PKI 기반 보안 웹 서비스 제공 방안에 관한 연구

김덕기*, 김종학**, 문영성**
*한국관광대학 디지털콘텐츠과
**숭실대학교 컴퓨터학과
e-mail:alberto1@ktc.ac.kr, mygiant@sunny.ssu.ac.kr,
mun@computing.ssu.ac.kr

A Study on supporting secure Web Service that based PKI

Duckki Kim*, Jonghak Kim**, Youngsung Mun**
*Dept. of Digital Content, Korea Tourism College
**Dept. of Computing, Soongsil University

요 약

정보통신기술의 발전과 정보화의 진전을 통한 PC 및 인터넷의 보급은 시간과 공간적인 제약을 최소화하여 기존 산업 분야에 많은 영향을 끼치고 있다. 특히, 웹을 활용한 전자상거래 운용 및 기업체의 지점 또는 분점과 같이 여러 기관으로 구성되어 있는 환경에서는 많은 기업 운영정보들을 관리하기 위하여 웹사이트나 웹 기반의 어플리케이션을 활용하고 있다. 그러나 자료 접근의 용이성을 강조하는 웹 서비스의 특성상 보안상의 취약성을 내제하고 있다. 이러한 문제를 해결하기 위한 기존의 방식들은 사용자 인증을 위한 공개키구조(PKI)기반 구조와 안전한 트렌젝션 처리를 위한 SSL을 이용하여 웹 서비스 보안에 사용하고 있다. 그러나 SSL을 이용한 웹 서비스 보안은 사용자 요구 트렌젝션 증가에 비례하여 웹 서버에게 과도한 부하를 초래한다. 이러한 문제점 해결을 위하여 본 연구에서는 웹 서비스에서 PKI의 인증 및 SSL설정 단계와 시간을 단축을 위한 PKI의 RA와 SSL의 SSL 가속기가 통합된 시스템을 제안한다.

1. 서론

정보통신기술의 발전과 정보화의 진전을 통한 PC 및 인터넷의 보급은 시간과 공간적인 제약을 최소화하여 기존 산업 분야에 많은 영향을 끼치고 있다. 특히, 웹을 활용한 전자상거래 운용 및 기업체의 지점 또는 분점과 같이 여러 기관으로 구성되어 있는 환경에서는 많은 기업 운영정보들을 관리하기 위하여 웹사이트나 웹 기반의 어플리케이션을 활용하고 있다. 그러나 자료 접근의 용이성을 강조하는 웹 서비스의 특성상 보안상의 취약성을 내제하고 있다. 이러한 보안 취약성을 해결하기 위하여 기존의 방법들은 웹 서비스 사용자의 인증을 위하여 PKI와 웹 서비스 사용자의 요구 트렌젝션을 보호하기 위하여 SSL등을 이용하고있다.

PKI(Public Key Infrastructure)는 공개키 알고리즘을 통한 암호화 및 전자서명을 제공하는 복합적인 보안시스템 환경이다[1]. 즉, 암호화와 복호화키로 구성된 공개키를 이용하여 송수신 데이터를 암호화하고 디지털인증서를 통해 사용자를 인증하는 시스템이다. 그러므로 PKI 기술은 웹을 이용한 전자상거래 및 정보유통의 안전성과 신뢰성을 확보하기 위한 시스템으로, 상대방의 신원을 확인하고 정보내용의 변경확인과 비밀유지기능을 갖는 지식정보화사회의 핵심기술이다.[1] SSL(Secure Socket Layer)은 클라이언트-서버 환경에서 TCP상의 응용 프로토콜에 대한 종단간 보안을 제공하기 위해 고안된 전송계층 보안 프로토콜로 웹 브라우저와 웹 서버가 각각 클라이언트와 서버 역할을 수행한다.

그러나 PKI를 이용한 인증 및 SSL을 이용한 웹 서비스 보안은 사용자 요구 트렌젝션 증가에 비례하여 웹 서버에게 과도한 부하를 초래한다.

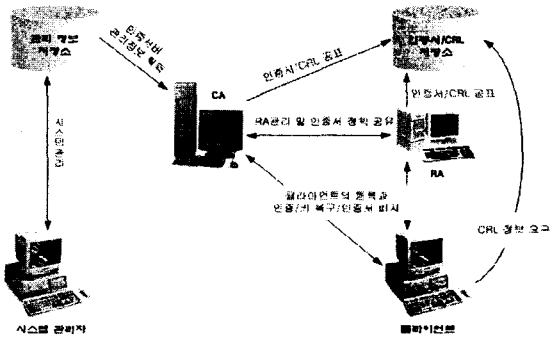
본 연구에서는 기존의 PKI와 SSL을 이용한 사용자 인증 및 안전한 웹서비스 제공을 위한 구현 상황의 분석 및 문제점의 도출을 통하여 보다 효율적이고 안전하게 웹 서비스를 제공하기 위한 새로운 방안을 제시하고자 한다.

본 논문은 2장에서 안전한 웹서비스를 위한 보안 프로토콜에 대해 살펴볼 것이며, 3장에서 안전한 웹서비스를 위한 보안 프로토콜의 문제점을 자세히 살펴보며, 4장에서는 문제점들을 해결할 수 있는 시스템을 제안하며 마지막으로 5장에서는 제안한 시스템의 특징 및 장점에 대하여 도출한 후, 향후 연구방안에 대하여 제시한다.

2. 안전한 웹서비스를 위한 보안 프로토콜

2.1 PKI(Public Key Infrastructure)

데이터를 암호화하는 방법에는 공개키와 비밀키 방식이 있다. 비밀키 암호시스템이 송수신자 양측에서 똑같은 비밀키를 공유하는 데 반해 공개키는 암호화와 복호화키가 다르기 때문에 데이터를 암호화하고 이를 다시 풀 수 있는 열쇠가 달라 거의 완벽한 데이터 보완이 가능하고 정보유출의 가능성이 적은 시스템이다. 그러므로 공개키 암호의 상용화를 위해서 키의 생성과 인증, 그리고 분배와 안전한 관리를 위한 체계를 마련한 것이 공개키기반구조이다.[2][3]



[그림 1] PKI 구성요소

PKI의 구현 절차는 [그림 1]과 같으며 각각의 구성요소의 역할은 다음과 같다.

(1) 인증기관(CA) : 인증기관은 PKI를 구성하는 가장 핵심 객체로 공개키의 진위여부를 확인하고 사용자의 공개키에 자신의 디지털 서명을 함으로써, 그 키를 이용한 사람의 신분을 증명해 주는 기관이다. 인증기관은 일반적으로 PKI를 공급하기 위해서 최상위에서부터 역할 및 기능에 따라 PAA, PCA 그리고 CA로 계층적으로 구성된다.

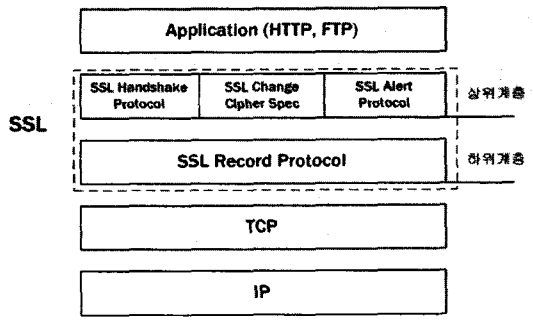
(2) 등록기관(RA) : 인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자 사이에 등록기관을 두어 인증기관 대신 사용자들의 인증서 신청시 그들의 신분과 소속을 확인하는 기능을 수행한다. 사용자들의 신분을 확인한 후, 등록기관은 인증서 요청에 서명을 한 후 인증기관에게 제출한다. 인증기관은 등록기관의 서명을 확인한 후 사용자의 인증서를 발행한 후 등록기관에게 되돌리거나 사용자에게 직접 전달한다.

(3) 인증서/CRL 저장소 :일반적으로 PKI에서 사용되는 인증서 양식은 ITU에 의해서 제안된 X.509 인증서 양식을 따르고 있다. X.509 인증서는 초기 버전1에 이어 버전 2에서는 인증서 취소 목록(CRL)이 추가되었고, 현재 대부분의 공개키 인증관련제품들에서 사용되는 버전3에서는 새로운 개념인 확장자를 도입함으로써, 다양한 환경을 고려한 조건 및 서명알고리즘을 선택 가능하도록 하였다. 즉, 인증서/CRL 저장소는 인증서와 인증서 취소 목록을 저장하고 있는 디렉토리를 의미한다.[4]

이 시스템을 도입하여 전자상거래를 할 경우, 전자상거래를 위해 전자서명을 한 뒤 공인인증기관의 인증을 받아 상대에게 제시함으로써 거래가 이루어지는데 개인정보나 거래정보가 외부에 노출되지 않아 안전하게 거래할 수 있다. 이 시스템은 인터넷상의 보완을 위한 광범위한 기업응용 프로그램에 보안솔루션을 제공한다. 솔루션은 웹보안, 전자우편보안, 원격접속, 전자문서, 전자상거래 어플리케이션 등 매우 다양한 분야에서 사용된다.

2.2 SSL(Secure Socket Layer)

SSL은 계층적 프로토콜이다. 각 계층에는 길이, 설명, 내용형식에 부합하는 메시지가 존재한다. SSL은 전송될 메시지를 다룰 수 있는 블록으로 나누고, 선택적으로 압축하고 MAC에 맞추어 변경하고, 암호화한다. 수신된 데이터는 복호화되고, 검증된 후 압축이 해제되고, 재조합되어 상위계층의 클라이언트에게 전달된다.[5]



[그림 2] SSL 프로토콜 구조

SSL 프로토콜은 [그림 2]에서 보는 바와 같이 하나의 프로토콜이 아니라 하위계층과 상위계층의 두 계층로 구성되어 있음을 볼 수 있다. 상위계층은

SSL Handshake, SSL Change Cipher Spec, SSL Alert Protocol 부분으로 구성되며, 하위계층은 신뢰할 수 있는 .전송 프로토콜(예, TCP)위에 위치하며 실직적인 보안 서비스를 제공하는 SSL Record Protocol 부분이다. SSL Record 프로토콜은 다양한 상위계층 프로토콜들의 캡슐화에 사용된다. 캡슐화된 프로토콜 중의 하나인 SSL Handshake Protocol은 서버와 클라이언트간의 인증을 가능하게 하며, 어플리케이션 프로토콜이 전송되거나 수신되기 전에 이루어지는 알고리즘, 암호 키에 관한 협상을 가능하게 한다. SSL의 이점 중의 하나는 독립적인 어플리케이션 프로토콜이라는 것이다. 상위계층 프로토콜은 SSL 프로토콜을 위에 독립적으로 위치하며 SSL은 상위계층 데이터 변조없이 통신 할 수 있다.

3. SSL 기반 안전한 웹 서비스 제공의 문제점

사용자의 웹 서비스 제공시에 보안을 위해 사용되고 있는 SSL은 아래와 같은 문제점을 가지고 있다.

첫째는 SSL의 사용에 따른 서버 성능 저하의 문제이다. 서명 생성과 검증 및 인증서의 교환에 필요한 수학적 연산과정은 높은 계산 능력을 필요로 한하며, 실제로 수행시에 CPU의 대부분을 점유한다. 그러므로 웹 서버에 수백, 수천명의 사용자가 동시에 웹 서비스를 요청시에 SSL을 유지하기 위하여 웹 서버는 과부하로 인한 긴 응답시간 지연이 발생하게 된다. 이 경우 웹 기반의 전자상거래 사이트들이나 실시간 서비스 제공 사이트들 에게는 치명적인 문제가 된다.[6]

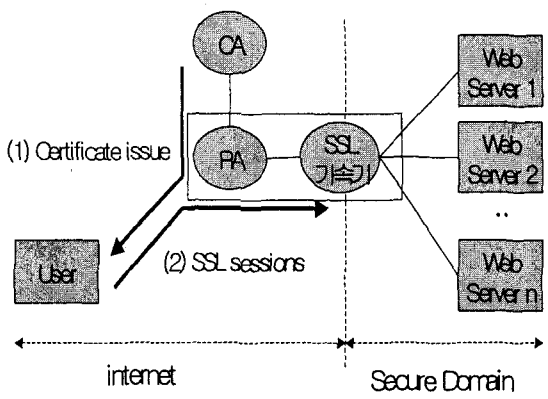
둘째는 웹 서버의 비밀키 보안의 문제이다. 일반적으로 서버의 비밀키는 하드 드라이브에 저장되며, 필요할시에 프로세서로 복사되어 사용된다. 그러나 하드 드라이브나 프로세서는 서버에 접근 가능한 사용자들에 대하여 보안 취약성을 노출하고 있다. 또한 웹 서비스가 여러 PC에 의해서 제공될 경우 키 공유에 문제에의해서 더욱 심각해 질 수 있다.

셋째는 트래픽 관리의 문제이다. SSL은 패킷을 악의의 사용자로부터 도청을 방지하기 위하여 암호화되기 때문에 URL, 쿠키, 응용프로그램 정보들에의해서 트래픽 경로를 변경하거나 분산하는 로드 벨런싱 및 콘텐츠 스위치 등의 트래픽 관리 프로그램등의 기능을 사용할 수 없게 한다.

4. 안정적인 서비스를 위한 웹 시스템 제안

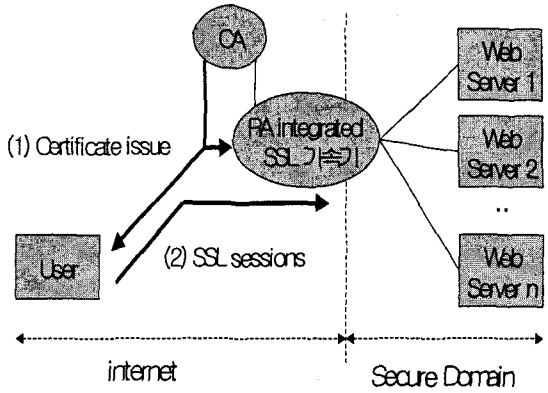
PKI 및 SSL 서비스는 높은 연산 기능을 요구하므로 웹 서버는 이러한 연산을 수행하기 위해 많은 자원을 소모하게 된다. 이는 웹 서버의 성능저하 문제를 발생시킬 수 있다. 현재 이를 해결하기 위해서 SSL 가속기라 하는 별도의 하드웨어가 등장하였다.

SSL 가속기는 PCI 카드와 같은 형태로 웹 서버 내부에 탑재할 수도 있으며, 웹 프록시 서버의 형태로 독립된 서버로 존재할 수도 있다.[7][8]



[그림 3] SSL 가속기를 적용한 시스템

그러나 현재 제공되는 SSL 가속기의 기능은 웹 서버에서 수행되는 SSL 기능을 SSL 가속기가 대신할 뿐 사용자가 얻는 이점은 적다. 즉, SSL 가속기의 등장은 웹 서비스를 제공하는 측면에서는 성능의 개선 효과가 있지만, 사용자의 입장에서는 큰 변화가 없다. 본 연구에서는 RA 서버를 사이트 도메인 영역에 위치하게 하여 PKI 기반 사용자의 인증 및 웹 서버를 위한 SSL 수행을 통합한 새로운 시스템을 제안한다.



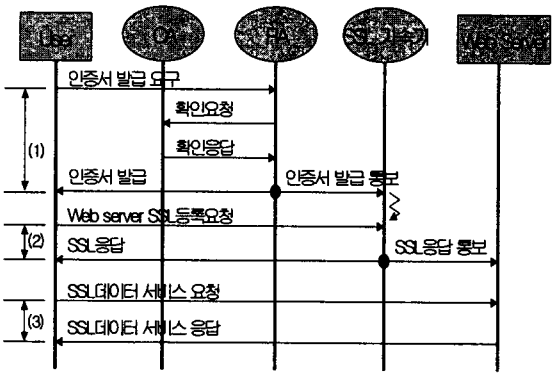
[그림 4] RA와 SSL 가속기가 통합된 시스템

제안된 시스템은 RA 서버와 SSL 가속기를 하나의 서버로 통합함에 따라 웹 서버에 가중되는 SSL 연산의 분산 및 추가적인 메시지 과정을 최소화할 수 있는 이점을 가질 수 있다. 이때 RA 서버에 SSL 가속기 기능이 통합된 서버는 RA intgrated SSL 가속기라고 한다.

RA intgrated SSL 가속기의 형태는 기존의 RA 서버에 SSL 가속기 기능을 추가 탑재를 통하여 해결할 수 있다.

제안한 시스템의 메시지 동작 절차는 [그림 5]와 같으며, 단계는 크게 PKI 인증단계 단계, 웹 서버와

인증단계 그리고 안전한 웹 서비스 제공 단계의 세 단계로 분류할 수 있다.



[그림 5] 제안된 시스템의 동작 절차

(1) PKI 인증단계 : 사용자는 자신의 등록기관에 인증서 발급을 요청한다. 인증서 발급을 요청받은 RA는 CA를 통하여 사용자의 신원을 확인하며, 정당한 사용자로 확인되면 인증서를 발급한다. 이때 기존의 방식과 달리 RA는 사용자에 대한 인증서 발급 사실을 사용자와 SSL 가속기에 동시에 전송한다. 사용자의 인증서 발급 사실을 통지받은 SSL 가속기는 사용자에 대한 SSL 세션을 위한 사전 준비를 시작한다.

(2) 웹 서버와 SSL 인증단계 : 사용자 인증을 위한 단계를 마친 후 사용자는 자신이 이용하고자 하는 도메인의 웹 서버에 SSL을 통하여 해당 도메인의 등록된 사용자임을 확인한다. 이때 과도한 암호학적 계산으로 인한 웹 서버의 부하를 줄이기 위해 SSL 가속기를 통하여 SSL 인증 절차가 진행되며, 사용자 인증시에 RA 서버에 등록된 사용자 정보를 활용함으로써 보다 신속하게 사용자가 웹 서버의 인증을 수행할 수 있도록 한다.

(3) 안전한 웹 서비스 제공 단계 : 이 단계는 실제로 사용자가 특정 도메인의 웹 서버를 통하여 서비스를 제공받는 단계로써, PKI와 SSL 인증을 마친 사용자는 안전하게 웹 서버 사용을 할 수 있다.

5. 결론 및 향후 연구 과제

본 연구에서 제안된 시스템은 PKI를 이용한 사용자 인증과 SSL 기반 안전한 웹 서비스를 효율적으로 수행할 수 있도록 RA 서버와 SSL 가속기를 하나 서버로 통합하는 시스템을 제안하였다.

제안된 시스템은 사용자입장에서 사용자 인증단계와 웹 서버 인증단계를 하나의 단계로 통합함으로써 웹 서버 접근의 신속성을 제공하며, 안전한 웹 서비스를 제공을 위한 SSL 기능을 웹 서버가 아닌 RA Intgrated SSL서버가 SSL 세션을 위한 암호학적 처리를 대신 수행함으로써 상대적으로 더 많은 사용자와 서비스 연결을 유지할 수 있도록 하였다. 또한 웹 서비스를 이용하여 전자상거래 운용 및 기업체의 지점 또는 분점과 같이 여러 기관으로 구성되어 있는 환경에서는 많은 기업 운영정보들을 관리를 필요로하는 경우에 효율성을 극대화 할 수 있다.

향후 연구 방안으로는 RA의 계층적인 관리에 대한 추가적인 연구가 필요하다.

참고문헌

[1] Carlisle Adams, Steve Lloyd, "Understanding PKI 2nd Edition", Addison-Wesley, 2002.

[2] 염흥렬, 홍기용, "공개키 기반 구조", 통신정보보호학회 학회지(PKI특집), 제8권 3호, pp.5-18, 1998.

[3] 이만영, 김지홍, 송유진, 염흥렬, 이임영, "인터넷 보안 기술", 생능출판사, 2002.

[4] Housley, "Internet X.509 Key Infrastructure Certificate and CRL Profile", RFC 9459, 1999.

[5] Eric Rescorla, "SSL and TLS", Addison-Wesley, 2001.

[6] Networkshop, Scaling security in ecommerce applications, Report synopsis. http://www.networkshop.ca/ documents/ icspreview.pdf.

[7] Lori MacVittie, Smashing the SSL Speed Trap, Network Computing, available at http://www.networkcomputing.com/1212/1212f4.html, 2001.

[8] 주학수, 주홍돈, 김승주, "고속 암호연산 프로세서 개발현황", 한국정보보호학회, 정보보호학회지, 제12권 제 3호, pp. 1-9, 2002.