전자도서관 시스템에서 Kerberos를 이용한 사용자 인증 방법

이 권일*

*한국전자통신연구소 소프트웨어공학연구실

User Authentication Mechanism Using Kerberos on the Digital Library System

Kwon-Il Lee

S/W Engineering Section, ETRI

요 약

초고속 정보 통신 기반 응용 서비스 분야 중의 하나인 전자 도서관 시스템은 많은 기술적인 요구 사항을 가지고 있다. 특히 보안 기술은 문서 서비스에 대한 사용료 지불 문제, 저작권 보호 문제 등과 밀접한 관계를 가지고 있는 쟁점 중의 하나이다.

전자 도서관에서 요구되는 보안 기술로는 문서에 대한 접근 통제 기술, 사용자 인증 기술, 문서와 사용자 데이터에 대한 비밀 보장 기능 등 여러 가지가 있다. 이 논문은 분산 환경에서 사용자 인증 기능을 제공하는 MIT Kerberos를 사용하여 전자 도서관에서 사용자 인증 기능을 제공하는 방법을 제안하였다.

I. 개 요

초고속 정보 통산망의 등장은 사용자들에게 보다 나은 정보를 제공하기 위한 많은 응용 서비스들을 필요로 할 것이다.

전자 도서관은 초고속 응용 서비스 분야 중 주목받고 있는 서비스 중의 하나로 현재 많은 연구 과제가 이루어지고 있다. 대표적인 과제로서 미국의 NSF, ARPA, 그리고 NASA에서 후원하는 DLI(Digital Library Initiative)는 미국 내의 6개 대학(Stanford University, University of Michigan, University

of California at Berkeley , University of California at Santa Barbara, University of Illinois Urbana Champaign, Carnegie Mellon University)들이 참여하여 전자 도서관의 다양한 분야들에 대해 연구를 수행하고 있다. 또한 각기 prototype 시스템을 개발하여 시범 운영 중이다.

전자 도서관 시스템에서 해결해야 할 중요한 문제 중의 일부로 전자 도서관 서비스에 대한 전자 지불 문제와 전자 문서의 저작권 보호 문제가 있다[1]. 전자 도서관 서비스와 연관된 전자 지불과 전자 문서에 대한 저작권 보호 문제를 해결하기 위해서는 보안 기술이 요구된다[2, 3]. 또한 안전한 전자 문서 서비스를 제공하기 위해서도 보안 기술이 필요하다[3].

본 논문에서는 MIT 에서 개발한 Kerberos[4]를 사용하여 전자 도서관 시스템에서 사용자 인증 기능을 제공하는 방법을 제안하였다.

본 몬문의 II 장에서는 전자 도서관 시스템에서 필요한 보안 기술을 살펴보고 III 장에서 전자 도서관에서의 사용자 인증에 Kerberos 를 사용하는 방법을 제안하고 IV 장에서 결론을 맺는다.

II. 전자 도서관에서 요구되는 보안 기술

본 장에서는 전자 도서관 시스템에서 필요한 보안 기술을 살펴본다.

전자 도서관에서 필요한 보안 기술은 다음 세 가지로 구분할 수 있으며, 이들은 시스템에서 기본적으로 필요로 하는 기능들로 분석되고 있다.

- 문서 서비스
- 저작권 보호
- 문서 사용에 대한 지불

1) 문서 서비스

사용자가 문서의 메타 정보에 접근하는 경우, 우선 저장된 메타 정보에 대한 사용자의 권한을 검사하여 정보 접근을 통제하는 기술의 필요성이 존재한다. 그리고 사용자의 사생활 보호 측면에서 문서 서비스를 요구하는 사용자 usage 와 사용자에게 전송되는 디지털 문서의 암호화 기능이 요구된다. 또한 사용자가 전송받은 디지털 문서가 유효한 전자 도서관으로부터 전송되었는지를 확인하는 문서

인증 기능이 필요하다. 사용자의 사생활 보호를 위해 어떤 사용자가 검색한 정보에 대한 기록을 유지하지 않는 기능 또한 필요하다.

2) 저작권 보호

저작권 보호를 달성하기 위해서는 보호하는 방법과 침해를 탐지하는 방법이 있다. 이 중에서 저작권 보호 방법이 보안 기술을 요구한다.

저작권 위반을 방지하기 위해서는 기본적으로 공개키 암호화 시스템(public key cryptosystem)이 필요하다. 또한 사용자 인증, 상호 전달되는 메세지의 암호화, 그리고 메세지에 대한 전자 서명 기술이 필요하다.

3) 문서 사용에 대한 지불 처리

사용자가 요구한 전자 도서관 서비스에 대한 사용 요금 지불(payment)에 관련되어서, 여러 형태의 보안 기술들이 이용된다.

지불에 관련된 보안 위협 요소는 도청과 지불 요청 서버로 위장하는 행위가 가장 주목받고 있다. 이러한 위협 요소들을 제거하기 위해 사용되는 보안 기술들은 공개키 암호화 시스템을 기반으로 하고 있다.

네트워크 상에 전송되는 지불 요청 메세지와 지불 처리 메세지 등의 강력한 암호화 기술, 사용자 인증 기술, 유효한 지불 요청 메세지인지 확인하기 위한 전자 서명 기술, 메세지의 무결성을 보장하기 위한 secure checksum 기술 등이 지불 시스템에서 요구되는 보안 기술이다.

위에서 살펴본 전자 도서관 시스템에서 요구되는 보안 기술 중 필수적인 요소 중의 하나가 사용자 인증 기술이다. 사용자 인증이라 함은 어떤 전자 도서관을 사용하고자 하는 사용자가 적법한 사용자인지를 판단하는 기능을 제공한다.

III. Kerberos

Kerberos는 MIT 대학에서 Athena 프로젝트의 일환으로 개발된 분산 환경에서의 개체(사용자) 인증 서비스로 아래와 같은 보안 위협에 대처하는 방안을 제공한다[4].

- 불법 사용자가 특정한 서버에 접속한 후, 합법적인 사용자인 것처럼 위장할 수 있다.
- 불법 사용자가 자신의 워크스테이션의 네트워크 주소를 합법적인 주소로 변경하여 서버에게 서비스 요구를 신청할 수 있다.
- 불법 사용자가 합법적인 사용자와 서버 사이의 통신 정보를 도청하여 재전송 공격(replay attack)이나 합법적인 사용자의 작업을 방해할 수 있다.

Kerberos는 사용자와 서버 사이의 인증 서비스를 중앙 집중식 인증 서버를 통해 제공한다. 대부분의 인증 프로토콜들이 공개키 암호 방식을 사용하는데 반해, Kerberos는 대칭키 암호 방식을 사용하고 있다. 일반적으로 두 가지 버전의 Kerberos가 사용되고 있는데 Kerberos 버전 4가 가장 널리 사용되고 있으며, 버전 5는 버전 4의 보안 결함 몇 가지를 수정하였고 인터넷 draft 표준(RFC 1510)으로 발표되었다.

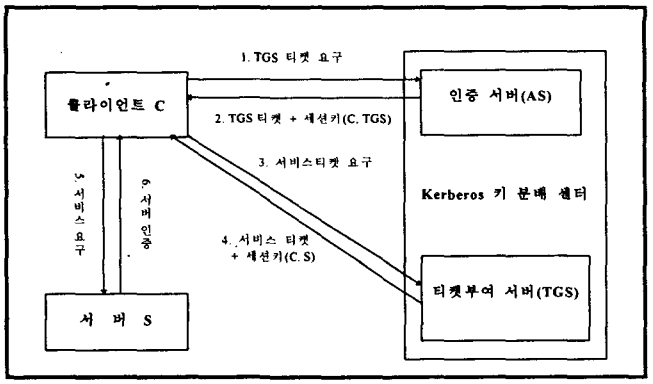

그림 1. Kerberos 개략

그림 1.은 Kerberos 시스템의 개략적인 구조와 인증 절차를 나타낸 것이다. 그림 1.에서 인증 서버는 사용자가 등록된 사용자인지를 검증하여 적법한 사용자인 경우 티켓 부여 서버로 접근할 수

있는 티켓을 발행한다. 티켓 부여 서버는 사용자가 접근하기를 원하는 서버가 이 사용자에 의해 접근 가능한지를 검증하여 접근이 허용된 사용자인 경우 서버로 접근할 수 있는 티켓을 발행한다.

Kerberos 시스템의 인증 절차는 다음과 같다. 사용자가 클라이언트 시스템에 로그온하면 클라이언트 시스템은 인증 서버(authentication server:AS)에게 인증을 요구한다(1). 인증 서버는 사용자가 적법한 사용자인지를 판단하여 적법한 사용자인 경우 티켓 부여 서버(ticket granting server:TGS)로 접근할 수 있는 티켓과 클라이언트와 티켓 부여 서버 사이의 세션키를 발행하여 클라이언트에게 전송한다(2). 티켓 부여 서버로 접근할 수 있는 티켓을 부여 받은 클라이언트는 실제 접근할 서버로의 접근을 허용받기 위해 티켓 부여 서버에게 서버로 접근할 수 있는 티켓을 요구한다(3). 티켓 부여 서버는 클라이언트가 보낸 티켓을 검증하여 유효한 티켓인 경우 서버로 접근할 수 있는 티켓과 클라이언트와 서버 사이의 세션키를 발행하여 클라이언트에게 전송한다(4). 서버로 접근할 수 있는 티켓을 얻은 클라이언트는 이 티켓을 가지고 서버에게 서비스를 요청한다(5). 서버는 클라이언트가 보낸 티켓을 검증하여 이 티켓이 유효한 경우 클라이언트에게 인증 확인 메세지를 보낸다(6).

그림 1.에서는 일반적인 Kerberos 구조와 인증 절차를 보여주고 있다. Kerberos 시스템은 두 개 이상의 영역(realm)으로 구성할 수 있으며 각 영역은 하나의 인증 서버와 티켓 부여 서버를 가진다. 일반적으로 영역은 동일한 관리 단위 또는 동일한 조직 단위로 이루어진다.

IV. 전자 도서관에서의 사용자 인증 구조

전자 도서관 서비스가 초고속 정보 통신망에서 사용할 수 있는 응용의 하나로 자리잡기 위해서는 분산 환경을 기반으로 하여 개발 구축되어야 한다. 따라서 현재 이루어지고 있는 전자 도서관에 관한 많은 연구들이 분산 환경을 기반으로 하고 있다.

이 장에서는 Kerberos를 사용하여 전자 도서관 시스템에서의 사용자 인증하는 방법을 제안한다.

그림 2.는 Kerberos를 사용하여 인증 기능을 제공하는 전자 도서관의 한 개념도이다. 이 그림에서 사용자는 자신의 browser을 통하여 정보 제공자들에 대한 정보를 얻을 수 있다. 정보 제공자들은 여러 개의 전자 도서관 서버들과 연결되어 다양한 자료의 인덱스를 제공한다. 이 경우 사용자는 자신의 browser를 통해 특정 정보 제공자에게 접근하여 원하는 정보를 얻고자 할 것이다. 사용자가 정

보 제공자를 선택하면 선택된 정보 제공자는 사용자를 인증하기 위해 사용자 id와 사용자 암호를 요구할 것이다. 사용자가 자신의 id와 암호를 입력하면 사용자 browser는 자신의 사용자 id와 password (US)를 정보 제공자의 public key로 암호화(EUS)하여 이를 정보 제공자에게 전송한다. 정보 제공자는 자신의 private key로 사용자 정보의 암호를 풀어 사용자 id와 password를 알아낸 후 Kerberos의 인증 서버(AS)에게 사용자 인증을 요구한다. 접근이 허용된 사용자이면 사용자의 browser에 자료 제공 서비스를 할 수 있는 인덱스 또는 명령문 입력 기능 등을 제공한다. 정보 제공자의 사용을 허용받은 사용자는 최종적으로 자신이 얻기를 원하는 정보에 관한 인덱스를 제공 받을 것이다. 사용자는 자신의 browser을 통해 자신이 얻기를 원하는 자료를 정보 제공자에게 요청한다. 사용자의 자료 검색 요청을 받은 정보 제공자는 사용자가 원하는 자료를 제공하는 하나 이상의 전자 도서관 서버의 id를 가져온다. 전자 도서관 서버의 id를 얻어 온 정보 제공자는 Kerberos의 티켓 부여 서버(TGS)에게 서버로의 인증을 요구한다.

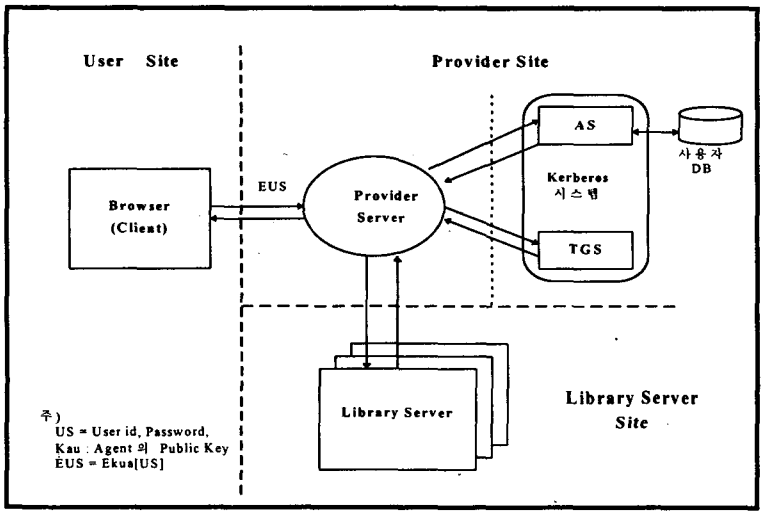

그림 2. 전자 도서관에서의 사용자 인증 방법

정보 제공자는 사용자 데이터베이스를 가지고 있으며 이 데이터베이스는 사용자와 서비스 제공자 사이의 계약 정보를 유지하고 있다. 이 정보는 서비스를 요구한 사용자에게 서비스 제공이 허락되어

있는지 만약 허락되어 있는 상태라면 어떤 전자 도서관의 사용이 허락되어 있는지 등의 정보를 유지하고 있어야 한다.

그림 2.에서 제시한 인증 방법은 특정 전자 도서관 접근 허용을 받은 사용자가 제한된 서비스만을 허용받을 때에도 사용할 수 있다. 이 논문에서는 1 단계 인증만을 언급하였다. 이를 확장하여 다단계 인증 기법을 도입할 수도 있으며 두 개 이상의 정보 제공자가 서로 정보 제공 계약을 맺고 사용자에게 정보를 제공하는 경우 등으로 확장 가능하다.

그림 2.에서 제시한 Kerberos를 이용한 사용자 인증 방법은 문서 서비스에 대한 사용료 지불, 저작권 보호 기술 등에서 요구되는 사용자 인증을 제공할 수 있다.

현재 Kerberos를 이용하여 HTTP(HyperText Transfer Protocol)에서의 인증 기능을 제공하는 연구가 이루어지고 있다[5]. 이러한 기능을 사용하여 전자 도서관 시스템에서의 인증 기능을 제공하는 방법도 있다.

V. 결 론

전자 도서관 시스템을 구축하기 위해서는 해결해야 할 많은 기술적인 문제점[1]들이 있다. 전자 도서관에서의 보안 문제도 이들 중의 한 문제로 제기되고 있다. 특히 정보 사용료 지불 문제, 저작권 보호 문제, 안전한 정보 제공 문제 등이 보안 기술과 밀접하게 연관되어 있다.

전자 도서관에서의 보안 기술은 사용자 인증 뿐만 아니라, 접근 제어 기능, 전달되는 문서의 진품 보장, 전달되는 문서의 무결성 보장, 사용자 privacy 보장 등 많은 분야에서 광범위하게 다루어져야 한다. 또한 문서 사용료 지불 기능, 저작권 보호 기능 등에서 사용될 수 있어야 한다.

참고문헌

[1] Edward A.Fox et al, "Digital Libraries", Communication of the ACM, p.27, 1995

[2] Steve B. Cousins, et al, "InterPay : Managing Multiple Payment Mechanisms in Digital Libraries", 1995, Available at http://www.csdl.tamu.edu/DL95/papers/cousins/cousins.html.

[3] Laura C. Anderson, Jeffrey B. Lotspiech, "Right management and security in the electronic library", IBM

research report, 1995.

[4] William Stallings, Network and Internetwork Security, Englewood Cliffs:Prentice Hall, 1995, pp.315-333

[5] "Kerberizing the Web", Available at http://snapple.ncsa.uiuc.edu/adam/khttp/intro.html