濟州大學校 白鹿論叢 第2集(2000. 4. 20)

웹-기반 가상대학에서 사용자 인증을 위한 인증시스템 구축 방안 연구

박 찬 정*

目 次

Ⅰ. 서 론

최근, 인터넷의 폭발적인 보급으로 인해 인터넷은 모든 분야에서 정보전달의 수단뿐만 아니라 불특정 다수에 대한 통신 수단으로 넓게 이용되고 있다. 또한, 하이퍼텍스트(hypertext)를 기반으로 하는 웹(web)의 출현은 사회의 전 분야에 걸쳐 많은 변화를 촉진시키고 있다. 웹의 발전은 정보화로 인한 사회의 변화와 맞물려 전자상거래, 가상대학, 원격 진료 등 새로운 응용을 창출하고 있다.

특히, 교육분야에서 사람들은 자신들이 원하는 시간에 학습을 하며 모든 과정에 참여하기보다는 자신에게 부족한 부분을 충족시킬 수 있는 부분에만 참여할 수 있는 수요자 중심의 학습환경을 필요로 하게 되면서, 인터넷에서 웹을 기반으로 학교와 집, 직장이 하나로 연결된 가상대학을 요구하게 되었다. 가상대학은 매우 체계적으로 설계되어야 하며, 많은 하드웨어적 자원 및 네트워크 자원, 교수학습 자원들을 요구한다. 현재, 국내에서도 가상대학이라는 이름으로 서비스를 제공하는 사이트들이 증가하고 있는 추세이다[1][2].

웹-기반의 가상대학은 단순히 학생들에게 지식을 전달하기 위한 매체가 아니라 상호작용 및 평가, 관리 등과 같은 기능을 함께 제공해야 한다. 그리고 웹을 기반으로 하기 때문에 웹에서 사용되는 많은 도구들을 그대로 가상대학을 구축하는데

* 컴퓨터교육과 전임강사

사용할 수 있다. 그렇기 때문에, 웹의 문제점들은 가상대학을 구현하는데 걸림돌이 될 수 있다. 즉, 인터넷과 같은 열린망을 이용하여 통신을 하고자 하는 경우, 여러 가지의 문제점이 발생될 수 있고 그 문제점들은 다음과 같다.

우선, 전송중인 정보를 인가 받지 않은 대상이 도청할 가능성이 있다. 따라서, 다른 사용자 ID나 패스워드(password) 등을 가로챌 수 있다. 둘째, 인위적으로 전송중인 데이터의 변조 가능성을 생각해 볼 수 있다. 즉, 온라인 평가 시에 다른 사용자의 답안이 전송될 때 변조시킴으로써 올바른 평가가 이루어지지 않도록 할 수 있다. 셋째, 인터넷 상에서는 통신하는 대상들끼리는 직접 볼 수 없기 때문에 자신을 위장할 가능성이 있다. 즉, 가로챈 ID를 이용하여 가상대학으로의 접근이 가능해진다. 넷째, 통신을 완료한 후 한쪽에서 그 통신에 대한 부인 가능성이 있다. 즉, 자신이 수행한 일에 대해 마치 수행한 적이 없는 것처럼 부인할 가능성이 있다 [3][4].

본 논문에서는 웹-기반의 가상대학 구현 시, 필요한 보안기술 중에서 사용자 인증기술에 대해 기술하고자 한다. 인증기술은 가상대학에 접근할 때 학습자나 교수자 혹은 관리자들의 신분을 확인하여 접근을 제어하는데도 사용되지만, 학습평가를 위해서도 중요한 역할을 수행한다. 일반적으로, 인증기술은 인터넷을 통해 상거래를 하는 전자상거래 분야에서도 활발히 거론되고 있는데, 웹-기반의 가상대학에서도 필수적인 기술이라 할 수 있다. 하지만, 가상대학에서 인증기술은 아직 초보적인 단계에 머물고 있다. 또한, 전자상거래에서 요구하는 인증기술[5]과 가상대학에서 요구하는 인증기술은 서로 요구사항이 다르기 때문에 다소 차이점을 가진다. 따라서, 가상대학에 적합한 인증기술을 제시하고 인증시스템 설계 대안을 기술하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 웹에서 다루어지는 보안 서비스를 기술한 후, 인증기술의 정의와 필요성, 응용분야 등에 대해 기술하고, 3장에서는 인증기술에 필요한 기반 기술을 제시한다. 4장에서는 가상대학에 인증시스템을 구축할 때 전자상거래에서 사용하는 시스템과의 차이점을 기술한 후, 가상대학에 맞는 인증을 위한 시스템 설계 대안을 기술하고, 5장에서 결론을 맺는다.

Ⅱ. 배 경

이 장에서는 중요한 보안기술을 기술하고, 인증 기능 및 인증 서비스의 필요성

등 개념을 소개한 후, 기존의 인증시스템과 기술 동향에 대해 기술한다.

1. 보안 서비스

이 전장에서 네 가지의 보안 위협들 - 도청, 변조, 가장, 부인 - 에 대해 기술하였다. 첫 번째 도청의 문제점을 방지하기 위한 기술을 정보에 대한 기밀성(confidentiality) 유지라고 하며, 두 번째 문제인 변조에 대한 기술을 데이터에 대한 무결성(integrity) 보장이라고 한다. 세 번째 문제점인 가장을 해결하기 위한 기술로는 인증(authentication), 마지막으로 언급된 부인 문제에 대한 해법으로 부인 방지(non-repudiation) 기술이 있다[3][4].

전송 중인 정보에 대한 기밀성을 유지하기 위한 방법으로 개발된 기술로 대표적인 방법이 수학적인 도구를 이용하는 암호화(encryption)가 있다. 정보를 암호화하는 방법에는 크게 두 가지가 있는데 아주 오래 전부터 이용되어온 대칭키 암호 알고리즘(symmetric encryption algorithm)을 이용하는 것과 비교적 최근에 개발된 비대칭키 암호 알고리즘(asymmetric encryption algorithm)을 이용하는 것이 있다[6].

전송 중인 데이터에 대한 무결성을 확인하기 위한 방법으로 개발된 기술로는 수학적으로 잘 만들어진 해시 함수(hash function)를 이용하는 것이다. 전송할 데이터를 해시 함수를 이용하여 압축한 다음 원래의 데이터와 함께 전송하는 것이다. 전송된 자료를 받은 수신자는 그 자료가 변조되었는지를 확인하기 위해서 다시 원래의 데이터를 해시 함수에 적용하여 압축된 값을 전송 받은 압축 값과 비교해 보면 된다[6].

통신 중에 상대방을 인증하기 위한 방법으로 개발된 기술로 오래 전부터 ID와 패스워드를 이용하고 있지만 전송 중인 정보에 대한 기밀성이 유지되지 않는다면, 도청으로 인해 인증으로서의 의미를 상실하게 된다. 이와같은 문제점을 보완하기 위해서 인증서(certificate)를 이용한다. 인증서 자체를 위조하는 일은 거의 불가능하며 인증서는 위에서 언급한 비대칭 암호 알고리즘의 개인키(private key)와 공개키(public key) 원리를 이용한다. 전통적인 관점에서 보면, 개인키는 패스워드에 공개키(인증서)는 ID에 해당된다[7].

통신을 완료한 후 어느 한 쪽에서 전송한 내용에 대한 부인이나 전송 발신자에 대한 부인을 방지하기 위해 서명(signature)을 사용한다. 비교적 간단한 수식의 성립을 확인함으로써 전송한 내용에 대한 타당성 및 전송 발신자의 신원을 보장하게

된다. 일반적으로, 서명을 하기 위해서는 위에서 설명한 비대칭 암호 알고리즘의 공개키와 개인키를 이용한다.

2. 인증 개념

인증이란 어떤 사실을 증명하거나 확인하기 위해 사용되는 것으로서, 여러 가지 경우에서 인용되고 있다. 일반적으로, 인증은 사용자의 정체(identity) 확인하는 기능인 사용자 인증, 거래 내용과 일시 등을 확인하는 내용 인증(전자 공증), 그리고 거래 상대의 신용 능력 확인을 하는 신용 인증으로 분류될 수 있다[8][9].

응용 분야 중에서 기존의 직접 거래와는 달리 개방화된 인터넷을 통한 전자상거래에서의 인증은 거래자의 전자적인 확인을 제공하고 그 거래를 완료하도록 하는데 결정적인 역할을 한다. 인증은 조직 내, 조직 간 및 개인 간 네트워크를 통해 전달되는 폭넓은 상거래 데이터의 도난, 누설 또는 위조를 제거함으로써 보안문제를 해결한다. 한편, 가상대학의 경우에도 전자상거래와 마찬가지로 교수자, 학습자의 데이터는 물론 평가 시에 전송되는 평가 데이터의 도난, 누설 또는 위조를 제거하는데 인증이 결정적인 역할을 수행한다고 할 수 있다.

공공 부문 및 민간 부문에서 네트워크를 통한 각종 정보의 교환이 더욱 활발해지고 있다. 향후에는 더욱 다양한 분야에서 인증 기능이 활용될 것으로 예상된다. 현재로써는 네트워크 인증이 활용되는 분야는 기업 간 거래 및 정보교환, 기업 내 결재 및 정보교환, 기업의 상품 판매, 금융기관의 서비스(송금, 이체 등), 의료기관의 원격 의료, 전자 공증, 행정/민원 기관, 학교, 우체국, 그리고 전자메일 등으로 분류할 수 있다.

3. 인증기관(certification authority:CA)의 기능 및 역할

이 절에서는 인증기술을 가장 많이 필요로 하는 전자상거래에서의 인증기관의 기능과 역할을 기술한다[10]. 이는 가상대학에서의 요구사항을 만족시키기 위해서 어떤 방식으로 도입될 수 있는지 방안을 마련하는데 도움이 될 수 있다.

1) 발행자의 비밀키 관리

인증서 발행자의 비밀키는 각 사용자의 공개키 인증서를 만들 때 전자서명을 붙이는데 사용되는 중요한 요소로써 저장 및 관리가 특히 중요하다. 대부분의 인증

시스템의 취약성은 이 부분을 보호하는데 있어서 문제가 된다. 따라서, 스마트카드 형태의 하드웨어를 이용해 안전하게 보관하는 것이 일반적이다.

2) 공개키 인증서 발행

여러 클라이언트와 서버 응용에서 인증서 발행을 요청하는 방법은 다양하다. 공개키 인증서를 이용하는 응용은 사용자의 공개키 쌍을 생성하기 위한 메커니즘을 제공하며, 생성한 공개키에 대한 인증서 발행을 요청한다. 이 때, 웹 브라우저나 전자우편 클라이언트에 포함되어 있는 다양한 온라인 공개키 인증서 발행 요청 기법을 이용한다. 서버의 인증서 발행 요청은 대개 수작업 또는 파일을 이용한 처리 기법으로 이루어진다. 현재의 추세는 사용자가 이용하기 쉽고, 인증서 발행 정책과 같은 인증서 발행 정보를 쉽게 제공할 수 있는 웹을 기반으로 인증서 발행 요청을 할 수 있게 하는 것이다.

3) 공개키 인증서 관리

발행된 인증서를 관리하는 일은 아주 중요하다. 즉, 인증기관이 발행한 공개키 인증서의 유효성을 결정할 수 있어야 한다. 인증서를 관리하기 위한 기법으로 인증서의 생명주기 관리를 위한 CRL(Certification Revocation List)을 발행하여 사용자들이 다른 사용자의 인증서 유효성을 쉽게 식별할 수 있어야 한다. 즉, 사용자 등록, 인증서의 등록 및 갱신, 인증서의 폐지(revoke), 유효성 확인(validate), 인증서 백업(backup), 키 복구(recovery)등과 같은 인증서 관리 기능이 필요하다.

4) 디렉토리 시스템 관리

디렉토리 서버는 인증기관이 발행한 사용자들의 공개키 인증서를 보관하는 장소이다. 이와 같은 디렉토리 서비스를 이용해 사용자 서로 공개키 인증서를 배포할 수 있게 된다. 인증서를 발행할 때 마다 인증기관은 디렉토리 서버에 인증서를 등록하고, CRL과 CKL(Compromised Key List)들을 작성하여 사용자들이 이용할 수 있도록 저장해 놓게 된다.

5) 정책 관리(policy management)

인증서를 발행하는데 있어서 인증기관마다 인증서 발행정책을 정의하고 있으며, 이 정책을 기준으로 사용자에게 공개키 인증서를 발행해 주게 된다. 인증서를 발행 받은 사용자의 신뢰정도에 따라 다양한 레벨의 인증서를 발행할 수 있다.

Ⅲ. 인증을 위한 기반기술

이 장에서는 우선, 인증을 위한 필요 기법에 대해서 기술한 후, 가상대학에서 필요로 하는 인증기술을 제시한다.

1. SSL과 S/MIME

Ⅱ장에서 설명한 네 가지 보안 서비스를 인터넷 상에서 제공하기 위하여, SSL (Secure Socket Layer) 프로토콜[11][12]과 S/MIME(Secure MIME)[13] 형식 등이 제안되었다.

SSL 프로토콜은 TCP 프로토콜을 이용하는 응용 프로그램들에 대한 보안 서비스를 제공하기 위하여 만들어졌지만, 지금은 주로 HTTP 프로토콜을 이용하는 응용 프로그램에 대한 보안 서비스를 제공하기 위하여 쓰여지고 있다. SSL이 제공할 수 있는 보안 서비스로는 기밀성, 무결성, 인증이고 부인봉쇄에 대한 기능은 SSL 자체로는 제공하지 못한다(그림 1 참조). 인증서 발급 신청서에는 신청자의 전자메일 주소 및 인증서 철회 시 필요한 패스워드 등을 포함하고 있기 때문에 전송 시 기밀성 및 무결성을 요구한다. 현재 SSL 프로토콜은 IETF에서 TCP보안 프로토콜 보안의 표준으로 되어 있으며, 나아가 TLS(TCP+SSL) 프로토콜을 RFC로 올려 놓고 있다[11][12].

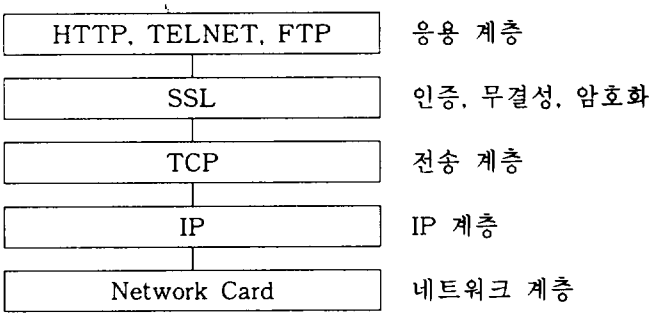

그림 1 프로토콜간의 관계

S/MIME은 MIME 형식의 모든 정보를 보호하기 위하여 개발된 특정한 명세(specification)이다. S/MIME이 제공할 수 있는 보안 서비스로는 기밀성, 무결성, 인증, 부인봉쇄이다. 특별히 전자메일 보안을 위해 현재 많이 이용되고 있다[13].

앞에서 말한 SSL과 S/MIME은 현재 인터넷에서 가장 많이 이용하고 있는 통신 방법인 웹 브라우저와 전자메일 응용을 위한 보안기술로서 모두 인증서를 이용하고 있다는 공통점을 가지고 있다. 인증서는 사용자에 대한 정보 및 공개키와 그것에 대한 신뢰할 수 있는 기관의 서명으로 이루어져 있다. 뿐만 아니라 인증서를 인위적으로 위조할 수 있는 가능성은 없다. 인증서는 앞에서 설명한 보안 서비스 이외에도 몇 가지 서비스를 제공할 수 있다. 따라서, 인증서를 생성하여 발급하는 일은 보안 서비스 제공 차원에서 여러 가지의 중요한 의미를 가지게 된다.

2. 인증서 신청 시 필요한 기술

인증서를 이용하는 응용 프로그램의 종류에 따라서 나누어 보면, 웹 브라우저와 웹 서버가 가장 일반적이다. 웹 브라우저는 SSL 프로토콜이나 S/MIME 형식을 동시에 지원하기 위해 인증서를 사용하고 있다. 웹 서버의 경우는 SSL 프로토콜을 지원하기 하기 위해 인증서를 이용하고 있다.

1) 키 생성(Key Generation)

웹 브라우저의 경우, 브라우저가 키를 생성하기 위한 환경을 제공한다. 이는 브라우저의 종류에 따라서 방식이 다르다. 넷스케이프(Netscape) 브라우저는 키를 생성하기 위하여 새로운 HTML 태그인 KEYGEN을 이용한다. 한편, Internet Explorer는 키를 생성하기 위하여 〈OBJECT〉 태그와 마이크로소프트사에서 공급하는 dll 파일 및 이를 제어하기 위한 스크립트(VBScript, JavaScript)가 필요하다[10].

2) 인증서 발급 요청 형식

SPKAC(Signed Public Key And Challenge)[14]는 생성된 개인키와 공개키는 응용 프로그램의 특정한 위치에 저장되는데, 이 때 개인키의 노출 및 임의 도용을 방지하기 위하여 넷스케이프사의 브라우저 경우, 패스워드를 입력하여 한다. SPKAC는 넷스케이프사의 웹 브라우저를 위해 자체적으로 고안된 인증서 발급 신청 양식이다.

PKCS(Public Key Cryptography Standards)#10[15]은 미국의 암호 기술 개발 전문업체인 RSA사에서 제안한 인증서 발급 신청 양식이고 현재 가장 널리 이용되고 있다. 인증서 발급 양식으로서 PKCS#10을 이용하고 있는 응용 프로그램은

IE, IIS을 비롯한 부분의 웹 서버들(Netscape Web Servers, Apache+SSL)이다. 일반적으로, 마이크로소프트사의 제품들은 PKCS#10을 인증서 발급 신청 양식으로 이용하고 있다.

3. 인증서 생성 시 필요한 기술

인증서 생성 시 필요한 기술로는 RSA 또는 DSA(Digital Signature Algorithm), X.509 인증서와 CA(Certification Authority)로서의 준칙 및 정책이 있다.

1) CA 준칙 및 정책

인증서 신청자의 일정한 기준과 같은 발급기준과 인증서의 유효기간 등이 그 예라고 할 수 있다. 인증서 발급 기준을 웹 브라우저와 웹 서버로 나눌 수 있다. 웹 브라우저용으로 발급할 인증서의 용도에는 크게 SSL과 S/MIME이 있으며, 이는 인증서를 신청할 때 결정된다. 신청자 기준에 대하여는 각 인증기관에 따라 다르고 인증서의 유효기간 설정은 보통 1년으로 한다. X.509 인증서의 v3에서 지원하는 확장 필드에 삽입할 항목도 여기서 결정한다.

2) 서명 알고리즘

인증서 서명 알고리즘으로서 현재 널리 이용되고 있는 것은 RSA(Rivest-Shamir-Adleman)이다. RSA는 원래 비대칭 암호 알고리즘으로서 개인키를 이용하여 서명할 수 있다. 인증기관은 자신의 개인키를 이용하여 인증서의 내용을 서명한다. 서명은 인증서의 마지막 부분에 위치하게 된다. RSA 서명 알고리즘은 단순히 RSA 비대칭 암호 알고리즘을 적용한 것이다. DSA(Digital Signature Algorithm)는 1991년 미국 NIST에서 제안한 서명 알고리즘으로서 현재 미국 내에서는 서명 알고리즘 표준으로 되어 있다.

3) X.509 인증서[10]

현재 인증서는 IETF에서 인증서 표준으로 제안한 X.509 v3를 따르고 있다. 인증서의 목적은 공개키의 안전한 분배에 있다. 일반 이용자들이 안전하게 자신 및 타인의 인증서를 취득하기 위해서는 먼저 자신이 믿고자 하는 인증기관을 결정하여야 한다. 즉, 인증기관의 인증서(공개키)를 안전하고 신뢰성 있는 방법으로 취득하여야 한다. 현재 가장 많이 이용하고 있는 인증서 양식은 그림 2와 같이 X.509

버전과 발급번호, 앞에서 설명한 서명 알고리즘, 발급자 순으로 되어 있고 유효기간은 위의 인증서 발급 기준과 같이 보통 1년이다. 그 다음엔 인증서 신청 양식에 포함된 발급 신청자 및 신청자 공개키에 대한 정보가 나온다. 최근에 추가된 확장 필드는 이 인증서와 관련된 다른 정보를, 예를 들면 이 인증서의 철회 여부를 알려주는 URL 등, 포함한다. 마지막으로, 위의 모든 내용을 인증서에 명시된 서명 알고리즘을 이용하여 서명한 값을 포함시킨다. 만약, 인증서 내용의 일부를 변경시킨다면, 인증서 검증자는 인증기관의 공개키를 이용하여 검증할 수 있다.

X.509 버전
일련번호 (발급번호)
서명 알고리즘
발급자
유효기간
발급신청자
발급신청자 공개키 정보
인증서 관련 정보
서명

그림 2 X.509 인증서 양식

3. 인증서 발급 시 필요한 기술

생성된 인증서는 데이터베이스에 저장된다. 저장된 인증서를 신청자에게 생성되었음을 알리는 방법으로 주로 전자메일을 이용한다. 신청자 전자메일 주소로 자신의 인증서가 있는 URL을 알려줌으로써 그 전자메일 주소가 실제로 존재하는지 여부와 그 전자메일 주소의 소유자가 실제 인증서 신청자인지를 확인할 수 있다. 전자메일을 이용하여 연락을 받은 신청자는 전자메일에서 가리키는 URL로 접속한 다음 자신의 인증서를 가져오면 된다. 인증서를 이용하는 응용 프로그램들은 가져온 인증서에서 신청자 공개키와 자신이 가지고 있는 개인키가 한 쌍임을 확인한 후 인증서를 설치한다. 설치가 완료된 후 자신의 인증서를 확인할 수 있다. 인증서 발급 시 필요한 기술로는 PKCS#7과 DER(Distinguished Encoding Rules) 등이 있다.

PKCS#7[16]은 앞에서 설명한 PKCS#10에 대응되는 메시지 형식으로서 RSA사에서 제안한 암호화된 메시지 표준에 관한 것이다. 인증서뿐만 아니라 철회 목록과 같은 일반적인 암호화된 메시지를 포함하기 위한 표준 형식이다. 인증서 발급시 PKCS#7을 이용하는 응용 프로그램으로는 Internet Explorer 3.0/4.0이 있다.

DER(Distinguished Encoding Rules)은 전송 및 저장을 위한 ASN.1(Abstract Syntax Notation 1) 메시지를 코딩 및 디코딩하는 규칙이다. DER은 이진 형태로 되어 있는데 이것을 다시 base64로 코딩한 것을 pem(privacy enhanced mail) 형식이라고 한다[18].

Ⅳ. 가상대학에서의 인증

이 장에서는 가상대학에서 필요로 하는 인증시스템이 전자상거래에서와 차이점을 가짐을 살펴본 후, 가상대학에 맞는 시스템을 설계하고자 한다.

1. 차이점

우선, 인증기관의 경우에 전자상거래에서는 신용이 있는 제 3의 기관 개입이 요구된다. 즉, 소비자와 상인 모두 인증이 필요하기 때문에 가상대학의 경우에 비해 보다 복잡하고 정교한 인증기법을 요구한다. 반면에, 가상대학의 경우에는 대학이 곧 인증기관이 되며, 대학에 맞는 서비스를 지원할 수 있다는 독립성을 갖게 된다.

가상대학의 경우에도 제 3의 기관을 개입시킬 수 있다. 하지만, 이와 같은 경우 매달 인증서의 발행과 더불어 제 3의 기관에게 사용료를 지불하는 등 경제적인 부담을 안게 된다. 또한, 경제적인 부담 이외에도 사용자에 대한 개인 정보를 함께 인증기관에 제공해야 되기 때문에 학교 내부 정보가 타 기관으로 흘러가게 된다. 이는 보안 측면에서 바람직한 현상은 아니다. 따라서, 학교 별도의 인증시스템 구축이 바람직한 방향이 될 수 있다.

한편, 일반적인 인증시스템을 구축하여 서비스를 시도하는 경우에, 서비스를 신청하는 대상이 웹 클라이언트일 경우도 있고 웹 서버인 경우가 있기 때문에 인증시스템에서는 모든 대상에 대해 서비스를 지원해야 되므로 그 기능이 복잡하다. 하지만, 가상대학의 경우, 서비스 대상이 모두 웹 클라이언트에 속하므로 기능을 축소시킬 수 있다.

2. 인증시스템의 설계

인증시스템은 SSL을 그대로 구현한 공개용 프로그램인 SSLeay[12]에 기반을 두고 있으며, 다음 그림 3과 같은 구조도를 갖는다.

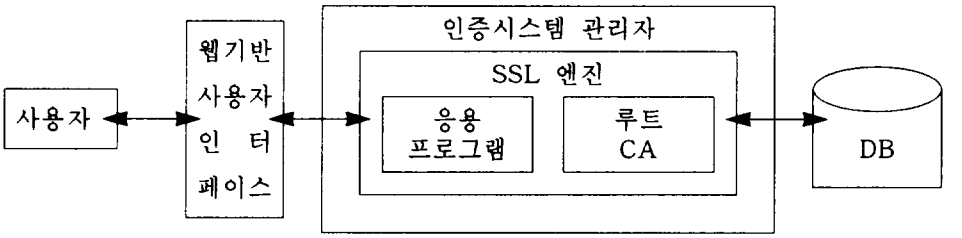

그림 3 인증시스템 구조도

1) 사용자 인터페이스

사용자 인터페이스는 인증시스템 관리자용 인터페이스와 사용자용 인터페이스로 분류할 수 있다. 인증시스템 관리자와 사용자들이 모두 웹 브라우저를 이용하여 서비스를 받도록 해야 한다. 관리를 위해서는 인증서 신청 접수와 인증서 생성, 인증서 발급과 같은 기본 기능을 수행할 수 있도록 한다. 그 이외에도 인증서 폐지, 유효성 확인, 백업 키 복구 등과 같은 작업도 수행할 수 있게 한다.

사용자 입장에서도 인증서를 신청 및 취소할 수 있고 신청한 인증서를 발급 받는 등의 서비스를 쉽게 받을 수 있도록 인터페이스를 제공한다.

2) 관리자

관리자 기능에서 응용 프로그램들은 실제로 인증서 신청을 접수받고 이를 생성하거나 취소하는 등의 기능을 수행할 수 있는 프로그램들로써 인증시스템의 핵심이라 할 수 있다. SSLeay에서 많은 부분을 지원하고 있지만, 다음에서 설명하는 것처럼 데이터베이스와의 연동이라는 문제점을 해결하지 못하고 있다. 따라서, 보다 신뢰할 수 있는 시스템이 되기 위해서 데이터베이스와 연동하는 프로그램이 구현된다.

응용 프로그램들에서 제공하는 기능들은 다음과 같다.

- CA 인증서 제공 기능:인증시스템 자신의 인증서를 제공하여 사용자들이 인증서를 설치하고 자신의 인증서를 신청할 수 있게 한다.

- 웹 브라우저와 SSL의 연결 기능:안전한 인증서 발급 신청을 위해 SSL 프로토콜을 사용한다.
- 웹 브라우저용 인증서 발급 신청 접수 기능:이름, 전자우편 주소, 조직, 부서, 지역, 지방, 국 적과 같은 인증서에 포함될 정보를 입력할 수 있는 기능을 제공한다. SPKAC나 PKCS#10 양식을 이용할 수 있다.
- 접수된 발급 신청 목록 검색 기능:데이터베이스에 저장된 발급 신청 목록을 검색할 수 있는 사용자 인터페이스를 제공하여야 한다.
- 웹 브라우저용 인증서 발급 기능:SSLeay에서 제공하는 명령어를 이용하여 인증서를 발급한 다, 발급한 후 데이터베이스에 저장한다.
- 발급된 인증서 검색 기능:발급된 인증서를 항상 검색해 볼 수 있는 기능을 제공하여야 하며, 이 때, 데이터베이스 사용이 권장된다.
- 인증서 철회 요청 접수 기능:인증서의 철회 요청은 그 인증서의 정당한 소유자만이 수행할 수 있는 기능이다. 인증서의 철회 요청은 그것에 대응되는 비공개 서명키를 분실하거나 도둑 맞은 경우에 이루어지는 절차로써 모든 인증시스템에서 지원해야 한다.
- 접수된 철회 신청 목록 검색 기능:발급된 인증서 검색기능과 마찬가지로 접수된 철회 신청 목록에 대한 검색 기능이 제공되어야 한다.
- 인증서 철회 기능:실제로 요청 접수된 철회를 실시하는 기능이다. 이 때, 철회된 인증서는 일 정 기간 보존되어야 한다.
- 인증서 철회 목록 갱신 기능:SSLeay에서 제공하는 명령어를 이용하여 자신이 발급한 인증서 에 대한 철회 목록을 만들 수 있다. 철회 목록은 X.509 양식을 따르고 pem 파일 양식으로 작 성된다.

루트 CA는 인증서 관련 정책을 결정하는 부분이다. 2장에서도 언급한 것처럼 인증기관은 인증서를 발행하는데 있어서 인증기관마다 인증서 발행정책을 정의하고 있으며, 이 정책을 기준으로 사용자에게 공개키 인증서를 발행해 주게 된다. 인증서를 발행 받은 사용자의 신뢰정도에 따라 다양한 레벨의 인증서를 발행할 수 있다. 이를 처리하는 부분이다.

3) 데이터베이스

인증시스템이 요청을 받거나 생성한 자료들을 저장한다. SSLeay를 이용하여 구현한 경우, 데이터베이스와 연동할 수 없게 되어 있다. 즉, SSLeay에서는 파일 시스템을 이용하여 자료를 처리하지만, 이는 많은 사용자를 관리하는 경우 바람직하

지 못하다. 따라서, 상용 데이터베이스 시스템과 연동할 수 있도록 응용 프로그램들이 개선되어야 한다.

V. 결 론

웹-기반의 가상대학은 단순히 학생들에게 지식을 전달하기 위한 매체가 아니라 상호작용, 평가 및 관리 등과 같은 기능을 함께 제공해야 되기 때문에 웹에서 지원하는 응용 프로그램들을 그대로 사용하는 경우가 많다. 따라서, 웹이 근본적으로 해결해야 하는 문제들을 가상대학 시스템에서도 그대로 상속받게 되며 이와 같은 문제들은 점차 해결되어져야 할 것이다.

본 논문에서는 웹-기반의 가상대학 구현 시, 필요한 보안기술 중에서 사용자 인증기술에 대해 기술하였다. 인증기술은 가상대학 접근 시, 학습자나 교수자들의 신분을 확인하는데도 사용되지만, 그 이외에 학습평가를 위해서도 중요한 역할을 수행한다. 가상대학에 적합한 인증기술을 살펴보고 인증시스템 설계 대안을 제시하였다.

본 논문에서는 우선 가상대학에서 접근제어와 같은 단순한 인증 기능에 추가적으로 고려할 수 있는 보안 서비스로써 인증서를 이용한 인증시스템의 도입을 제안하였지만, 보다 안정된 서비스를 위해서는 향후에는 디렉토리 서버를 연계하여 운용하는 방안에 대해 고려해야 될 것이다. 또한, 빠른 시일 내에 시범적으로 운영될 수 있는 모형이 구현되어져야 한다.

참 고 문 헌

1. 김홍래, 송기상, "구성주의적 접근을 통한 웹 기반의 가상학교의 설계 및 구현", 한국컴퓨터교육학회 논문지, 제1권, 제1호, 1998. 6.
2. 김현주, 이옥화, 김홍기, "WBI 프로젝트의 분석을 통한 한국형 WBI 모델", 한국컴퓨터교육학회 논문지, 제1권, 제1호, 1998. 6.
3. Charles P. Peleeger, Security in Computing 2nd. Ed., Prentice Hall, 1997.
4. Simson Garfinkel and Gene Spaford, Web Security & Commerce, O eilly & Associates, Inc., 1997.
5. Halakota and Whinston, Frontiers of Electronic Commerce, Addison-Wesley, 1996.
6. William Stallings, Cryptography and Network Security:Principles and Practice 2nd. Ed., Prentice Hall, 1999.
7. Lincoln D. Stein, Web Security:A Step-by-Step Reference Guide, Addison-Wesley, 1999.
8. E. Gerck, Overview of Certification Systems:X.509, CA, PGP, and SKIP, http://www.mcg. org.br/cert.htm, 1998.
9. 전자서명인증관리센터, 전자서명 개요, http://www.rootca.or.kr, 1999.
10. Marc Branchud, A Survey of Public Key Infrastructures, Ph.D. Thesis McGill University, 1997.
11. Transport Layer Security Working Group, The SSL Protocol Version 3.0, Internet Draft, 1996.
12. T. J. Hudson and E. A. Young, SSLeay and SSLapps FAQ, http://psych. psy.uq.oz.au/~ftp/ crypto/, 1998.
13. Herman Van Uytven, Using KULeuvenNet and Internet, http://spo5.cc. kuleuven.ac.be/~systhvu /ic/ic.html, 1998.
14. OpenSSL Documents, SPKAC, http://www.openssl.org/docs/apps/spkac.html#, 1999.
15. RSA Laboratories Technical Note, PKCS#10:Certification Request Syntax Standard Version 1.5, http://www.rsa.com/rsalabs/pkcs/pkcs-10/index.html, 1993.
16. RSA Laboratories Technical Note, PKCS#7:Cryptographic Message Syn-

tax Standard Version 1.5, http://www.rsa.com/rsalabs/pkcs/pkcs-7/index.html, 1993.

17. Cetin Kaya Koc, High-Speed RSA Implementation, Technical Report #201, RSA Data Security Inc., 1994.
18. D. Balenson, Privacy Enhancement for Internet Electronic Mail:Part III: Algorithms, Modes, and Identifiers,http://www.cis.ohio-state.edu/htbin/rfc/rfc1423.html, 1993.

Abstract

A Study on Constructing a Certification System for User Authenticaton in Web-based Virtual Universities

Chan-Jung Park

With the advance of computer and communication technologies, a lot of organizations operate virtual universities that provide learning environments out of temporal and spacial constraints. And many research works on the web-based virtual universities where learner-centered, situated learning, and problem-centered learning are fulfilled have been proposed. Various techniques are required to build the virtual universities efficiently. Among them, security is considered as an important skill in the virtual universities. In this paper, when a web-based virtual university is implemented, the certification technique for the virtual university is presented, And a method for constructing a certificate system to support the virtual university is also presented.