通信情報保護論文誌
第9券 第2號 1999. 06

전자상거래에서 상점에 대한 신용 보증 시스템 구현

백 기영* · 손 기욱** · 신 기수** · 류 재철*

Implementation of a Credit Authentication System for Merchants in Electronic Commerce

Ki-Young Baek* · Ki-Wook Sohn** · KiSoo Shin** · Jae-Cheol Ryou*

요약

인터넷은 학술, 연구용으로 이용되었으나, 현재 일반사용자에게도 친숙한 World-Wide Web의 발달과 더불어 인터넷을 상업적으로 이용하려는 시도가 증가하고 있다. 인터넷의 상업적 이용으로 가장 큰 예는 인터넷 상점을 들 수 있다. WWW을 이용하여 물건을 광고하고 사용자는 자신이 원하는 물건을 선택하여 온라인으로 대금을 지불하는 형태이다. 이런 인터넷 상점이 증가함에 따라 고객과 상점사이에 서로의 신용도를 확인할 수 없는 문제점이 발생하게 되었다.

이 논문에서는, 인터넷 상점의 신용을 인정할 수 있는 시스템 개발에 대해 설명하고 있으며, 이를 통해 사용자가 인터넷 상점을 사용할 수 있는 믿을 수 있는 환경을 구축하려고 한다. 인터넷 상점에 대한 신용인증 시스템 개발을 위해서 상점의 신용정보는 사용자에게 안전하게 전송되어야 하며, 쉽게 확인할 수 있어야 한다. 또한 도청 될 수 없어야 한다.

Abstract

The Internet has been used as the academic, researching purposes. Nowadays, accordance with improving and being familiar with the World-Wide Web, Many people are giving it a try to use the Internet as commerce markets. The noticeable example of Internet-based use of the commerce is the Internet shopping mall.Using the WWW, companies exhibit their products and users select the ones and take the payment for ones in the on-line. Increasing the the Internet shopping mall, there needs to be the countermeasure that companies and clients must verify each other.

In this paper, there are explained the development credit authentication system of the Internet shopping mall and the construction of the trusted environment clients can use Internet shopping mall. That is to develop the credit authentication system the credit-rating of Internet shopping mall can be sent securely and easily to clients and the information of credit-ranting cannot be eavesdropped.

Keyword: credit, credit authentication, certificate, X.509, authentication

Ⅰ. 서론

현재 인터넷의 상업적 이용으로 가장 큰

이 논문은 충남대학교 소프트웨어연구센터의 지원에 의해서 연구되었음
* 충남대학교 컴퓨터과학과(cloud@home.chungnam.ac.kr), (jcryou@esperosun.chungnam.ac.kr)
** 한국전자통신연구원 (kiwook@etri.re.kr), (ksshin@etri.re.kr)

예는 인터넷 상점을 들 수 있다. WWW을 이용하여 물건을 광고하고 사용자는 자신이 원하는 물건을 선택하여 온라인으로 대금을 지불하는 형태이다. 이런 인터넷 상점이 증가함에 따라 고객과 상점사이에 서로의 신용도를 확인할 수 없는 문제점이 발생하게 되었으나 대부분의 인터넷 상점에서는 고객에 대한 인증을 함으로써 이런 문제점을 해결하려는 노력을 하고 있다. 고객이 정당한 고객인가, 신용 카드 만기일은 지나지 않았나 하는 것에 초점을 맞추어 진행하고 있다. 그러나 인터넷 상점의 증가에 따라 대금을 지불하고도 물건을 받지 못하는 사례가 증가하고 있고, 고객의 신용 카드 번호 유출 및 구매 정보, 더 나아가서 개인 정보를 타 회사에 매매하는 경우도 발생하고 있다. 이에 따라 현재까지 고객 인증 중심에서 이제는 상점의 신용 인증에 대한 관심이 증가하고 있다.

요즈음 이런 요구가 증가하면서 TRUSTe와 ICSA (International Computer Security Association)와 같이 WWW 서버에 대한 신용 보증을 해 주는 기관이 생겨나고 있다. TRUSTe는 EFF(Electronic Frontier Foundation)와 CommerceNet에서 설립한 비영리 기관이며, WWW 서버의 개인 정보 유출에 관한 신용 보증을 해 주는 기관이다. TRUSTe의 보증 서비스를 받고자 하는 상점은 비용으로 500 ~ 5000달러를 지불해야 하는데, 상점의 크기, 제공하는 정보에 따라 비용이 각기 달라진다[1].

TRUSTe에서 보증해준 WWW 서버는 자신들의 WWW 페이지에 (그림 1)과 같은 보증 마크를 사용하게 되는데, 이 보증 마크는 WWW 페이지에 보여지는 단순한 이미지이기 때문에 다른 서버에서 쉽게 도용할 수 있다. TRUSTe에서는 보증 마크의 도용을 막고자 두가지 방법을 제시하였다. 첫번째로 보증해준 WWW 서버에서 제공하는 모든 보증 마크를 TRUSTe의 웹 사이트에 연결시켜 놓아 고객이 보증 마크를 클릭하면 WWW 서버의 신용도에 관해 설명해 놓은 TRUSTe 사이트에 연결되어 고객이 이를 직접 확인할 수 있게 하였다. 두번째로 TRUSTe의 웹 사이트에 자신들이 보증해준 모든 상점의 리스트를 올려 놓아 고객이 이를 비교할 수 있게 하였다. 그러나 이 두 방법 모두가 고객이 상점에 접속하여 상점에서 제시하는 TRUSTe의 보증 마크를 보고 TRUSTe에서 보증해 주었다는 것을 바로 확인할 수 있는 방법이 아니라, 보증 마크를 클릭하여 TRUSTe의 WWW 사이트에 연결되는가를 확인하거나 TRUSTe에서 제공하는 상점의 리스트와 비교해 보는 것과 같은 부가적인 노력을 요구하는 문제점이 발생하고 있다.

그림 1 TRUSTe의 보증 마크
(Fig. 1) The credit mark of TRUSTe

그림 2 ICSA 보증 마크
(Fig. 2) The credit mark of ICSA

한편, ICSA는 WWW 서버가 보안 측면에서 안전하게 관리되고 있는 지에 관해 보증 서비스를 제공하고 있다[2]. 어떤 기관이 ICSA의 보증 받기를 신청하면 ICSA는 90일간 검사를 하여 요구 조건에 만족하면 WWW 서버에 (그림 2)와 같은 보증 마크를 사용할 수 있도록 한다. 또한 WWW 서버가 안전하게 관리되고 있는지

일년을 주기로 계속적으로 검사하고 있으나, 보증 마크를 위조하는 경우에 대한 대비책이 전무한 상태이다.

본 논문에서는 인터넷 상점에서의 신용을 보증할 수 있는 인터넷 등급 서비스를 설계함으로써 사용자가 인터넷을 이용하여 전자상거래를 행할 경우 믿을 수 있는 인터넷 상점을 선택할 수 있는 환경을 구축하고자 한다. 이를 위하여 제 3기관에서 상점의 신용도에 대해 등급을 설정하고 설정한 등급을 전자서명을 이용하여 등급 보증서로 만들어 이를 상점에 배포해 사용자가 상점에 접속할 때 이를 확인할 수 있게 하는 신용 보증 방법을 구현하였다.

이는 현재 다른 기관에서 단지 등급 정보만을 상점에 주어 등급에 대해 위조가 가능한 문제점과 보증해준 상점의 리스트를 유지하고 이를 사용자가 확인하게 하는 등의 등급 확인의 복잡한 문제점을 해결한 것으로 상점에 배포된 보증서는 위조가 불가능하며 사용자가 브라우저를 이용하여 상점에 접속하면 등급의 유효성 검사를 비롯한 모든 과정을 플러그인에서 자동으로 처리해 줌으로써 사용자는 화면에 등급 정보가 출력되면 다른 확인과정 없이 이를 신뢰할 수 있게 된다.

신용 보증 시스템의 구축을 위해서는 신용 등급에 대한 보증서가 필요한데, 이러한 등급보증서는 사용자 인증에 사용되는 인증서를 수정하여 이용한다. 이에 따라 2장에서는 X.509 인증서에 대해 분석하며, X.509 버전 3에서 새로 추가된 확장 필드의 형식과 표준확장필드로 정의된 필드들에 대해 알아본다. 3장과 4장에서는 이를 바탕으로 신용 보증 시스템의 전체 구성 및 각각의 구성 요소의 기능에 대해 정의하고, 이들 구성 요소 사이에 메시지 흐름을 설계한다. 또한 설계를 바탕으로 신용 보증 시스템의 구현에 필요한 사항들에 대해 알아보며, 4장에서 결론을 맺도록 한다.

II. X.509

X.509는 ITU-T(International Telecommunication Union - Telecommunication Standardization Sector)에서 정의한 X.500 디렉토리 서비스에서 서로간에 인증을 위해 개발되었다[3]. X.509의 인증 방식은 인증서(Certificate)가 기반이 되며, PEM(Privacy Enhanced Mail), PKCS(Public Key Cryptography Standard), S-HTTP(Secure HTTP), SSL(Secure Socket Layer), S-MIME(Secure MIME)등에서 지원된다.

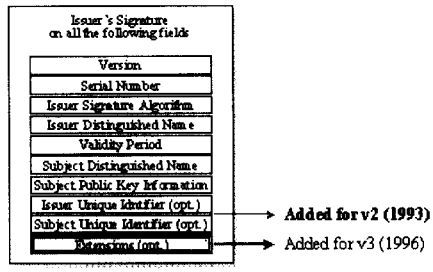


그림 3 X.509 인증서 형태
(Fig. 3) The format of X.509 certificate

X.509는 1988년에 버전 1이 발표된 뒤 계속적으로 수정 보완을 거쳐 현재 버전 3까지 발표되었으며, X.509 인증서는 기본적으로 필요한 CA 정보와 사용자 정보, 사용자의 공개키에 CA가 서명을 붙인 것으로 형태는 (그림 3)과 같다

X.509 인증서의 역할은 CA가 사용자의 공개키를 인증해 주는 것으로 이 공개키에 해당하는 소유주의 신원을 명확하게 하는 것을 주 목적으로 하고 있다.

X.509 인증서 버전 2와 버전 3의 가장 큰 차이점은 확장 필드(extensions)가 추가되었다는 것이다. 확장 필드로 인하여 X.509 인증서에도 좀 더 유동적으로 부가적인 정보를 넣을 수 있게 되었으며, X.509 버전 3에서는 많이 사용되는 정보들

을 표준 확장 필드로 정의해 놓았다. 또한 양자간이 동의하는 환경에서 새로운 확장 필드를 정의해서 사용할 수 있다. 이를 이용하여 본 논문에서 제시하는 신용 보증 시스템에서는 신용 정보를 보증할 수 있도록 설계하였다. 등급 설정기관에서는 상점에 대해 등급 설정을 하고, 이 정보를 X.509 인증서의 확장 필드 부분에 넣어 보증서를 발행함으로서 X.509 인증서를 등급 정보를 보증해 줄 수 있는 보증서의 역할을 하도록 설계하였다.

III. 상점에 대한 신용 보증 시스템 설계 및 구현

1. 전체 시스템 흐름도

각각의 구성 요소간의 전체 시스템의 대략적인 흐름은 (그림 4)와 같다.

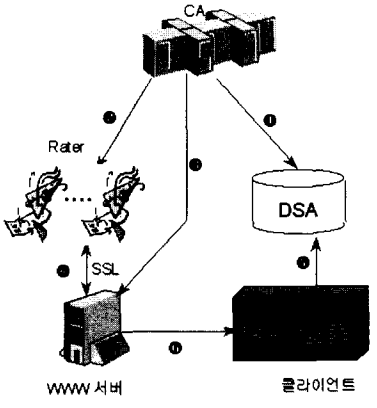


그림 4 전체 시스템 흐름도
(Fig. 4) The process of credit authentication system

1. CA의 인증서를 DSA에 등록한다.
2. 각각의 Rater에 대해 CA가 인증서를 발행해 주고 발행한 인증서를 DSA에 등록한다.
3. Rater와 WWW 서버사이에 SSL을 이용한 통신을 위하여 CA는 WWW 서버에 대해 인증서를 발행해 주고 발행한 인증서를 DSA에 등록한다.
4. WWW 서버가 Rater에 등급 설정을 요청하고 Rater는 요청에 따라 등급을 설정해 준다.
5. 인증서 관리 클라이언트는 등급 설정의 유효성 검증시 사용할 Rater의 인증서를 DSA로부터 가져와 저장하며 주기적으로 갱신한다.
6. 유효성 검사 플러그인은 WWW 서버로부터 가져온 페이지 또는 서버에 대한 등급 설정을 검증하여 유효하면 등급 정보를 화면에 표시해 주고 유효하지 않으면 유효하지 않다는 메시지를 화면에 표시해 준다.

2. 시스템 구성요소

전체 시스템은 CA, Rater, WWW 서버, DSA(Directory Service Agent), 클라이언트와 같이 5개로 구성되며, 각각 구성 요소의 역할은 다음과 같다.

CA는 Rater, WWW 서버 및 자신을 위한 인증서를 발행한다. Rater에 대해 인증서를 발행하는 것은 Rater가 보증서를 발행할 때 서명을 하기 위해서이며, 이 인증서는 WWW 서버와의 안전한 통신을 위해서도 사용된다.

Rater의 주요 기능은 상점에 대한 신용 등급을 정하는 일이며, 하나 이상의 Rater가 존재 할 수 있다. 먼저 Rater에게 등급 설정 요청에 들어오면, 각각의 Rater는 자신에게 맞는 등급 기준을 가지고 있어 이 기준에 따라 상점의 신용을 평가하여 등급을 증명해 주는 등급 보증서를 발행하며, 이와 같은 일은 등급 보증서를 발행한 후에도 주기적으로 계속된다. Rater와 CA의 차이점은 CA는 상대방의 신원을 확인하고 이를 증명하는 인증서를 발행하는 반면에 Rater는 상점의 신용을 평가하고 이를 증명하는 보증서를 발행하는 역할을 한다는 점이다.

설정한 등급은 등급 보증서 형태로 상점

에 전달되며 등급 보증서는 X.509를 기본 형식으로 하고 있다. 등급 설정에 관한 정보는 보증서의 확장 필드부분을 이용하여 저장한다.

DSA는 인증서 관리 클라이언트의 요청에 의해 CA, Rater와 WWW 서버의 인증서를 전달해 주는 역할을 한다. X.500에서 정의된 DSA는 인증서를 검색하여 인증서 체인을 만드는 기능 등의 다양한 기능들이 있으며, 다른 DSA와도 DAP(Directory Access Protocol)을 이용하여 통신하여야 하는 등 복잡한 구조로 되어 있으나, 신용 보증에 사용되는 DSA는 인증서 관리 클라이언트의 요청에 따라 변경된 인증서를 갱신해 주는 최소한의 요구 사항만을 만족하는 DSA이다.

클라이언트는 인증서 목록을 관리하며 DSA로부터 주기적으로 인증서를 갱신하는 인증서 관리 클라이언트와 등급 보증서의 유효성을 검사하는 Netscape 플러그인으로 구성된다. 사용자가 Netscape 브라우저를 이용하여 상점에 접속하게 되면 상점으로부터 등급 보증서를 받게 되며, 플러그인이 상점으로부터 전달받은 보증서의 유효성을 검사하여 유효 여부를 화면에 출력해 주게 된다.

3. 개발 환경

Rater와 플러그인에 사용되는 암호화 모듈과 보증서 구성에 관련된 부분은 SSLeay 0.8.1을 사용하였다. <표 1>은 프로그램 개발시 사용된 운영체제와 언어를 기술한 것이다.

표 2 개발환경
<Table. 1> A development environment

개발환경 / 구성요소	개발	
	운영체계	언어
CA, Rater, DSA	Solaris 2.5	CGG 7.2
클라이언트	Win 95	VC++ 4.2

1) SSLeay

SSLeay는 호주의 Eric A. Young에 의해 만들어진 SSL 2.0 라이브러리이며, 버전 0.8.0이상은 SSL 3.0을 완벽하게 지원한다 [4]. SSLeay는 전적으로 SSL 프로토콜을 구현하기 위해 만든 것이지만, SSL 프로토콜을 구현하기 위한 암호화 라이브러리를 생성하고 있으며, 이 암호화 라이브러리에는 관용 암호방식, 공개키 암호방식, 해쉬 함수등이 포함되어 있고, X.509 인증서, PKCS, PEM등을 다룰 수 있는 함수도 포함되어 있다.

그러나 SSLeay는 SSL프로토콜을 위해 만든 패키지로서 SSL API는 비교적 명확하게 사용할 수 있도록 되어 있으나, 그 하부의 암호화 알고리즘에 대한 API는 설명이 충분치 못해서 SSL이외의 암호화 시스템을 만들기 위해서는 상당한 노력을 해야 가능하다.

이런 문제점에도 불구하고 SSLeay가 가지는 장점은 다음과 같다.

- 현재 사용되는 대부분의 암호화 방식이 구현되어 있다.
- X.509 버전 3 인증서를 발행하고 관리하는 함수를 제공한다.
- 공개용으로 특별한 라이센스 없이 사용할 수 있다.
- 암호화 라이브러리를 이용한 CA를 구현해 놓았다.
- 안전성을 인정받아 전 세계적으로 널리 사용되고 있다.

SSLeay는 처음에 UNIX용 라이브러리로만 만들 수 있었으나, 0.5.2부터는 Window NT와 MS-DOS로도 만들 수 있게 되었으며, 0.6.0부터는 Windows 3.1 DLL(Dynamic Link Library)으로도 만들 수 있게 되었다. 따라서 본 논문에서는 윈도우 기반의 플러그인이나 인증서 관리 클라이언트에서도 SSLeay 라이브러리를 사용하였다.

2) 플러그인

Netscape 플러그인 기술은 써드 파티(Third Party) 개발자나 사용자들에게 브라우저의 성능을 확장할 수 있게 하기 위해 만들어진 스펙이다[5]. 이러한 기술은 브라우저 환경안에서 특정한 MIME(Multipurpose Internet Mail Extensions) 타입의 데이터를 보여 주거나, 사용할 수 있도록 해준다. 또한 정보를 표시하거나 응용 프로그램 실행, 응용 프로그램 간의 통신을 하고, 다른 웹사이트와의 연결을 가능하게 한다.

Netscape Navigator는 프로그램이 실행될 때 Netscape의 Plugins 디렉토리에 있는 플러그인 모듈을 검사한다. 이때 각각의 모듈이 등록되고, 해당하는 MIME에 플러그인 실행 모듈을 설정한다. 그리고 특정한 MIME을 가지는 HTML 문서가 로드될 때 플러그인 프로그램으로 실행된다. MIME 타입과 더불어 플러그인 모듈을 구분지어 주는 것으로 화일 확장자가 있다. 따라서 기본적으로 플러그인을 정의해 줄 때는 MIME 타입과 화일 확장자를 같이 정의해 준다.

플러그인은 윈도우즈 DLL(동적인 모듈) 형태로 존재함으로 플러그인의 등록은 해당 DLL화일을 위와 같은 Plugins 디렉토리에 넣어 주면 된다.

4. CA (Certification Authority)

CA는 SSLeay에 기본적으로 구현되어 있는 CA를 이용하였으며, CA는 CA 자신을 인증하기 위해서 자체 서명한(Self-signed) 인증서를 발행한다. Rater를 위해 발행한 인증서는 DSA에 등록한다.

CA는 인증서 발행에 필요한 기본 값 및 적용하는 방침등이 설정되어 있는 config 화일을 가지고 있어, 인증서 발행시 특별히 정해 주지 않을 때에는 <표 2>와 같은 기본값이 사용된다. 기본적인 인증서의 유효기간은 1년이며, 해쉬 알고리즘으로는 MD5를 사용하고 인증서 발행에 있어서 신청한 Rater의 국가명과 CA의 국가명이 일치하지 않을 때는 인증서를 발행해 주지 않는다.

표 3 인증서 발행 방침
<Table. 2> The policy for issuing certificate

방침종류	기본 값
유효 기간	1년
기본 해쉬 알고리즘	MD5
국가명	일치해야 함

CA가 발행한 모든 인증서는 DSA에 저장되어, 사용자가 인증서를 필요로 하는 경우 DSA로부터 가져갈 수 있도록 하며, 인증서를 취소할 경우 CA는 DSA에 삭제 요청을 한다.

DSA에 저장할 인증서는 CA의 certs 디렉토리 밑에 있는 인증서들로 CA가 새로운 인증서를 생성할 때마다 certs에 보관할 뿐만 아니라, 전자우편 시스템을 통해 자동적으로 DSA에 전달할 수 있도록 구현하였다.

5. Rater

표 4 등급 보증서 설정 정보
<Table.3> The information contained in credit certificate

종류	의미
보증서 버전 (gradeVersion)	현재 값은 1
보증서 종류 (certificateType)	서버 등급 보증서
등급 정보 (gradeInfo)	상점의 등급에 관한 정보로 숫자로 표시된다
등급 정보 이미지 (gradeImage)	등급을 나타내는 이미지로 등급 정보와 함께 화면에 표시된다.
서버 URL (urlValue)	상점의 URL로 보증서가 설치된 상점의 진위 여부 판정을 위해 필요하다.

X.509 확장 필드를 이용하여 보증서에 첨가되는 부가적인 정보는 등급을 나타내는 등급 정보(gradeInfo), WWW 서버의

URL(serverURL), 등급 이미지(gradeImage)와 등급 이미지가 있는 URL(gradeImageURL)로 구성되며, 자세한 사항은 <표 3>과 같다.

보증서 발행

Rater도 CA와 마찬가지로 보증서를 발행할 때 적용되는 기본 값과 방침등을 참조하는 config화일을 가지고 있어 보증서를 발행할 때 이를 참조한다. 보증서 발행에 적용되는 기본 방침은 CA의 기본 방침인 <표 2>와 같으나 <표 4>에서와 같이 유효기간이 다르고 보증서를 위한 2가지가 추가되었다. 본 논문에서는 유효기간을 일단 3개월로 정하였으나, 필요에 의해 변경이 가능하다. 기본값들은 보증서 발행시 특별히 정해주지 않을 경우에 적용된다.

표 5 보증서 기본 방침
<Table. 4> The basic policy of a credit certificate

방침 종류	기본값
유효 기간	3개월
보증서 종류	서버 등급 보증서
보증서 버전	1

발행한 보증서는 CA와 마찬가지로 SSLeay에 구현되어 있는 데이터베이스를 이용하여 관리되며, 데이터베이스의 디렉토리 구조와 화일은 CA와 같다. 그러나 보증서의 관리를 위해 CA와는 다른 인덱스 화일을 사용하며, 인덱스 화일에 저장되는 필드는 <표 5>와 같다.

표 6 보증서 관리 인덱스 파일
<Table. 5> The index file for managing credit certificate

필드명	의미
SERIAL	보증서의 일련 번호. (하나의 Rater에서 발행한 보증서사이에는 중복되는 일련 번호가 존재하지 않는다.)
TIME	유효 만료 기일
NAME	서버의 DN

6. DSA (Directory Service Agent)

X.509 인증서에는 인증서의 유효한 기간을 나타내는 유효 기간이라는 필드가 있으나, 인증서의 유효기간 내에 사용자의 비밀키가 노출되거나 사용자의 소속이 달라져 인증서의 사용 권한이 없어지면 비록 인증서가 유효 기간내에 있더라도 인증서를 취소해야 한다.

X.509 인증서를 사용하는 시스템에서 인증서의 취소에 사용하는 방법은 다음과 같이 크게 두가지가 있다.

1. X.509 인증서 취소에 기본적으로 사용되는 방법으로 CRL을 이용하는 방법이 있다. CRL이란 취소된 인증서의 리스트로써 CA는 주기적으로 취소된 인증서들의 목록을 CRL이란 것으로 만들어 DSA에 저장해준다. 사용자가 인증서를 받았을 때 인증서의 유효성 검사를 위해 DSA로부터 CRL을 받아 인증서가 취소되었나를 확인해야 한다[3].
   - 이와 같은 방법은 CRL 자체의 데이터 크기가 크기 때문에 발생하는 트래픽이 많고, 인증서의 유효성 검사에 많은 시간이 걸리게 된다.
2. 요즘 한참 논의 되고 있는 온라인 유효성 검사 방법이다. DSA는 항상 유효한 인증서만을 저장하고 있으며, 사용자가 전자 서명된 문서를 받아 서명자의 인증서를 필요로 할 때 이를 DSA에 문의하여 인증서를 받아올 수 있으면 유효한 것이고 그렇지 않으면 취소된 것으로 받아들이면 된다[6].
   - 이와 같은 방법 또한 문제점이 있는데, 만약 사용자가 저녁에 메일을 받고 다음날 메일의 서명을 확인하려 할 때 서명자의 인증서가 밤사이 취소되었다 한다면 서명한 시각에는 인증서가 유효했지만 유효성 검사를 하

려는 시점에서는 무효한 인증서가 되고 만다.

본 시스템에서 Rater 인증서가 취소될 경우를 위해 두번째 방법을 변형하여 사용하였는데, 두번째 방법을 그대로 사용하지 않은 이유는 클라이언트에서 상점에 설치된 보증서의 유효성 검사시 DSA로부터 유효한 인증서를 가져오는 것으로 인증서의 유효성 검사를 수행한다면, 인증서의 유효성 검사를 실시간에 처리하는데 문제가 생길 수 있다.

사용자 입장에서 살펴보았을 때 상점에 접속하면 상점의 WWW 페이지가 브라우저를 통해 출력되고, 플러그인으로 구현되는 등급 설정에 해당하는 부분만 등급 설정의 유효성 검사를 위해 화면에 출력되는 것이 지연되게 된다. 이때 DSA로부터 유효한 인증서를 가져와서 유효성 검사를 한다면 유효성 검사 시간이 더 길어지게 되어, 사용자는 등급 설정 정보가 출력되는 것을 기다리지 못하고 다른 페이지로 가는 경우가 발생할 수도 있다. 따라서 보증서의 유효성 검사시 DSA부터 유효한 인증서를 가져오는 과정 대신에 인증서 관리 클라이언트 프로그램이 주기적으로 DSA로부터 유효한 인증서를 가져다 사용자의 하드디스크에 저장하는 방법을 사용함으로써 인증서의 유효성 검사 시간을 단축하였다.

위에서 설명한 인증서 취소 방법 중 첫번째 방법을 사용하지 않은 가장 큰 이유는 CRL이 발생시키는 트래픽의 양이 많으며, 빠른 시간 내에 보증서의 유효성 검사를 끝내어 그 결과를 화면에 출력해 주어야 하기 때문이다. 본 시스템에서 사용한 인증서 취소를 위한 방법이 CRL을 사용하는 방법보다 DSA에 접속하여 정보를 가져오는 횟수는 많으나 그 데이터의 양이 적으므로 발생시키는 트래픽의 양이 CRL이 발생시키는 트래픽의 양보다 적다.

또한 빠른 시간 내에 유효성 검사 결과를 화면에 출력시키기 위하여 클라이언트가 주기적으로 DSA로부터 CRL을 가져와 인증서의 유효성을 검사하는 방법을 사용할 수도 있지만, 이는 인증서의 유효성 검사 시간은 단축할 수 있으나 CRL 자체가 발생시키는 트래픽의 양은 주기적으로 DSA부터 CRL을 가져오는 만큼 증가하게 되는 문제점을 가지고 있다.

7. 클라이언트

1) 인증서 관리 클라이언트

인증서 관리 클라이언트는 상점에서 제공하는 등급 보증서의 유효성을 검사하기 위해 필요한 Rater의 인증서를 관리하며, 독립적인 프로그램으로 구현된다. 사용자는 먼저 DSA에 Rater 목록을 요청하여 DSA로부터 받은 Rater 목록에서 자신이 신뢰하는 Rater를 선택한다. 인증서 관리 클라이언트는 주기적으로 사용자가 선택한 Rater들의 인증서를 DSA로부터 가져와 갱신한다. 인증서 관리 클라이언트를 이용하여 Rater의 인증서를 주기적으로 갱신하는 목적은 2가지가 있다. 첫번째는 상점 등급 보증서의 유효성 검사 시간을 줄이기 위해서이며, 두번째는 사용자도 자신이 신뢰하는 Rater를 선택할 수 있게 하기 위함이다.

인증서 관리 클라이언트는 (그림 5)와 같이 갱신할 인증서 목록을 보여주며, 목록에 있는 인증서들은 설정한 값에 따라 주기적으로 DSA의 인증서와 비교하여 갱신되며 갱신할 목록에서 인증서를 삭제하려면 인증서를 선택하고 Delete 버튼을 누르면 된다.

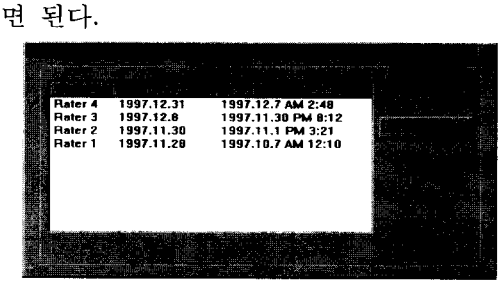


그림 5 인증서 갱신
(Fig. 5) Updating certificate

(그림 5)에서 갱신할 인증서 목록을 추가하기 위하여 Get List 버튼을 누르면, 인증서 관리 클라이언트는 DSA에 접속하여 DSA가 저장하고 있는 모든 인증서 리스트를 가져와 (그림 6)과 같은 인증서 추가 윈도우에 표시한다. 사용자는 DSA가 갖고 있는 전체 인증서 목록 중에서 추가하고자 하는 Rater의 인증서를 선택하고 Add 버튼을 누르면, 선택한 인증서가 인증서 갱신 목록에 추가되며 DSA로부터 주기적으로 갱신된다.

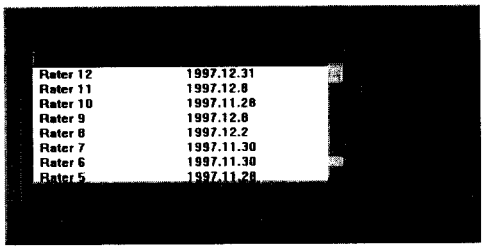


그림 6 인증서 목록 추가
(Fig. 6) Adding certificate list

앞에서 설명한 바와 같이 인증서 관리 클라이언트가 주기적으로 DSA에 접속하여 Rater의 인증서를 갱신하는 이유는 Rater 인증서의 취소 여부를 확인하기 위해서이다.

2) 유효성검사 플러그인

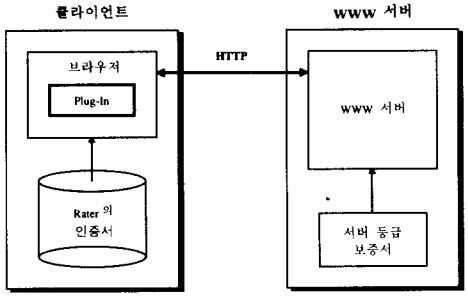


그림 7 시스템 개략도
(Fig. 7) The process between client and server

(그림 7)과 같이 유효성 검사 플러그인은 WWW 서버에서 전송되는 등급 보증서의 유효성을 검사하며, Netscape의 플러그인 기술을 이용하여 구현했다. 유효성 검사에 필요한 Rater의 인증서는 인증서 관리 클라이언트에 의해 미리 가져와 있다고 가정한다.

앞에서 살펴본 바와 같이 플러그인이 동작하기 위해서는 MIME 타입이 필요하며 상점의 신용보증을 위해 <표 6>과 같은 MIME 타입을 정의하였다.

표 7 신용보증 플러그인의 MIME 타입
<Table. 6> The MIME type of credit authentication plug-in

Key	Value
파일 확장자	mca
MIME 타입	Application/x-credit-plugin
FileOpenName	Merchant Credit Authentication(*.mca)
File Version	1,0,0,1

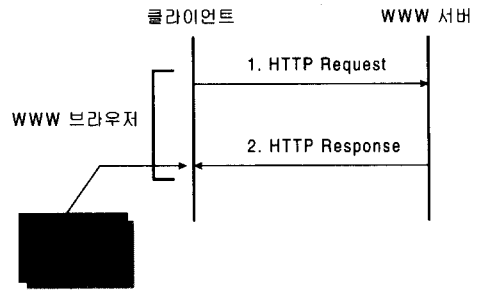


그림 8 서버-클라이언트
(Fig. 8) Server - client

서버별 등급 설정의 유효성 검사시 WWW 서버와 클라이언트 사이의 시스템 흐름도는 (그림 8)과 같다.

1. WWW 브라우저에 의한 HTTP Request
2. WWW 서버에 의한 HTTP Response
   - 전달되는 메시지 : Page ‖ 보증서
   - HTML의 <EMBED> 태그에 의해 플러그인이 load된다.
   - 보증서는 보증서 버전 ‖ 보증서 종류 ‖ 등급 정보 ‖ 등급 정보 이미지 ‖ 서버 URL ‖ SR[H(보증서 버전 ‖ 보증서 종류 ‖ 등급 정보 ‖ 등급 정보 이미지 ‖ 서버 URL)]로 구성되며, SR은 Rater의 전자서명을 의미한다.
   - 보증서의 유효성을 검사하기 위해서 먼저 저장하고 있는 Rater의 인증서

를 이용하여 Rater의 전자서명을 확인한다. 이 때 Rater의 인증서는 인증서 관리 클라이언트에 의해 주기적으로 갱신된 인증서이다. 따라서 사용자가 인증서 관리 클라이언트에서 선택하지 않은 Rater가 발행한 보증서는 유효성 검사에서 실패하게 된다.

- 두번째로 플러그인의 Live connect 기법을 이용하여 보증서가 표시되는 웹 페이지의 URL을 구해오며, 이 URL이 보증서에 들어 있는 URL로 시작되는지 검사하여 제대로 된 서버에 설치되었는지 검사한다.
- 세번째로 등급 보증서가 만료기일 전인가 검사한다.
- 세가지 모두 유효하면 보증서에 있는 등급 정보를 화면에 표시해 준다.

8. 인터넷 상점과의 연동

본 논문을 통해 구현된 신용 보증 시스템을 전자상거래의 한 상점과 연동하여 실증 실험을 수행하였으며, 이를 위한 보증서 설치와 브라우저에서의 보증서 유효성 검사 결과는 다음과 같다.

1) 상점에 보증서 설치

사용자는 보증서의 유효성 검사를 위해 Netscape의 플러그인을 이용하는데, 플러그인을 이용하여 보증서의 유효성을 검사하기 위해서는 상점에서 HTML문서의 <EMBED> 태그를 이용하여 보증서를 설치해야 한다. 상점의 보증서가 credit.mca라 할 때, 상점에서는 HTML문서에 (그림 9)와 같은 부분을 추가해 주면 된다.

```
<EMBED SRC="credit.mca" WIDTH=200 HEIGHT=200
TYPE="application/x-credit-plugin">
```

그림 9 상점의 보증서 설치
(Fig. 9) Installing a credit certificate of a merchant

2) 유효성 검사 결과

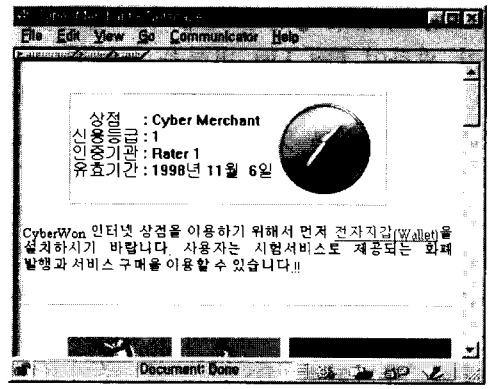


그림 10 보증서의 유효성 검사
(Fig. 10) The validation check of a credit certificate

사용자는 브라우저를 이용하여 상점에 접속한 후 상점이 제공하는 보증서가 유효한 경우 (그림 10)과 같은 화면을 보게 된다. 사용자가 브라우저를 통해 상점의 신용 등급과 그에 해당하는 이미지 및 다른 정보들을 본다는 것은 상점이 제공하는 등급 보증서가 유효하다는 것을 의미한다.

Ⅳ. 결론

인터넷을 이용한 물건의 구매 및 광고와 같은 전자상거래 시장은 해가 갈수록 기하급수적으로 늘어가고 있으며, 각국에서는 이들 시장에서 주도권을 잡기위해 많은 노력을 기울이고 있다. 더구나 백화점의 인터넷 상점과 같은 경우 전체수익에서 전자상거래가 차지하는 부분이 점차 증가함에 따라 많은 기업들 또한 전자상거래에 참가하려는 움직임이 증가하고 있다.

이와 같은 현실에서 주도적인 기술로 손꼽히는 것은 전자상거래 보안이다. 개인정보 및 신용카드 번호와 비밀번호 같은 정보가 네트워을 타고 상점에 전달되기 때문에 이를 안전하게 보호할 수 있는 방안이 커다란 이슈로 되고 있다. 그러나 이런 시점에서 간과할 수 없는 사항이 상점에

대한 신용이다. 현재 대부분의 인터넷 상점은 백화점과 같이 많은 사람들에게 알려진 상점이거나 또는 대기업이 주축이 되어 개설하는 경우가 많아서 일반인들이 믿고 사용하는 경우가 많지만, 외국에 있는 인터넷 상점과 거래하게 되거나 널리 알려지지 않은 기업에서 운영하는 인터넷 상점을 방문하게 될 때면 상점에 대한 신용을 한번쯤 의심하게 된다.

또한 E-mail을 통한 광고의 홍수 시대에 살고 있는 우리들에게는 자신의 정보를 상점에 공개한다는 것이 매우 꺼림직한 일이 되고 있다. 개인의 정보가 다른 기업에 공개됨에 따라 원치않은 광고 메일에 시달리는 일이 비일 비재하기 때문이다.

따라서 고객들이 접속하게 되는 상점에 대한 신용평가가 중요한 문제로 대두되고 있다. 우리가 방문하고 거래하고자 하는 상점이 얼마만큼의 신용을 가지고 있는 가에 대한 기준이 필요하게 된 것이다. 이는 고객이 상점에 제공하는 정보가 네트웍을 통해 다른 사람에게 노출되지 않고 안전하게 전달되는지, 대금을 지불하고도 물건을 못받게 될 경우는 없는지를 포함하여 고객이 상점에 제공한 정보가 어떤 용도로 사용되게 되는 지도 의미한다.

이와 같은 문제점을 해결하고자 본 논문에서는 전자상거래에서 상점에 대한 신용보증을 해 줄 수 있는 기반을 설계, 구현하였다. 제 3기관에서 상점의 신용도에 대해 등급을 설정하고 설정한 등급을 공개키 암호 기법을 이용하여 등급 보증서로 만들어 이를 상점에 배포해 사용자가 상점에 접속할 때 이를 확인할 수 있게 하였다. 이는 현재 다른 기관에서 단지 등급 정보만을 상점에 주어 등급에 대해 위조가 가능한 문제점과 인증해준 상점의 리스트를 유지하고 이를 사용자가 확인하게 하는 등의 등급 확인의 복잡한 문제점을 해결한 것으로 상점에 배포된 보증서는 위조가 불가능하며 사용자가 브라우저를 이용하여 상점에 접속하면 등급의 유효성 검사를 비롯한 모든 과정을 Plug-in에서 처리해 줌으로써 사용자는 화면에 등급 정보가 출력되면 다른 확인과정 없이 이를 신뢰할 수 있게 된다.

한편, 상점에 대한 신용 평가 뿐만 아니라 각각의 WWW 페이지에 대한 내용 확인 문제가 부각되고 있다. 중요 문서들이 WWW을 통해 제공되는 현실에서 사용자가 접한 WWW 페이지가 제대로 된 문서인지, 서버가 그 내용에 대해 부인하지는 않는지 등의 문제가 따르며, 문서의 내용에 따라서는 제 3자의 공증이 필요한 경우도 발생하고 있다.

본 논문에 의해 개발된 신용 보증 시스템은 이러한 문제를 해결하는데 사용될 수 있으며, 상점의 신용을 보증해 주는 용도 외에 상점의 체인점을 증명해 주는 형태로 활용될 수도 있어 다가올 전자상거래 시대에 중요한 역할을 수행할 것으로 예상된다.

참고문헌

[1] TRUSTe, Web Site Coordinators Guide, http://www.truste.org/join/guide.html, 1997

[2] NCSA, ICSA Certification Program, http://www.icsa.com/public/activities/certification.html, 1997

[3] ITU-T Recommendation X.509, The Directory : Authentication Framework, 1993

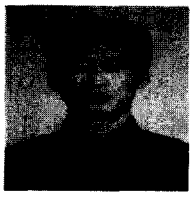
[4] Hudson, T.J., Young, E.A., "SSLeay and SSLapps FAQ", http://www.psy.uq.oz.au/~ftp/Crypto

[5] Netscape Corp., "The LiveConnect/Plug-in Developer's

Guide", http://www.netscape.com/eng/mozilla/3.0/handbook/plugins/index.html
[6] National Institute of Standards and Technology, A Public Key Infrastructure for U.S. Government Unclassified but Sensitive Applications, 1995

□ 著者紹介

백 기 영 **정회원**



1996년 : 충남대학교 컴퓨터과학과 졸업 (학사)
1998년 : 충남대학교 대학원 컴퓨터과학과 (석사)
1998년~현재 : 충남대학교 대학원 컴퓨터과학과 박사과정

〈관심분야〉 보안 프로토콜, PKI, LDAP

손 기 욱 **정회원**

1990년 2월 : 성균관대학교 정보공학과(학사)
1992년 2월 : 성균과대학교 정보공학과(석사)
1992년~현재 : 한국전자통신연구원 선임연구원

〈관심분야〉 통신망 정보보호, 암호 프로토콜

신 기 수 **정회원**

1975년 2월 : 서강대학교 전자공학과(학사)
1989년 2월 : 충북대학교 전자공학과(석사)
1977년~1980년 : 삼성전자
1980년~현재 : 한국전자통신연구원 책임연구원

〈관심분야〉 데이터 통신 정보보호, 네트워크 보안, 전자상거래

류 재 철 **정회원**

1985년 : 한양대학교 산업공학과(학사)
1988년 : Iowa State University 전산학과(석사)
1990년 : Northwestern University 전산학과(박사)
1991년~현재 : 충남대학교 컴퓨터과학과 부교수

〈관심분야〉 컴퓨터 및 통신망 보안, 전자상거래, 분산