PKI와 SOAP에 기반한 분산 컴퓨팅 보안 프로토콜에 관한 연구

한윤택* 김주한* 김지호* 배두현* 박세현* 송오영*
*중앙대학교 전자전기공학부

Secure Distributed Computing System Based on PKI and SOAP

YounTack Han*, JooHan Kim*, DuHyun Bae*, JiHo Kim*
SeHyun Park*, OhYoung Song*
*School of Electrical and Electronic Engineering, Chung-Ang University

요 약

분산 컴퓨팅 시스템에 관한 연구가 네트워크가 발달함에 따라 점차 다양한 분야에서 활발하게 이루어지고 있다. 하나의 컴퓨터의 성능으로는 처리하기 힘든 일을 여러 컴퓨터 시스템이 분산하여 처리함으로써 효율성을 극대화 시킬 수 있도록 하는 이 기술은 네트워크가 발달할 수록 점점 더 각광 받을 것이다. 본 논문에서는 분산 컴퓨팅 시스템에서 무결성, 기밀성을 보장하기 위해 인증 시스템을 이용한 보안 프로토콜을 제시한다.

I. 서론

1. 분산 컴퓨팅 시스템 개요

분산 컴퓨팅 시스템이란 하나의 컴퓨터 시스템만으로는 처리하기 힘든 하나의 커다란 프로젝트를 수행하기 위하여 네트워크를 통하여 연결되어 있는 컴퓨터 시스템들 간에 그 프로젝트를 분산하여 각기 자신이 맡은 부분을 처리하고 중앙 서버로 처리된 부분을 모아 효율적으로 프로젝트를 수행할 수 있도록 하는 시스템을 말한다. 분산 컴퓨팅 시스템에서는 서버와 에이전트가 존재하며 에이전트들은 서버로부터 자신의 역할을 분배 받아 수행하게 된다.

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터(중앙대학교 홈네트워크 연구센터) 지원 사업의 연구결과로 수행되었음

이러한 분산 컴퓨팅 시스템에 대한 연구는 네트워크가 점점 발달해감에 따라 점점 더 활발하게 이루어지고 있다. 하지만 이러한 연구들의 대부분은 무결성에 대한 문제나 인증에 관한 문제 등의 보안 문제에 대한 대비가 아직 많이 이루어지고 있지 않아 보안에 많은 취약점을 드러내고 있는 실정이다. 에이전트와 서버 사이에 이루어지는 데이터의 교환이 네트워크 상에서 노출되기 쉬워 누군가 서버에 대해 공격을 하거나 데이터를 중간에 스니핑하는 등 해킹을 시도 할 경우, 이에 대한 대책이 부족하다. 이러한 보안상의 문제점을 해결하기 위해서 가장 중요한 것은 오직 분산 컴퓨팅 시스템의 서버에 확실하게 인증된 사용자만이 접근할 수 있어야만 한다.

이를 위해 본 연구에서는 PKI(Public Key Infrastructure), 전자 서명(Digital Signature)

그리고 SSL(Secure Sockets Layer)를 사용하여 분산 컴퓨팅 시스템에서의 보안성을 강화시키기 위한 시스템을 설계하였다.

II.본론

1. 제안한 전체 시스템 개요

그림1은 분산 컴퓨팅 시스템에서의 보안성 강화를 위해 인증 절차를 포함시킨 시스템을 보여 주고 있다.

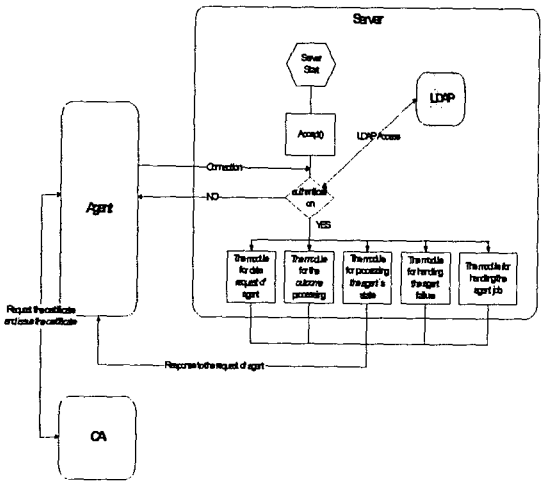

그림1.시스템의 기본 구조

이 시스템의 구조를 살펴보면 위의 LDAP (Lightweight Directory Access Protocol)은 사용자들의 인증서를 저장하기 위해 사용된다. LDAP는 x.500을 기반으로 한 디렉토리 데이터베이스에 접속하기 위한 통신 규약으로써 디렉토리 정보의 등록, 갱신, 삭제와 검색 등을 실행할 수 있다.

인증기관(CA: Certificate Authority)은 분산 컴퓨팅 시스템의 서버에 접근하기 위해 인증을 요청하는 에이전트의 인증을 위한 인증서를 발급한다. 여기서 에이전트는 분산 컴퓨팅 시스템에 참가하는 인터넷 상에 분산되어 있는 시스템을 뜻한다. 이러한 시스템들은 하나의 플랫폼으로 지정되어 있지 않으며 각기 다른 플랫폼에서 동작하는 시스템일 수도 있다.

에이전트들이 시스템에 참여하기 위해 서버로 정해진 절차에 따라 인증을 받아 접속하게 되면 서버는 에이전트의 요청에 대한 응답 메세지를 전송한다.

이 응답메세지에는 Job Processing을 위한 파일이나 서버가 에이전트로 요구하는 요청메세지에 대한 정보가 담겨있다.

이 시스템은 SOAP 메시지의 생성을 위한 SOAP(Simple Object Access Protocol)와 Binary Data를 위한 DIME(Direct Internet Message Encapsulation)을 사용한다.

1.1. SOAP(Simple Object Access Protocol)

SOAP는 XML(eXtensible MarkUp Language)과 HTTP(하이퍼텍스트 전송 규약)을 기반으로 하여 분산 컴퓨팅 시스템 내의 Peer들 사이에서 정보를 구조화하고 정형화하여 서로 다른 플랫폼에 있는 Peer의 데이터나 서비스를 호출하기 위해 사용된다. 분산 컴퓨팅 시스템에서 각 Peer는 각기 다른 플랫폼에서 동작하기 때문에 데이터의 전송 시 문제가 발생할 수 있다. 하지만 SOAP를 사용함으로써 어떤 플랫폼이든지, SMTP(Simple Mail Transfeer Protocol), MIME(Multipurpose Internet Mail Extensions), and HTTP(Hypertext Transfer Protocol) 등의 어떤 프로토콜을 이용하든지 해당 시스템이나 서비스에 접근하는 것이 가능해 진다.

기본적으로 이 시스템에서 SOAP는 HTTP 프로토콜을 이용하여 메시지를 전송한다. 그러므로 다른 프로토콜에 의해 접근이 힘든 NAT (Network Address Translation), 혹은 방화벽을 사용하는 시스템에서도 적절하게 이용될 수 있다. 위와 같은 특성 때문에 이 시스템에서는 SOAP를 사용하였으며 이로 인해 네트워크 상의 각기 다른 시스템을 가진 시스템도 분산 컴퓨팅 시스템의 일부로서 상호 연동 하는 것을 쉽게 할 수 있었다. 더욱이 SOAP-RPC를 이용하게 되면 서버가 유지하고 있는 커넥션에 의해 부하가 걸리는 것을 줄일 수 있도록 도와준다.

1.2 제안한 인증 프로토콜

기본적으로 본 연구에서 설계된 시스템은 PKI 기반의 SSL을 사용한다. PKI 기반이기 때문에

에이전트는 서버로부터 인증을 받기 위해서는 CA로 먼저 접근을 하여 인증서를 발급 받아야 한다. 이 절차는 서버가 인증을 원하는 에이전트만을 시스템에 접근할 수 있도록 인증서를 통해 증명하거나 서버나 에이전트 사이에 주고받는 데이터의 무결성을 획득하기에 유용하게 이용된다. 또한 이 시스템은 SSL을 사용함으로써 기밀성을 유지할 수 있고, 인증 문제와 데이터에 대한 무결성에 대한 문제를 해결하려고 하였다. SSL은 상호간의 인증에 있어서 증가할 수 있는 부하를 줄여줄 수 있다. 그림2는 이 시스템에서 채택한 SSL 프로토콜을 간략하게 묘사해 놓은 것이다.

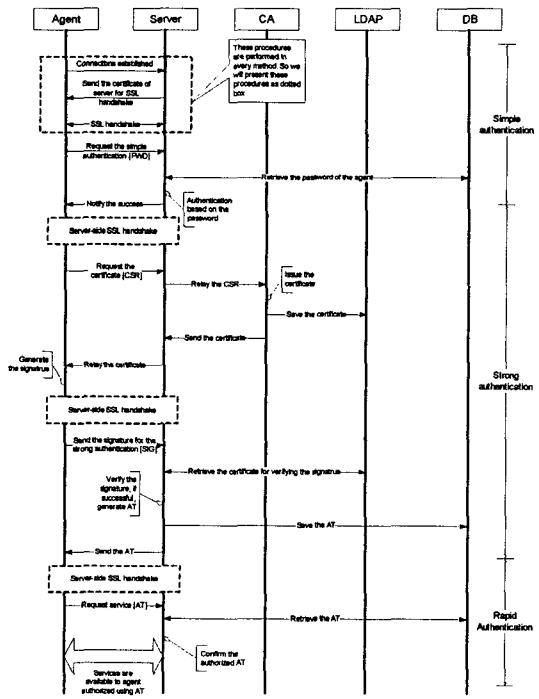

그림2. 전체 인증 프로토콜

3가지의 인증 방법

인증은 경량인증(Simple Authentication), 강한 인증(Strong Authentication), 고속 인증(Rapid Authentication) 이렇게 3가지의 방법으로 구성된다. 그림2에서 나와있는 것과 같이 각 방법은 각각 SSL Handshake를 수행한다.

1.3. 경량 인증(Simple Authentication)

경량 인증은 시스템에 접근하는 각 에이전트의 아이디와 암호를 기반으로 이루어지는 단순한 인증 방법이다. 경량 인증의 기본은 데이터베이스에 입력되어 있는 허가받은 에이전트의 아이디와 암호를 시스템에 접근하는 에이전트의 아이디와 암호를 비교하여 에이전트가 시스템에 등록이 되어 있는지 아닌지를 체크함으로써 인증을 하게 된다.

암호는 MD5(Message Digest Algolithm 5)의 방법으로 암호화한다. MD5란 RFC1321에 규정되어 있는, 가장 널리 사용되고 있는 알고리듬으로 일방향 해시함수로 메시지를 압축하여 32Bit의 길이로 인코딩하여 사용하는 방법을 말한다.

경량 인증의 자세한 흐름도는 그림3에서 그리고 있다.

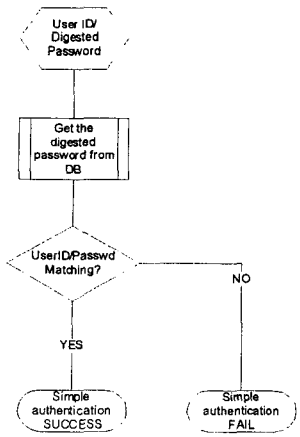

그림3.경량 인증(Simple Authentication) 흐름도

1.4. 강한 인증(Strong Authentication)

강한 인증은 전자 서명을 기반으로 하는 인증 방법이다. 에이전트는 인증을 위해 인증기관으로 접속하여 인증서를 받아야 한다.

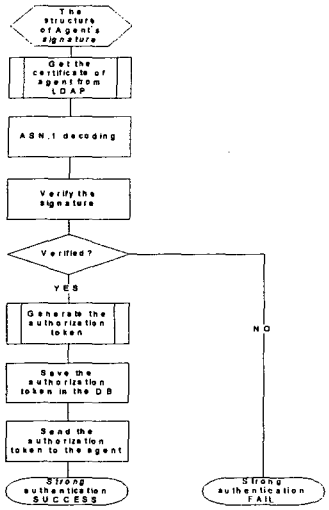

그림4. 강한인증(Strong Authentication)흐름도

그림4에 나온 것과 같이 에이전트는 서버로부터 인증 받기 위한 ANS.1(Abstract Syntax Notation 1)을 기반으로 한 서명을 생성하여 LDAP로 전송한다. 서명의 구조는 Fig5에서 보여진다.

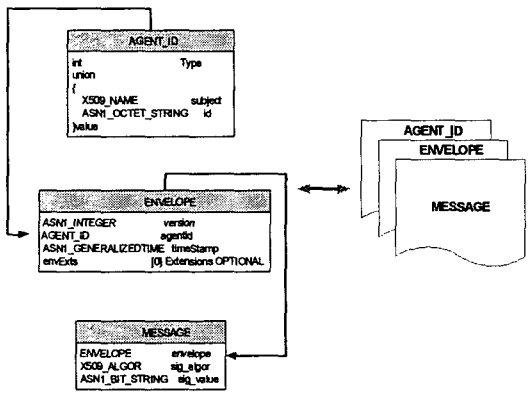

그림5. 서명 메시지의 구조

이 시스템에서 서명메세지의 구조는 MESSAGE, ENVELOP, AGENT _ID 영역으로 구성이 된다.

AGENT _ID는 에이전트에 대한 정보를 포함하며, ENVELOPE 은 추가로 타임스탬프(Time Stamp)와 버전에 대한 정보를 담고 있다. MESSAGE는 X.509 알고리즘과 Base64의 방법으로 인코딩된 에이전트의 서명에 대한 정보를 담고 있다. 에이전트는 이러한 구조로 이루어진 서명을 하여 서버에 인증을 요청한다. 이것에 대한 자세한 절차는 그림6에서 그려져 있다.

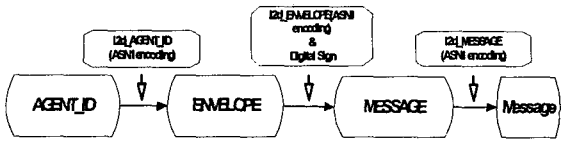

그림6. 전자 서명의 절차

이렇게 해서 생성된 서명은 서버로 전송되고 서버는 LDAP에 저장되어 있는 에이전트의 인증서를 검색하여 에이전트의 서명을 증명하게 된다. 그리고 서버는 ASN.1을 이용하여 에이전트의 서명를 디코딩하여 에이전트의 서명이 확실한 지를 증명한다.

2.3. 고속 인증(Rapid Authentication)

고속 인증은 인증토큰(AT:Authentication Token) 기반이다. 인증 토큰은 앞의 강한 인증의 절차에서 이미 생성되어 데이터베이스에 저장이 된다. 인증 토큰을 이용하면 서버는 에이전트의 전자서명을 다시 증명하지 않고도 에이전트에 대해서 인증을 할 수 있게 된다. 그림 7은 이러한 고속인증의 흐름도를 그리고 있다. 고속인증은 데이터베이스를 통하여 인증토큰을 받아 에이전트가 보내는 인증토큰을 증명함으로써 에이전트를 인증하게 된다. 만일 두 개의 토큰이 매치 된다면 에이전트는 시스템에 접근할 권한을 얻게 되고 그렇지 않으면 시스템에 접근할 수 없게 된다.

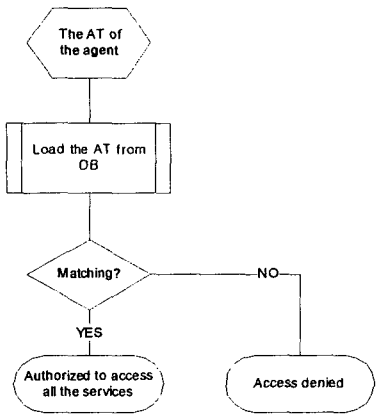

그림7. 고속인증(Rapid Authentication) 흐름도

III. 결론

본 논문에서는 분산 컴퓨팅 시스템에서의 보안문제를 해결하기 위한 보안 프로토콜에 대해 논의해 보았다. 분산 컴퓨팅 시스템무결성과 기밀성을 SSL을 사용하여 해결하였고 이것은 여러 에이전트와의 접속에 대한 부하를 줄여줌으로써 시스템이 더욱 원활하게 작동될 수 있도록 도와준다. 더욱이 SOAP-RPC에 의해 NAT나 방화벽으로 인해 발생하는 문제 또한 해결할 수 있다. 무엇보다도 이 시스템에서 중점을 둔것을 에이전트의 인증에 관한 것이었다. 경량인증(Simple Authentication)은 MD5와 Base64를 이용한 암호를 사용하였고, 강한 인증(Strong Authentication)은 PKI와 인증서를 이용한 서명을 사용한 것이었다. 특히 강한 인증(Strong Authentication)에서 전자 서명을 표시하고 검증하기 위해 특정한 서명메시지 구조를 디자인 하였다. 또한 고속인증(Rapid Authentication)은 인증된 에이전트에게 인증토큰을 전송하여 인증토큰을 지닌 에이전트는 모든 서비스에 접근할 수 있도록 하여 인증절차를 간단하게 함으로써 시스템의 부하를 줄일 수 있도록 하였다. 본 논문에서는 분산 컴퓨팅 시스템 내에서의 이러한 인증 프로토콜에 관한 연구를 통해 효율성 있고 보안이 강화된 분산 컴퓨팅 시스템을 제안해 보았다.

[참고문헌]

[1] Distributed Computing Info. (http://distributedcomputing.info/)

[2] Leon Erlanger, Distributed Computing: An Introduction, Extreme Tech, April 4, 2002

[3] Jeannine Hall Gailey, DIME Sending Files, Attachments, and SOAP Messages Via Direct Internet Message Encapsulation, the December 2002 issue of MSDN Magazine.

[4] Robert A. van 뚱디두, Kyle A. Gallivan, The SOAP Toolkit for Web Services and Peer-To-Peer Computing Networks, Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid.

[5] Don Box, David Ehnebuske, Gopal Kakivaya, Andrew Layman, Noah Mendelsohn, Henrik Frystyk Nielsen, satish Thatte, Dave Winer, SOAP: Simple Object Access Protocol, 18 April 2000.