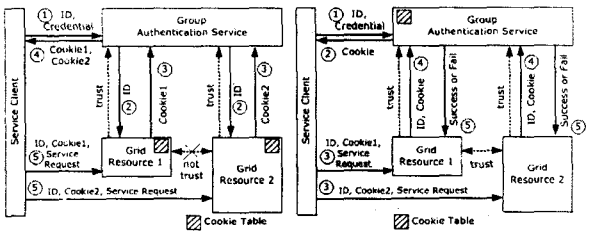
(a) ID/PW 방식을 이용 (b) 공개키 인증서를 이용
그림2. 서비스 기반 구조에서 사용자 인증 방법

로써 (a), (b)의 그림에서 동일하다. (a)의 경우는 아이디/패스워드 방식의 인증방법을 적용한 경우이다. 사용자는 그리드 상에서 자신의 아이디(이메일 주소와 같은)와 해당 그리드 자원에 미리 설정되어 있는 패스워드를 전달한다. 그리드 자원은 인증정보를 확인한 뒤 일정시간 동안만 사용할 수 있는 일정한 길이의 임의의 비트열인 쿠키(HTTP 프로토콜에서 사용되는 Cookie와 유사함)를 생성하여 클라이언트에게 전달한다. 클라이언트는 서비스 이용단계에서 서비스 요청 내용에 덧붙여 자신의 아이디와 쿠키를 전송함으로써 해당 서비스 요청이 정당한 것임을 증명하게 된다. 그림2의 (b)에서는 사용자 인증단계에서 비밀번호를 이용하지 않고, 사용자 인증서를 이용하는 것이 다르다.

이상의 기본 구조에서 고려할 것으로 첫째, 인증정보 및 쿠키전송이 공격자에게 노출되지 않도록 해야 한다는 것이다. 이것은 경우에 따라 필요하거나 필요하지 않을 수 있으며, 공개키 인증서를 이용하는 경우 SSL(secure socket layer)등을 적용하여 보안 수준을 높일 수 있다. 둘째, 쿠키가 공격자에게 노출되었다고 판단되었을 경우 혹은 사용자가 그리드 서비스를 더 이상 이용하지 않게 될 경우 사용자가 기존의 쿠키를 무효화 시키는 매커니즘이 필요하다. 그리드 자원으로부터 받은 쿠키는 그리드 자원에 유효기간과 함께 등록되어 일정 시간동안 관리된다. 그러나 이와 같은 경우에 쿠키를 무효화 시킬 수 있게 함으로써 공격위험을 줄일 수 있다.

4. 통합 인증을 위한 확장 모델

이상 3절에서 설명한 기본 모델을 확장하여 여러 그리드 자원에 대한 사용자 인증 과정을 단일화 할 수 있는 통합 인증을 위한 보안 구조를 그림3에 나타내었다. 통합 인증을 위해서 통합 인증을 담당하기 위한 그룹 인증 서비스(Group Authentication Service, 이하 GAS)가 추가 되었다. 그리드 자원은 하나 이상의 GAS에 등록 되어 있으며(이로써 그리드 자원과 GAS사이에 신뢰관계가 형성된다), 그룹 인증 서비스가 담당하고 있는 그리드 자원에 대해서만 통합 인증이 이루어진다. 그림3의 (a)의 경우는 같은 GAS가 관리하는 그리드 자원들이 서로 신뢰하지 않는 경우이고, (b)는 그 반대의 경우이다. 그림3(a)에서 서비스 클라이언트는 GAS에 사용자 ID와 인증정보를 제출함으로써 그리드 자원에 대한 쿠키를 얻는다. 이 과정에서 GAS는 각각 그리드 자원에 요청을 하고 서로 다른 쿠키를 전달 받아 클라이언트로 전달한다.



(a) 그리드 자원간 비신뢰 (b) 그리드 자원간 신뢰

그림3. 통합 인증을 위한 확장 모델

클라이언트는 서로 그리드 자원에 접근하기 위해 각 그리드 자원에 해당하는 서로 다른 쿠키를 이용하여야 한다. 그림3(b)는 그리드 자원간 신뢰관계가 형성되어 있을 때 단일 인증과정을 나타낸다. 사용자는 GAS로부터 받아온 하나의 쿠키만 관리한다. 클라이언트가 서비스를 요청할 때 이 쿠키값을 그리드 자원으로 전달하고, 그리드 자원은 해당되는 GAS를 통하여 클라이언트가 보내온 쿠키의 유효성을 검사한 후 서비스 하게 된다.

통합 인증과 관련하여 공격자의 공격에 의해 쿠키가 노출되었을 경우를 생각해 보자. 그림3(a)에서 Cookie1이 공격자에게 노출되었다 하더라도 공격자는 그리드 자원1에 대해서만 공격이 가능할 뿐 같은 GAS 그룹내의 다른 그리드 자원은 공격할 수 없다. 그림3(b)에서는 하나의 쿠키로 모든 그리드 자원에 공통적으로 사용되므로, 공격자에게 쿠키가 노출되면 GAS 그룹내의 모든 그리드 자원이 영향을 받게 된다.

5. 권한 위임을 위한 확장 모델

그리드에서 사용자는 자신을 대신하여 어떤 작업을 수행해 줄 것을 서비스에 요청하며, 이때 사용자의 일부 권한을 서비스에게 위임시켜 주어야 한다.[4] 예를 들어 사용자 A가 R1이라는 그리드 자원이 그리드 자원 R2에 위치하고 있는 어떤 파일을 읽어 오도록 하는 간단한 시나리오를 생각해 보자. R1은 R2에서 특정 파일을 읽을 수 있는 사용자 A의 권한을 위임 받아야 사용자 A의 요청을 수행할 수 있다. 그림4에서 사용자 A는 먼저 R2로부터 특정 파일을 읽을 수만 있는 제한된 권한을 가진 쿠키 C2를 받아 오게 된다.(①,②) 그와 동시에 R1으로부터는 파일을 읽어 오는 작업을 수행하기 위한 쿠키를 받아오게 된다.(③,④) 이제 사용자 A는 R1에게 "R2로부터 특정파일을 읽어!"라는 작업 요청과 함께 R2로부터 받는 쿠키인 C2도 함께 전달하게 된다.(⑤) R1은 C2를 이용하여 R2로부터 파일을 읽어 올 수 있게 된다.(⑥) 이 시나리오에서 가정하고 있는 것은 그리드 자원이 사용자의 권한을 제한시킬 수 있는 쿠키를 생성할 수 있다는 것이다. R2가 사용자에게 넘겨준 쿠키인 C2는 파일을 읽음(다운로드) 수만 있을 뿐 파일을 쓰거나(업로드), 작업을 실행하는 등의 작업은 할 수가 없다는 것이다. 그리드 자원은 쿠키를 생성할 때 그 쿠키로 할 수 있는 권한을 명시하여 두고, 작업 요청이 들어 왔을 때 쿠키에 해당하는 작업 권한이 적절한지 판단할 수 있어야 한다.

사용자의 권한이 위임되는 시점이 권한이 필요한 시점

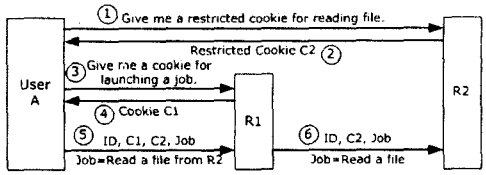


그림4. 권한 위임 적용 예

에 이루어 져야 하는 경우가 있다. 두 번째 시나리오는 앞의 시나리오와 비슷하나, R1이 읽어 와야 될 파일이 어떤 그리드 자원이 가지고 있는지 알지 못하는 경우이다. 그림5에서 보는 바와 같이 사용자는 R1에게 어디 있는지 모르는 특정 파일을 읽어 오라는 요청을 보내게 된다.(③) R1는 작업을 수행하기 위해 파일을 가지고 있는 그리드 자원을 검색하여 R2가 그것을 가지고 있다는 사실을 알게 되었다.(④) 그러나 R1에게는 R2로부터 파일을 읽을 수 있는 권한이 없으므로, 사용자 A에게 요청 메시지를 보내어 대신 권한(쿠키)를 얻어 줄 것을 부탁하게 된다.(⑤) 사용자는 R2에 파일을 읽을 수 있는 제한된 쿠키(C2)를 요청하여 얻는다.(⑥,⑦) 사용자가 C2를 R1에게 전달하여 줌으로써 비로소 R1에게 권한이 위임되고,(⑧) R1은 R2로부터 파일을 읽는다.(⑨)

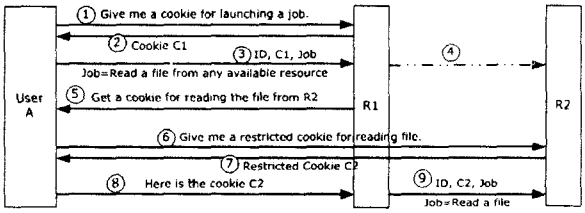


그림5. 권한이 필요한 시점에서 위임이 이루어짐

5. 결론

수많은 그리드 자원을 편리하고 안전하게 이용하기 위해서는 통합된 사용자 인증과 권한 위임이 해결되어야 할 중요한 문제이다. 본 연구에서는 간단하면서도 통합 인증 및 권한 위임을 위해 확장 가능한 사용자 인증 방법을 제시하였다.

참고문헌

[1] Globus Project, http://www.globus.org

[2] "Security Architecture for Computational Grids", I. Foster, C. Kesselman, G. Tsudik, S. Tuecke. Proc. 5th ACM Conference on Computer and Communications Security Conference

[3] X.509 Proxy Certificates for Dynamic Delegation, Von Welch, et. al., Submitted to 3rd Annual PKI R&D Workshop, http://www.globus.org/Security/papers/pki04-welch-proxy-cert-draft.pdf

[4] "Toward Realizable Restricted Delegation in Computational Grids", Presented at HPCN 2001 (European High Performance Computing and Networking), Amsterdam, June 25-27, 2001. http://legion.virginia.edu/papers.html