전자상거래에서 상점에 대한 신용 보증 시스템 설계

백 기 영* · 손기욱** · 신기수** · 류 재 철*
* 충남대학교 컴퓨터과학과
** 한국전자통신 연구원

Design of Credit Authentication System for Merchant in Electronic Commerce

Ki-Young Baek* · Ki-Wook Sohn** · KiSoo Shin** · Jae-Cheol Ryou*
* Dept. of Computer Science, Chungnam National University
** Electronics and Telecommunications Research Institute

kybaek@esperosun.chungnam.ac.kr

요약

인터넷 상점을 이용하여 물건을 구매하는 방식이 쇼핑의 한 수단으로 자리잡고 있지만, 상점에 의한 고객의 신용 카드 번호 및 구매 정보등의 개인정보 유출이라는 심각한 문제가 부각되고 있다. 이와 같은 현실에서 물건을 구매하는 고객이 상점이 믿을 수 있는 상점인지를 판단할 수 있는 방법이 필요해지고 있다. 이에 본 논문에서는 상점에 대한 등급 정보를 X.509 인증서를 이용하여 배포하고, 고객이 브라우저를 이용하여 상점에 접속하였을 때 상점의 신용도를 편리하게 확인할 수 있는 시스템을 제안한다.

1 서론

현재 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 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 물건을 주문하여 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.

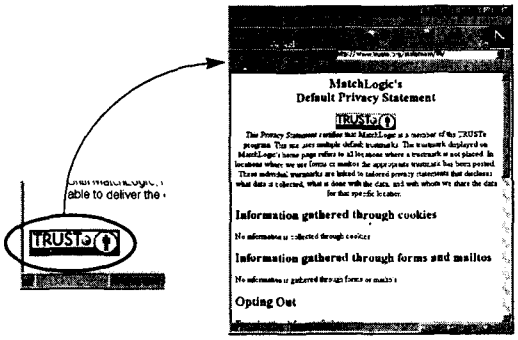
요즈음 이런 요구가 증가하면서 TRUSTe와 NCSA(National Computer Security Association)와 같이 WWW 서버에 인증을 해 주는 기관이 생겨나고 있다. TRUSTe는 EFF(Electronic Frontier Foundation)와 CommerceNet에서 설립한 비영리 기관이며, WWW 서버의 개인 정보 유출에 관한 신용 인증을 해 주는 기관으로 [표 1]과 같이 3가지 등급으로 나누어 관리한다. TRUSTe의 인증 서비스를 받고자 하는 상점은 비용으로 500 ~ 5000달러를 지불해야 하는데, 상점의 크기, 제공하는 정보에 따라 비용이 각기 달라진다[1].

TRUSTe에서 인증해준 WWW 서버는 자신들의 WWW 페이지에 [표 1]과 같은 인증 마크를 사용하게 되는데, 이 인증 마크는 WWW 페이지에 보여지는 단순한 이미지이기 때문에 다른 서버에서 쉽게 도용할 수 있다. TRUSTe에서는 인증 마크의 도용을 막고자 두가지 방법을 제시하였다. 첫번째로 인증해준 WWW 서버에서 제공하는 모든 인증 마크를 TRUSTe의 웹 사이트에 연결시켜 놓아 고객이 인증

마크를 클릭하면 WWW 서버의 신용도에 관해 설명해 놓은 TRUSTe 사이트에 연결되어 고객이 이를 직접 확인할 수 있게 하였다. [그림 1]과 같은 경우에 MatchLogic WWW 서버에서 제공하는 인증 마크를 클릭하면 TRUSTe의 MatchLogic WWW 서버의 신용도에 관해 설명해 놓은 사이트에 연결된다. 두 번째로 TRUSTe의 웹 사이트에 자신들이 인증해준 모든 상점의 리스트를 올려 놓아 고객이 이를 비교할 수 있게 하였다. 그러나 이 두 방법 모두가 고객이 상점에 접속하여 상점에서 제시하는 TRUSTe의 인증 마크를 보고 TRUSTe에서 인증해 주었다는 것을 바로 확인할 수 있는 방법이 아니라, 인증 마크를 클릭하여 TRUSTe의 WWW 사이트에 연결되는가를 확인하거나 TRUSTe에서 제공하는 상점의 리스트와 비교해 보는 것과 같은 부가적인 노력을 요구하는 문제점이 발생하고 있다.

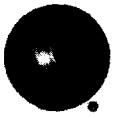
등급	의미
TRUSTe	고객의 정보를 암호 알고리즘을 이용하여 안전하게 전송 받으며, 수집된 고객 정보를 절대로 외부로 유출시키지 않는다.
TRUSTe	고객의 정보를 암호 알고리즘을 사용하여 안전하게 전송 받으며, 수집된 고객 정보를 고객 관리용으로만 사용한다.
TRUSTe	고객의 정보를 전송 받을 때 암호 알고리즘을 사용하지 않고, 또한 수집된 고객 정보를 외부에 유출시킬 수도 있다

[표 1] TRUSTe의 인증 등급



[그림 1] TRUSTe의 인증 마크 사용

한편, NCSA는 WWW 서버가 보안 측면에서 안전하게 관리되고 있는 지에 관해 인증 서비스를 제공하고 있다[2]. 어떤 기관이 NCSA의 인증 받기를 신청하면 NCSA는 90일간 검사를 하여 요구 조건에 만족하면 WWW 서버에 [그림 2]와 같은 인증 마크를 사용할 수 있도록 한다. 또한 WWW 서버가 안전하게 관리되고 있는지 일년을 주기로 계속적으로 검사하고 있으나, 인증 마크를 위조하는 경우에 대한 대비책이 전무한 상태이다.



[그림 2] NCSA 인증 마크

본 논문에서는 인터넷 상점에서의 신용을 보증할 수 있는 인터넷 등급 서비스를 설계함으로써 사용자

가 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 공개키 암호 기법을 이용하여 등급 보증서로 만들어 이를 상점에 배포해 사용자가 상점에 접속할 때 이를 확인할 수 있게 하는 신용 보증 방법을 설계하였다. 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.

신용 보증 시스템의 구축을 위해서는 신용 등급에 대한 인증이 필요한데, 이러한 등급의 인증은 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. 3장에서는 이를 바탕으로 신용 보증 시스템의 전체 구성 및 각각의 구성 요소의 기능에 대해 정의하고, 이들 구성 요소 사이에 메시지 흐름을 설계한다.

2 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.

X.509는 보안 응용 프로그램중 PEM에서 사용되었으나 암호화 통신을 하기 전 CA로 부터 인증을 받아야 하는 과정과 믿을 수 있는 CA가 존재하지 않는 점, 구성의 복잡함등 많은 문제점이 제기되었다. 따라서 사용자 서로가 인증을 해 주는 방식인 PGP(Pretty Good Privacy)가 사용의 편리함 때문에 널리 사용되게 되었다. PGP에서는 사용자가 모르는 사람의 키를 받았을 때 키에 첨가된 서명을 보고 자신이 믿고 있는 사람이 서명을 하였으면 지금 받은 키를 믿고 사용하고, 그렇지 않을 때에는 경고메시지를 보여 준다. 또한 부분적으로 신뢰하는 두 사람 이상이 키에 서명을 함으로써 키를 믿고 사용할 수도 있다. 따라서 CA와 같은 기관이 없어도 PGP에서는 상대방의 키를 믿고 사용할 수 있는 환경이 구축되어 있다[4][5].

그러나 전자상거래가 확산됨에 따라 믿을 수 있는 기관에서 인증을 해 주는 것이 아닌 서로간에 인증을 해 주는 방식인 PGP인 경우 신뢰성 문제가 제기 되면서, X.509에 따른 인증 서비스가 주목을 받고 있다.

2.1 X.500 디렉토리 서비스의 구성 요소

X.500 디렉토리 서비스는 크게 CA(Certification Authority), DSA(Directory Service Agent), 사용자 이렇게 3개의 구성요소를 가지고 있다[6].

CA는 사용자 또는 다른 CA의 공개키를 인증하여 인증서를 발행하는 기관이며 계층적인 구조를 가지고 있다. 따라서 Root CA에서 CA의 공개키에 대해 인증을 하여 인증서를 발행해 줄 경수 Root CA를 믿는 사용자는 CA가 인증해준 인증서도 신뢰하게 된다.

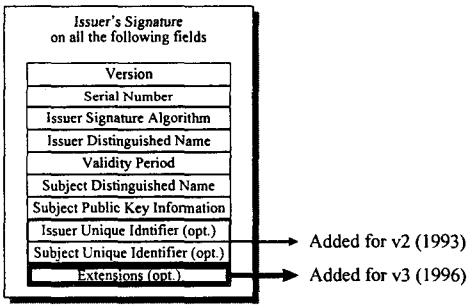
X.500 디렉토리 서비스의 기본 구성 요소는 아니지만 요즈음 그 중요성이 증가하고 있는 것으로 ORA(Organizational Registration Authority)가 있다. ORA는 CA와 사용자 사이에서 사용자의 신원을 증명해 주는 역할을 수행하고, CA는 ORA의 요청을 받아 인증서를 발급하는 역활을 담당한다. CA가 사용자에게 인증서를 발행해 주기 위해서는 먼저 사용자의 신원을 확인해야 하는데 인증문제가 중요해

지면서 신원확인 업무와 발급업무를 분리하려는 것이 보편적인 추세이다. 예를 들면 만약 어떤 은행에서 고객들을 위한 인증서 발급을 원할 때 고객 자신이 CA에 인증서를 신청할 경우에 자신의 신원을 증명하기 위해서 많은 서류를 제출하거나 복잡한 과정을 거쳐야 될 것이다. 그러나 은행이 CA를 대신하여 고객에 대한 신원확인 업무를 대신한다면 CA는 은행이 제시한 정보를 이용하여 별다른 확인 과정 없이 고객에 대한 인증서를 발행해 줄 수 있다. 기본적으로 은행에서는 고객에 대한 신원확인 업무를 하고 있으므로 CA에 고객에 대한 인증서 요청을 위하여 부가적인 신원확인 업무를 하지 않아도 되며, CA 또한 신원확인에 대한 부담이 줄어들게 된다.

DSA는 CA가 발급한 인증서를 보관하는 곳이다. 사용자는 안전한 암호화 통신을 하기 위해 상대방의 공개키를 검증해야 하는데 이때 상대방의 인증서가 필요하다. 필요한 인증서는 특별한 확인 과정 없이 DSA로 부터 가져올 수 있다. 이와 같이 사용자 또는 CA의 인증서를 CA가 배포하지 않고 DSA가 배포하는 이유는 CA가 통신 보안에서 굉장히 중요한 위치를 가지고 있기 때문이다. 사용자가 CA를 믿으면 그 CA에서 발급되는 모든 인증서를 믿게 된다. 따라서 CA가 임의로 인증서를 발급한다거나 CA의 비밀키가 유출되면 크게 혼란이 일어나므로 보안에 각별히 신경써야 한다. 따라서 CA는 네트워크를 통한 공격에 대비하기 위해 off-line으로 운영되어야 하며, 인증서는 DSA를 통해 배포된다.

2.2 인증서 (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



[그림 3] X.509 인증서 형태

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 필드는 확장 필드 이름, criticality flag, 확장 필드 값, 이렇게 3가지 요소로 구성되어 있으며, 여기에서 criticality flag는 확장 필드의 중요성을 의미하는 요소로서 사용자가 인증서를 검증하는 과정에서 criticality flag가 설정되어 있는 확장 필드를 인식하지 못하는 경우에는 인증서 자체를 무효하다고 판단하지만, criticality flag가 설정되어 있지 않는 확장 필드를 인식하지 못하는 경우에는 인식하지 못하는 확장 필드만 무시하고 다음 확장 필드를 검증한다. 표준 확장 필드로 정의 되지 않은 확장 필드는 criticality flag가 설정되어 있지 않은 것으로 간주한다.

확장 필드로 인하여 X.509 인증서에도 좀 더 유동적으로 부가적인 정보를 넣을 수 있게 되었으며, X.509 버전 3에서는 많이 사용되는 정보들을 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 인증할 수 있도록 설계하였다. 등급 설정기관에서는 상점에 대해 등급 설정을 하고, 이 정보를 X.509 인증서의 확장 필드 부분에 넣어 인증서를 발행함으로서 X.509 인증서를

등급 정보를 보증해 줄 수 있는 보증서의 역할을 하도록 설계하였다.

3 상점에 대한 신용 보증 시스템 설계

3.1 배경

현재 인터넷의 발전은 WWW의 발달에 기인한 거라 해도 과언이 아니다. 그만큼 인터넷 하면 대부분의 사용자들은 WWW을 생각하게 된다. 초창기의 WWW은 학교, 연구소등을 중심으로 구축되기 시작되다가, WWW 구축 열기는 기업에 까지 번지게 되었다. 그 결과 오늘날 WWW서버의 수는 헤아릴 수 없을 정도로 많아졌으며 지금도 꾸준히 증가하고 있다. 더구나 초창기의 학교, 연구소, 기업 중심이 아닌 심지어 동네에 있는 주유소의 WWW 서버가 있을 정도로 대중화 되고 있다.

이렇게 WWW 서버의 수가 증가함에 따라 많은 문제점이 발생하고 있는데, 그 중 하나는 접속한 서버를 믿을 수 없다는 점이다. 사용자가 의도한 서버에 정확히 접속하였는지, 그 서버에서 제공하는 서비스는 신뢰할 수 있는지, 개인 정보를 무단으로 유출하지는 않는지 등 사용자는 많은 의심을 가지게 된다. 이에 따라 제 3 기관에서 서버의 신용도에 대한 등급을 정해줄 필요성이 발생하였으나, 특정 기관에서 등급을 정해주었다는 것을 증명할 방법이 없으며, 서버에서 등급을 위조해도 이를 확인할 수 있는 방법이 없다.

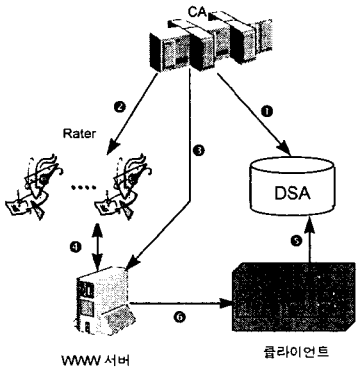
위와 같은 문제점을 해결하고자 본 논문에서는 공개키 암호 기법을 이용하여 제 3기관에서 등급 정보에 서명을 한 보증서를 WWW 서버에 배포하여 사용자가 상점에 대한 신용도를 알아볼 수 있게 하는 전자상거래에서 상점에 대한 신용 보증 시스템을 설계하였다.

3.2 시스템 구성요소

본 절에서는 제안하고자하는 시스템의 전체 구성 및 흐름에 대해 살펴 보고 각각의 구성요소의 특징, 기능에 대해 정의한다.

3.2.1 전체 시스템 구성 및 흐름

전체 시스템은 [그림 4]와 같이 CA, Rater, WWW 서버, DSA, 클라이언트등 5개로 구성되며, 전체 시스템의 대략적인 흐름은 다음과 같다.



[그림 4] 전체 시스템 구성 요소

1. CA의 인증서를 DSA(Directory Service Agent)에 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. WWW 서버로부터 가져온 페이지 또는 서버에 대한 등급 설정을 검증하여 유효하면 등급 정보를 화면에 표시해 주고 유효하지 않으며 유효하지 않다는 메시지를 화면에 표시해 준다.

3.2.2 CA (Certification Authority)

CA는 Rater, WWW 서버 및 자신을 위한 인증서를 발행하며, CA 자신을 위한 인증서는 자체 서명한 (Self-signed) 인증서이다. 발행한 인증서를 e-mail을 이용하여 DSA에 등록한다.

3.2.3 Rater

Rater는 상점에 대해 등급 설정을 해 주는 기관이며 하나 이상의 Rater가 존재 할 수 있다. 설정한 등급은 등급 보증서를 이용하여 상점에 전달되며 등급 보증서는 X.509를 기본 형식으로 하고 있다. 등급 설정에 관한 정보는 보증서의 확장 필드(extensions) 부분을 이용하여 저장한다.

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 구성되어 있다.

3.2.4 DSA (Directory Service Agent)

인증서 관리 클라이언트의 요청에 의해 CA, Rater와 WWW 서버의 인증서를 전달해 주는 역확을한다. X.500에서 정의된 DSA는 인증서를 검색하여 인증서 체인을 만드는 기능등의 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.

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.509에서 인증서 취소는 CRL(Certificate Revocation List)을 이용한다. CRL이란 취소된 인증서의 목록을 의미하며 CA는 주기적으로 CRL을 DSA에 등록하여 사용자가 인증서의 유효성 검사를 할 때 DSA로부터 CRL을 가져와 비교할 수 있게 한다.

본 시스템에서는 X.509를 기본 인증서를 사용하지만 인증서의 취소는 CRL을 이용하지 않고 DSA에 항상 유효한 인증서만을 저장해 놓고 클라이언트에서 주기적으로 인증서를 갱신하여 인증서의 취소 여부를 확인하는 유효기간이 짧은 인증서 방법을 사용한다. CRL을 이용하지 않고 이와 같은 방법을 사용하여 인증서의 취소 여부를 확인하는 이유는 클라이언트에서 유효성 검사시 DSA로부터 CRL을 가져와 인증서의 유효 여부를 검사한다면, 클라이언트에 유효한 인증서를 가져다 놓고 유효성 검사를 하는 것보다 더 많은 시간이 소요되게 된다. 사용자 입장에서 살펴보았을 때 상점에 접속하면 상점의 WWW 페이지가 브라우저를 통해 출력되고, Plug-in으로 구현되는 등급 설정에 해당하는 부분만 등급 설정의 유효성 검사를 위해 화면에 출력되는 것이 지연되게 된다. 이때 CRL을 이용하여 등급 설정의 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 유효성 검사시 시간을 단축하기 위해서 CRL을 사용하지 않기로 하였다.

3.2.5 클라이언트

클라이언트는 인증서 목록을 관리하며 DSA로부터 주기적으로 인증서를 갱신하는 인증서 관리 클라이언트와 등급 보증서의 유효성을 검사하는 Netscape Plug-in으로 구성된다.

인증서 관리 클라이언트는 WWW 서버에서 제공하는 등급의 유효성을 검사하기 위해 필요한 Rater 및 WWW 서버의 인증서를 관리하며, 독립적인 프로그램으로 구현된다. 사용자는 먼저 DSA에 인증서 목록을 요청하여 DSA로부터 받은 인증서 목록에서 자신이 필요로 하는 Rater의 인증서를 선택한다. 인증서 관리 클라이언트는 주기적으로 사용자가 선택한 인증서들을 DSA로부터 가져와 갱신한다. 사용자가 주기적으로 갱신되는 인증서를 추가 또는 삭제하기를 원한다면 인증서 관리 클라이언트를 이용하여 다시 DSA에 인증서 목록을 요청하고 DSA로부터 받은 인증서 목록에서 자신이 필요로 하는 Rater의 인증서를 추가 또는 삭제하면 된다.

Netscape Plug-in은 WWW 서버에서 제공하는 등급의 유효성을 검사하며, Netscape의 Plug-in으로 구현된다. 유효성 검사에 필요한 인증서는 인증서 관리 클라이언트에 의해 미리 가져와 있다고 가정한다.

3.2.6 WWW 서버

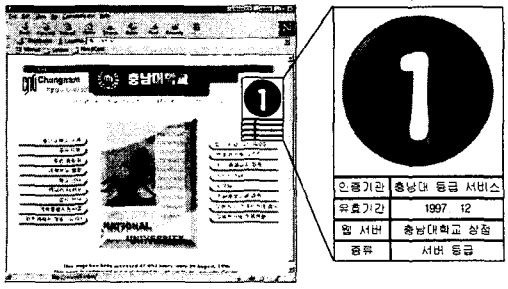
Rater로부터 받은 등급 보증서를 이용하여 WWW 서비스를 해 주는 곳이며, 서버 또는 페이지에 대해 하나 이상의 Rater로 부터 등급 설정을 받을 수 있다. 각각의 서버는 SSL을 이용한 Rater와의 안전한 통신을 위하여 CA로부터 서버의 공개키에 대해 인증서를 받아야 한다.

3.3 시스템 흐름도

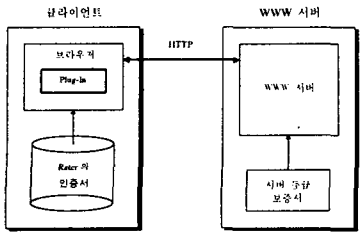
3.3.1 WWW서버 - 클라이언트

Netscape을 이용하여 서버 등급이 설정된 상점에 접속하면 사용자는 [그림 5]와 같은 화면을 볼 수 있다. Netscape의 오른쪽 위 부분에 작게 보여지는 부분이 서버에 인증된 등급을 표시해 주는 부분이며 페이지의 어느 곳이나 위치할 수 있다. 오른쪽에 보여지는 것은 등급을 확대해 보인 것이며 인증 기관, 등급의 유효 기간, 상점의 이름, 등급의 종류와 등급에 해당하는 이미지등이 표시된다.

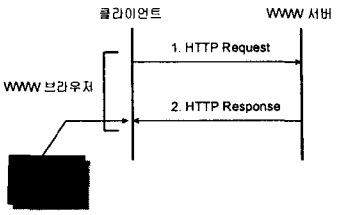
서버별 등급 설정의 유효성 검사시 WWW 서버와 클라이언트 사이의 관계는 [그림 6]과 같으며 먼저 브라우저의 요청에 따라 WWW 서버는 요청한 페이지와 서버 등급 보증서를 보내준다. 브라우저는 요청한 페이지를 화면에 표시해 주며 Plug-in을 실행시키고 보증서를 Plug-in에 넘겨 준다. Plug-in에서는 보증서의 유효성을 검사해 유효하면 보증서에 있는 등급 정보를 화면에 표시해 준다. 보증서는 등급 정보와 WWW 서버의 URL로 구성되어 있으며, 서버 등급 보증서의 경우 WWW 서버 전체에 대해 등급을 설정해 주는 것이므로 보증서가 제대로 된 WWW 서버에 설치되었나를 브라우저에 출력된 페이지의 URL이 보증서에 들어있는 WWW 서버의 URL로 시작되는 지로 검사한다. 예를 들어 브라우저에 보여지는 페이지의 URL이 www.grade.com/ index.html이고 보증서에 들어 있는 WWW 서버의 URL이 www.grade.com이면 이 보증서는 제대로 된 서버에 설치된 것이다.



[그림 5] 서버 등급의 예



[그림 6] 시스템 개략도



[그림 7] 서버-클라이언트

시스템 흐름도에 사용되는 기호는 [표 2]와 같다.

서버별 등급 설정의 유효성 검사시 WWW 서버와 클라이언트 사이의 시스템 흐름도는 [그림 7]과 같으며 자세한 사항은 다음과 같다.

1. WWW 브라우저에 의한 HTTP Request
2. WWW 서버에 의한 HTTP Response
   - 전달되는 메시지 : Page || 보증서
   - HTML의 <EMBED> 태그에 의해 Plug-in이 load된다.
   - 보증서는 보증서 내용과 Rater가 서명한 보증서 내용의 해쉬 값(S_R[H(보증서 내용)])으로 구성된다. 보증서의 유효성을 검증하기 위해서 저장하고 있는 Rater의 인증서를 이용하여 S_R[H(보증서 내용)]을 풀어보면 보증서 내용의 해쉬 값(H(보증서 내용))이 나온다. 이를 평문으로 전송된 보증서 내용을 해쉬 함수를 이용하여 구한 값과 비교하여 같으면 유효한 것이고 그렇지 않을 때에는 유효하지 않은 것이다.
   - Plug-in의 Live connect 기법을 이용하여 Plug-in이 들어 있는 URL을 구해온다. (NPP_GetURL("javascript:document.location"))
   - Live connect 기법을 이용하여 얻어온 URL이 보증서에 들어 있는 URL로 시작되는지 검사하여 제대로 된 서버에 설치되었는지 검사한다.
   - 유효하면 보증서에 있는 등급 정보를 화면에 표시해 준다.

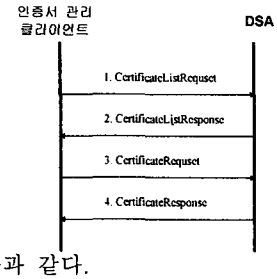
기호	의미
보증서 내용	[G, URL]
보증서	보증서 내용 || S_R[H(보증서 내용)]
G	등급 정보
Page	HTML 문서
S_R	서명용으로 사용되는 Rater의 비밀키
P_R	Rater의 공개키

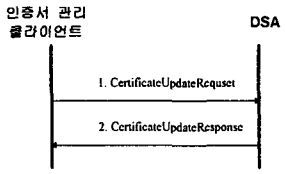
[표 2] 서버별 등급 설정에 사용되는 기호

3.3.2 인증서 관리 클라이언트 - DSA

인증서 관리 클라이언트와 DSA와의 시스템 흐름은 크게 DSA로부터 가져올 인증서들을 갱신 목록에 추가 또는 삭제하는 부분과 인증서들을 DSA로부터 주기적으로 가져오는 두 가지 과정으로 나누어 생각할 수 있다.

[그림 8]은 DSA로부터 주기적으로 가져올 인증서들을 갱신 목록에 추가 또는 삭제하는 부분이며 자





세한 사항은 다음과 같다.

[그림 8] 갱신 목록 추가/삭제 [그림 9] 갱신

1. Certificate List Request
   - DSA가 저장하고 있는 인증서의 목록을 요청한다.
2. Certificate List Response
   - DSA는 저장하고 있는 인증서의 목록을 전달해 준다.
   - 사용자는 인증서의 목록에서 갱신할 인증서들을 선택한다. 만약 인증서 관리 클라이언트가 주기적으로 인증서들을 갱신하는 상황이면, 이미 갱신해야할 인증서들의 목록이 있으므로 갱신해야할 인증서들을 추가 또는 삭제할 수 있다. 목록에서 삭제된 인증서들은 로컬 시스템에서 삭제된다.
3. Certificate Request
   - 사용자는 자신의 원하는 CA 또는 Rater의 인증서들를 요청한다.
4. Certificate Response
   - DSA는 사용자가 요청한 CA 또는 Rater의 인증서들를 전달해 준다

[그림 9]는 갱신 목록에 있는 인증서들을 DSA로부터 주기적으로 가져오는 부분이며 자세한 사항은 다음과 같다.

1. Certificate Update Request
   - 전송되는 데이터는 [인증서 || ... || 인증서]이며 여기에서 인증서는 [인증서의 DN || S_{CA}[H(인증서)]]으로 구성되어 있어 DSA에서는 이를 이용하여 인증서의 변경여부를 확인할 수 있다. S_{CA}는 CA의 비밀키를 의미한다.
   - DSA에게 갱신하고자 하는 인증서의 목록을 전달한다.
2. Certificate Update Response
   - DSA는 전달받은 인증서의 목록을 검사하여 인증서의 갱신, 취소 또는 변함 없음 여부를 판별하여 변함이 없는 인증서에 대해서는 어떤 처리도 해 주지 않으며 갱신된 인증서는 플래그를 갱신으로 설정하여 [DN || 플래그 || 인증서] 메시지를 클라이언트에게 보내주고, 취소된 인증서는 플래그를 취소로 설정하여 [DN || 플래그] 메시지를 인증서 관리 클라이언트에게 보내준다.
   - DSA로부터 갱신 또는 취소 메시지를 받은 인증서 관리 클라이언트는 갱신된 인증서는 로컬 시스템에 있는 인증서를 새로 받은 인증서로 교체하며 취소된 인증서는 로컬 시스템에서 삭제한다.

3.3.3 Rater - WWW서버

Rater와 WWW 서버간에 등급 설정을 하는 과정은 다음과 같다.

1. 서버는 Rater에게 등급 판정을 요청한다.
2. Rater는 등급 보증서를 발급하기 위해 다음의 요구 사항을 가진다.
   - Rater는 WWW 서버의 내용을 SSL(Secure Socket Layer)을 이용하여 가져올 수 있어야 한다.

등급 설정을 하기 위하여 Rater는 WWW 서버의 내용을 검사한다. 이 때 불순한 의도를 가진 사람이 전송되는 내용을 변경, 손상 시킬 수 있으며, Rater는 변경 또는 손상된 내용을 이용하여 등급 설정을 할 위험이 있다. 따라서 전송되는 내용이 제 3자에 의해 변경 및 손상되는 것을 방지하기 위해서 안전한 통신수단인 SSL을 사용한다.

3. 위의 요구 조건을 만족하면 Rater는 다음과 같은 과정을 거쳐 보증서를 발급한다.
   ① WWW 서버의 내용을 확인하여 등급을 설정한다.
   ② 설정한 등급과 WWW 서버의 URL을 이용하여 보증서를 만든다.
4. 발급한 보증서를 서버에 전달해 준다.
   - 보증서의 전달은 e-mail을 이용한다.

4 결론

전자상거래란 단어가 일반인들에게도 낯설지 않고 WWW을 이용한 쇼핑이 구매 수단의 하나로 자리 잡혀가고 있는 현 시점에서 상점에 대한 믿음 없이 물건을 구매한다는 것이 전자상거래가 확산 되는데에 커다란 걸림돌이 되고 있다. 요즈음 이런 문제점을 해결하고자 하는 노력이 증가하면서 상점에 대해 신용을 인증해 주는 기관이 생겨나고 있으나, 이들 기관에서 해주는 인증과 같은 경우에는 특정 기관에서 인증해 주었다는 것을 증명할 방법이 없으며, 서버에서 등급을 위조해도 이를 확인할 방법이 없다.

이와 같은 문제점을 해결하고자 본 논문에서는 전자상거래에서 상점에 대한 신용 보증을 해 줄 수 있는 기반을 설계하였다. 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.

따라서 향후 이와 같은 설계를 바탕으로 WWW 페이지에 대한 공증이 추가된 전자상거래에서 상점에 대한 신용 보증 시스템을 구현함으로써 사용자가 전자상거래를 행할 경우 믿을 수 있는 상점을 선택할 수 있는 환경을 구축할 예정이다.

참고문헌

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

[2] NCSA, FAQ Regarding The NCSA Web Server Field Guide, 1997, http://www.ncsa.com/webcert/wcfaq.htm

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

[4] Simson Garfinkel, PGP : Pretty Good Privacy, OReily & Associations, Inc., 1995

[5] 박현동, 류재철, 임채호, 변혹환, 전자우편 보안, 한국통신정보보호학회, 1995.9

[6] ITU-T Recommendation X.500, The Directory : Overview of Concepts, Models, and Services, 1988