Kerberos를 이용한 전자상거래 인증시스템 디렉토리서버 구현에 관한 연구

심완보

충청대학교 컴퓨터학부 멀티미디어전공

Study on the directory server implementation using the Kerberos for the authentication system in the electronic commerce

Won-Bo Shim

Division of Computer, ChungCheong College

요 약

앞으로 전자상거래는 미국, 일본등 경제선진국을 중심으로 확대, 발전해 나갈 것이고 이에따라 이를 시스템적으로 지원할 수 있는 지불 시스템의 필요성은 더욱 부각될 것이다.

이 지불 시스템에서 핵심적인 기능은 인증기능이 될 것이고 인증에 대한 데이타를 관리하는 디렉토리 서버의 기능과 성능향상은 전체 지불시스템 더 나아가 전자상거래를 활성화 시키는데 절대적인 역할을 할 것이다. 이러한 현시점에서 세계 각국의 대응에 관심을 가지고 국내에서도 독자적인 기술로 국내 환경에 맞는 인증 시스템의 개발이 절실하게 필요한 때이다.

본고에서는 X.500시리즈와 MIT의 Kerberos Authentication System을 접목시켜 운용 가능한 전자상거래 모델을 제시하고 이를 구현시 고려해야할 사항들을 제시함으로 해서 향후 보안 및 전자상거래 관련 분야에서 급속한 수요 증가가 예상되는 디렉토리 서버구현을 위한 모델을 제시하고자한다.

1. 서론

날로 발전하는 컴퓨터와 통신분야의 기술발전으로 이미 종이가 없는 거래로 대변되는 전자상거래는 국내를 비롯하여 세계 경제선진국에서 시행되고 있고 우리 정부는 EDI 사업을 일찍부터 추진하여 무역업무 자동화 촉진에 관한 법률을 1991년에 제정하는 등 이 분야에 관하여는 선진국 대열에 접어들고 있다 할 수 있다.

전자문서는 시간과 노력, 비용의 절감면에서 탁월한 효과를 가지고 있으나 반면에 보안성 문제등 몇가지 단점을 노출하고 있다.

이를 보완하고자 나타난 것이 전자서명과 인증기관의 개념이다.

또한 인증기관의 출현은 전자문서에 대하여 종래 공증인이 수행하던 인증업무를 인증기관이 하게 된다는 것을 의미한다.

한편 인증기관의 국제화가 이루어질 경우 신용도가 높고 각국에 지점을 보유할 능력을 갖춘 미국등 선진국들의 거대 인증기관의 전횡도 우려되고 인증기관이 매번 전자 상거래 때마다 받는 수수료의 수입은 엄청날 것이다.

또한 국가기밀, 기업정보의 인증기관을 통한 누설

가능성이 높아 국가안보와 생존에도 영향을 미칠 것이다.

이렇듯이 전자상거래에 대한 인증기관의 인증업무 중요성은 분명하다 할 수 있다.

미국, 일본 등 경제 선진국에서는 이에 관한 연구와 전자상거래 분야에 대한 적용을 위해 다양한 노력을 하고 있으며 이미 일부 분야에서 적용 가능한 시스템을 내놓고 있다.

가까운 미래에 상거래중 많은 부분이 전자문서를 사용한 전자상거래로 변화 될 것임을 감안할 때 국내적으로도 이 분야에 대한 연구와 구현기술 확보는 국가 경쟁력 및 안보에 있어 대단히 중요한 의미를 갖는다 할 수 있다.

이에 이와 관련된 기술중 핵심적인 모듈인 디렉토리 서버를 이용한 인증 시스템 기술 확보를 위해 최근의 기술동향과 적용사례들을 통해 국내 디렉토리 서버 기술 확보를 위한 제반 사항을 연구하고 이를 구현하기 위해 인증 시스템을 위한 디렉토리 서버 시스템을 연구하고자 한다.

2 국내외의 연구개발 현황

인터넷의 사용자가 96년 11월을 기준으로 북아메리카(미국, 캐나다)에는 2-3천만명의 사용자가 있으며 나머지 국가에서 500만 내지 1천만명 정도의 사용자가 있는 것으로 추정된다. 따라서 전체적으로는 3-4천만명 정도의 사용자가 인터넷을 사용하고 있는 것으로 추정된다. 2000년에는 사용자가 2억명에 이를 것으로 전망되고 있다.

전자상거래 시장은 2천년께 6,579억 달러 규모로 급성장 할 것으로 전망돼 이를 선점하기 위한 각국의 경쟁이 치열해 지고 있다.

선두 주자인 미국은 94년 연방정부와 캘리포니아 주정부가 600만 달러를 투자, 전자상거래 연구를 위한 비영리기관인 커머스넷을 설립했다.

이 단체가 새로운 전자지불 방식을 시험하고 국제 표준 제정을 주도하고 있다.

일본의 경우 정부의 예산 지원을 받아 민간기구들이 전자상거래 관련 10개 프로젝트를 추진중이다. 일본정부는 일본전신회사(NTT)를 비롯, 64개 업체가 참여한 스마트아일랜드 컨소시엄(SIC)등 민간주도 전자상거래 컨소시엄을 활성화 하기 위해 적극적으로 투자하고 있다.선진 7개국도 초고속 정보통신 10여개의 프로젝트중 하나로 전자상거래 구축에 나서고 있다.

우리나라의 경우 전자상거래에 대한 연구와 활용이 아직 미흡한 실정이다. 현재 데이콤, 롯데백화점등 민간 기업과 국제정보 산업진흥 협회등이 전자상거래 구축의 걸림돌 제거를 위해 노력중이다. 한편 이러한 전자상거래를 활성화 시키는데 있어 중요한 문제는 안전한 대금결제이다. 서로 마주보고 하는 일반 상거래와는 달리 인터넷이라는 망을 통해 거래해야 하는 특수성 때문에 대금결제를 책임져줄 기관이 필요한데 일정의 수수료를 받고 대금결제에 따른 제반문제를 해결하게 되는데, 이와 같은 역할이 미래의 전자상거래에 필수적이라 보고 이를 준비하는 기업이 증가하고 있다. 안전한 대금결제 시스템에 반드시 필요한 기능으로는 거래에 임하는 당사자들에 대한 신분확인이다. 인증을 위한 방법은 여러 가지가 있지만 전자상거래에서의 인증을 위해 가장 적합한 것은 디렉토리 서버를 이용한 ISO의 X.509라 할 수 있다. 이에 대한 표준화를 위해 이미 국제적 표준으로 ISO의 디렉토리 서버(X.500)와 이를 이용한 인증 시스템(X.509)의 표준 규정안이 마련되어 있다. X.509를 이용한 인증 시스템의 구성요소로는 크게 CA(Certification Authority), 디렉토리 서버, 사용자를 들 수 있다. CA는 사용자의 공개키에 인증을 해주는 기관이며 디렉토리 서버는 CA가

발행하는 인증서와 인증서 취소 목록을 저장하고 있다가 사용자 또는 인증서를 필요로 하는 구성요소의 요청에 의해 특별한 확인과정 없이 해당하는 인증서를 전송하게 된다. 이러한 디렉토리 서버의 활용은 인터넷상의 인증 시스템에서 필수적인 요소라 할 수 있다. X.509는 (Table 1)과 같이 발전해왔다.

1988	X.509 v1
1993	X.509 v2, PEM(RFC 1422)
1994	ISO/ICE와 ANSI X9에서 X.509 v2 개선
1995.1	X.509 v3,인증서,v2 CRL에 대한 오류입안
1995.8	오류 입안 채택
1996.6	최종적인 X.509를 위한 표준 확장 (Standard extension) 개정

Table 1. Development of X.500

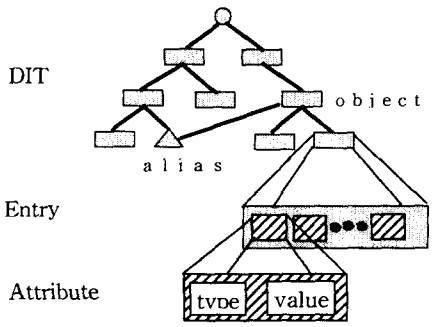
3. 연구개발의 세계적 수준

세계 각국에서는 전자상거래에서의 안전성과 신뢰성을 보장하기 위한 기반기술 확보에 많은 노력을 하고 있으며, 이런 노력은 정부 주도하에 이루어지는 것도 있지만 민간 부문에서도 기반 기술 확보를 위한 노력이 활발하게 이루어 지고 있다.

또한 기반기술 확보 뿐만 아니라 인증 서비스와 같은 유료서비스도 계획하고 있으며, 일부에서는 이미 유료서비스중에 있다. 이에 따라 전자상거래에서의 인증이 인터넷에서 중요한 사업항목으로 등장하고 있다.

각국의 인증기술 확보현황을 보면 미국의 표준기관인 NIST에서 CA의 자동개념, 기술적 명세서와 다른 CA와의 상호 연동서에 촛점을 맞추어 연구를 진행하고 있으며 미국 우정공사에서도 (Picture 1) 과 같은 DIT(Directory Information Tree)구조를 적용하여 인증서 등록, 검색, 취소를 할 수 있는 유료서비스를 준비하고 있다.

이에 RSA Data Security Inc, Verisign과 GTE가 연합하여 Cybertrust란 이름으로 전자상거래 분야의 인증 시스템 개발 및 서비스를 준비하고 있다. 이런 노력은 미국 뿐만이 아니라 캐나다 CSE의 GOC PKI, Certicom, 일본의 통산성, 일본 전자상거래 진흥협회(ECOM)과 유럽의 ICE-TEL, 영국의 우체국 공사에서도 활발하게 진행되고 있다.



Picture 1. DIT(Directory Information Tree)

4. Kerberos Authentication System과 디렉토리서버를 이용한 전자상거래 서비스 모델

1) Kerberos Authentication System 개요

Network환경에서 불법 침입자를 막는 방법으로 Firewall을 많이 사용하고 있다.

그러나 Firewall의 약점은 불법 침입자가 외부망으로 부터만 들어 온다고 가정하는 것인데 사실은 많은 보안 누출 사고가 대부분 내부에 있는 침입자에 의해 이루어 지고 있다는 것이다. 이러한 약점을 보완하기 위한 System을 만들기 위해 1983년 MIT가 주축이 되고 DEC과 IBM이 참가해 Athena Project를 시작했다. Kerberos 라는 단어는 원래 그리스로마 신화에 나오는 지옥의 문을 지키는 머리가 세개인 개를 말하며 Computer의 정보와 Resource를 지키는 상징으로 쓰여 졌다. Version 1, Version 2, Version 3는 MIT내부에서만 사용되어

졌고 이 System의 효용성이 알려 지면서 1987년 Version 4가 만들어 지기 시작했다. 이 Version 4는 MIT내부 뿐만이 아니라 외부에도 널리 쓰여지게 됐고 1989년 부터는 이 Version 4 사용시 나타났던 단점을 보완하기 위해 Version 5의 개발이 시작 되었다.

2) 제안된 Kerberos Authentication을 이용한 디렉토리서버 모델

Kerberos Authentication과 디렉토리 서버를 결합한 전자상거래에서의 제안된 모델은 다음 Picture 3 과 같다.

제안된 디렉토리서버 모델에서의 인증절차는 다음과 같은 순서로 이루어진다.

(1) Client가 AS에게 TGS를 위한 ticket을 요청한다.

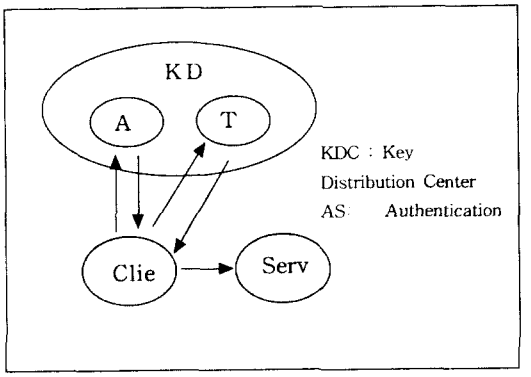
(2) AS는 Client에게 ticket-granting ticket 을 만들어 준다.

이에는 client의 identity와 session key의 copy가 포함되어 있다.

(3) Client는 TGS에게 message를 보내는데 이에는 target server의 이름, ticket-granting ticket, session key로 encrypt된 인증자(authenticator)가 포함 되어 있다.

(4) TGS는 client와 target server간에 필요한 새로운 session key를 생성하여 client에게 넘겨준다.

(5) Client는 target server에게 ticket을 보내 주게 되는데 이에는 TGS가 생성한 session key로 encrypt된 인증자가 포함된다.



Picture 2. Authentication

3) 디렉토리서버 구현시 고려사항

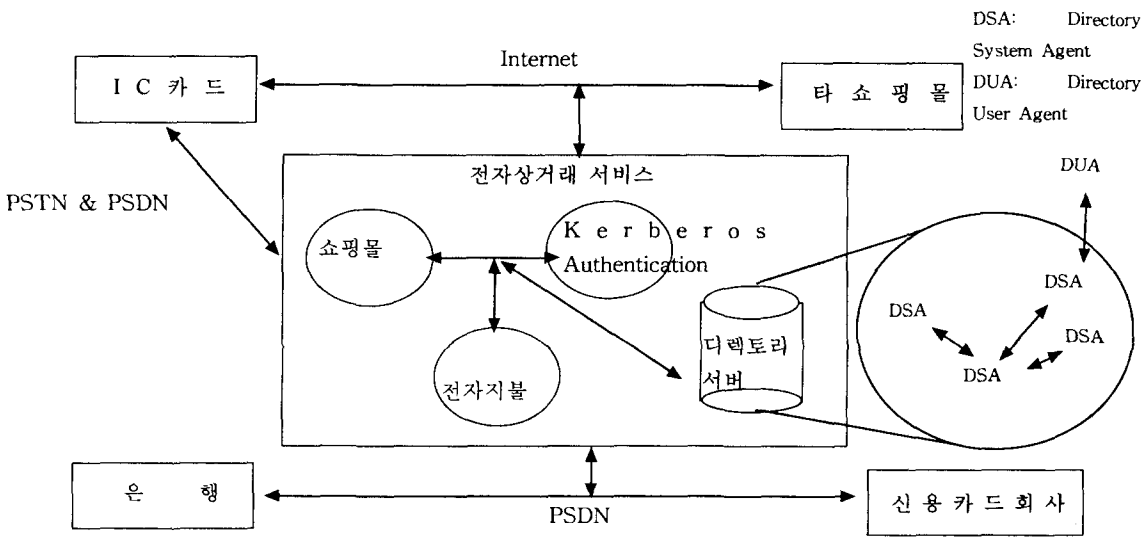
디렉토리서버를 구현함에 있어 실용성을 높이기 위하여 다음과 같은 요소들을 고려하여 구현해 나가는 것이 필요하다.

(1) X.500 시리즈는 전체를 일시에 구현하기에는 너무 복잡하므로 먼저 디렉토리서버를 이용해 인증 시스템을 구현하는데 있어 기본적으로 필요한 부분만을 먼저 구현하고 점진적으로 기능을 확장시켜 나간다.

(2) 개발된 디렉토리 서버를 이용해 전자상거래를 위한 인증뿐만 아니라 인터넷 메일과 뉴스를 위한 디렉토리 서버, 실시간 Audio, Data, Video통신 디렉토리서버, 사람과 자원에 관한 공공 저장용 디렉토리 서버, 전화번호 디렉토리 서버, 회사 및 캠퍼스용 디렉토리 서버의 용도를 고려한 시스템 설계가 필요하다.

(3) 디렉토리 서버를 이용해 자료검색시 사용자 위주의 편리하고 다양한 질의 검색 지원이 가능해야 한다.

(4) GUI 및 멀티미디어 기반의 사용자 인터페이스로 디렉토리 서버 운용의 용이성이 제고 되어야 한다.



Picture 3. A Model of electronic commerce using directory server

(5) 객체지향 개념의 객체 클래스 채택으로 수정 및 확장의 용이성 제공되어야 한다.

(6) 검색속도 향상을 위해 다음과 같은 아키텍처 및 기반기술이 활용되어야 한다.

- SMP(Symmetric Multiprocessor)지원으로 성능 향상
- 검색속도 향상을 위한 인덱스 서버 채용
- 분산형 디렉토리 서버 구현
- Scalable한 디렉토리 서버 구현

5. 결 론

앞으로 전자상거래는 미국, 일본등 경제선진국을 중심으로 확대, 발전해 나갈 것이고 이에따라 이를 시스템적으로 지원할 수 있는 지불 시스템의 필요성은 더욱 부각될 것이다.

이 지불 시스템에서 핵심적인 기능은 인증기능이 될 것이고 인증에 대한 데이타를 관리하는 디렉토리 서버의 기능과 성능향상은 전체 지불시스템 더 나아가 전자상거래를 활성화 시키는데 절대적인 역할을 할 것이다. 이러한 현시점에서 세계 각국의 대응에 관심을 가지고 국내에서도 독자적인 기술로 국내 환경에 맞는 인증 시스템의 개발이 절실하게 필요한 때이다.

본고에서는 X.500시리즈와 MIT의 Kerberos Authentication System을 접목시켜 운용 가능한 전자상거래 모델을 제시하고 이를 구현시 고려해야할 사항들을 제시함으로 해서 향후 보안 및 전자상거래 관련 분야에서 급속한 수요 증가가 예상되는 디렉토리 서버구현을 위한 모델이 될 수 있으리라 생각 된다.

인증 시스템의 주요 구성요소인 디렉토리 서버의 개발에 따라 다른 구성 요소와의 연동을 통해 국내 환경에 적합한 인증 시스템 구축에 활용되고, 이를 전자상거래에 적용하면 안전한 전자상거래 운영을 통해 인터넷사업에서의 신규 고부가가치

서비스가 개발되고
인증서 및 여러가지 다른 정보의 저장, 검색을 위한 시스템으로 상품화가 가능하게 될 것이다.

[참고문헌]

1. S.P. Miller : B.C. Neuman, Project Athena Technical Plan Section E.2.1, Oct 1988
2. G.R. Johnson : C.L. Athey, Final report and recommandations of the Esnet authentication pilot project, 1995
3. Edward G. Amoroso : Fundamentals of computer security technology, 1994
4. Larry J. Hughes : Actually useful internet security technique, 1995
5. 암호기법, 정보과학회지, 1997. 4
6. 심영철 : 인터넷 인증기술, 제3회 한국 전산망 보안기술 워크숍 발표자료집, P95 ~ 122, 1997. 5
7. 강창구 : 전자화폐기술, 제3회 한국 전산망 보안기술 워크숍 발표자료집, P141 ~ 160, 1997. 5
8. 류재철 : Certificate Authority, 제1회 한국통신 인터넷 보안 워크샵, P103 ~ 118, 1997.10
9. 권도균 : 한국적 전자 상거래 테스트베드 구축 협의회 http://madang.dacom.co.kr/dgguen/payment/summary.html, 1996
10. Information technology, Open Systems Interconnection
    The Directory : Overview of Concepts, Models and Services Recommendation X.500, ISO/IEC 9594-1
11. Information technology, Open Systems Interconnection
    The Directory : Authentication Framework Recommendation X.509, ISO/IEC 9594-8
12. Information technology, Open Systems Interconnection
    The Directory : Protocol Specifications Recommendation X.519, ISO/IEC 9594-5
13. Information technology, Open Systems Interconnection
    The Directory : Selected Object Classes Recommendation X.521, ISO/IEC 9594-7
14. http://www.contrib.andrew.cmu.edu/~shadow/kerberos/html
15. http://www.iso.ch/list2, 1997