안전한 네트워크 전송 메시지를 이용한 웹 서비스 보안 시스템에 관한 연구

김창수* · 정회경**

*청운대학교 인터넷학과 · **배재대학교 컴퓨터공학과

A study of Web Service Security System using the Secure Network Transfer Message

Chang-su Kim* · Hoe-kyung Jung**

*Dept. of Internet, Chungwoon University · **Dept. of Computer Engineering, Paichai University

요약

현재의 인터넷은 짧은 기간에 급속한 성장을 했으며 이를 기반으로 하는 전자상거래도 급성장 했다. 이러한 인터넷 기반의 전자상거래는 사용자와 공급자 간의 효과적인 상호 사용자 인증 방법으로 웹 클라이언트 메시지 기술이 활용되고 있다.

클라이언트 메시지의 사용은 사용자 인증 및 전자상거래를 비롯한 웹 서비스의 효율성을 높여줄 뿐 아니라, 다양한 목적으로 여러 가지 기능을 제공해 주기도 한다. 하지만, 클라이언트 메시지는 평문 형태로 전송되고 저장되기 때문에 네트워크 공격, 종단 시스템 공격, 쿠키 획득공격에 정보가 쉽게 노출될 수 있다.

본 논문에서는 네트워크 전송 메시지에 보안 서비스 제공을 위해 암호 알고리즘을 이용하여 클라이언트 메시지의 보안상 문제 해결을 위해 안전한 메시지와 메시지 생성과 검증에 사용되는 클라이언트 사용자 입력 정보를 안전하게 웹 서버로 전송하기 위해 네트워크 전송 메시지에 대한 보안 서비스를 설계하였다.

abstract

As th Internet grew rapidly, the Electronic Commerce that is based on Internet increased. The Electronic Commerce is unsubstantial in the mutual authentication between the parties and a commerce As a solution to this issue, a Web server uses a Client Message technology.

The purpose of Client Message is to validate the user and the electronic commercial transaction. Further, it increases efficiency and offers several ability at various purposes. However, the Client Message is transferred and stored as an unencrypted text file, the information can be exposed easily to the network threats, end system threats, and Client Message harvesting threats.

In this paper designed by used crypto algorithm a Secure Message as a solution to the issue have proposed above. Further, designed a security service per Network transmitting message to transfer client's user input information to a Web server safely.

키워드

secure message, RSA public key, MD5 hash functions

Ⅰ. 서론

인터넷 환경으로 전환되고 정보화 시대가 되어감에 따라 많은 곳에서 웹 서비스 기반 정보 시스템을 구축, 운영하고 있고 대부분의 작업들이 웹 서비스 기반 정보 시스템을 통해 이루어지고 있으며, 데이터의 이동 또한 컴퓨터와 네트워크를 통해 이루어진다. 하지만 웹 서비스 기반 정보 시스템 구축의 보안관리 및 네트워크 시스템 보안 운영에 정보 보안에 많은 허점이 노출되고 있다.

따라서 개인 정보 노출을 방지할 수 있는 안전한 메시지 전송을 이용한 웹 서비스 보안 시스템의 필요성이 더욱 커지게 되었다.

웹 서버와 클라이언트간의 메시지 정보는 보안 기능이 취약하기 때문에 보안 기능을 추가하여 안전성을 보장하면, 웹 서버는 사용자의 접근 제어를 비롯한 여러 가지 보안 서비스를 제공할 수 있다. 이에 본 논문에서는 기존의 네트워크 전송 메시지에 보안 문제를 보안하여 안전한 네트워크 전송 메시지를 이용하여 사용자 인증을 제공하고,

어떠한 웹 환경에서도 사용 가능한 웹 서비스 보안 시스템을 설계 하였다.

II. 관련 연구

2.1 공개키 암호 시스템

공개키 암호 시스템(Public Key Cryptosystem)[1,2,3]은 암호화(Encryption)와 복호화(Decryption)에 사용되는 두 개의 키를 가진다. 즉, 암호화와 복호화에 사용되는 키가 다르며, 각각 공개키(Public key)와 개인키(Private key)라고 한다. 이는 암호 알고리즘과 암호 키를 알 때 복호키를 아는 것이 계산적으로 불가능한 특징이 있다. 이러한 공개키 암호화 과정을 그림 1에서 보여주고 있다. 여기서 필요한 과정은 다음과 같다.

① 네트워크상의 각 종단 시스템들은 송수신할 메시지의 암호화와 복호화에 사용되는 한 쌍의 키를 생성한다.

② 각 시스템은 공개키 서버 등을 통해 공개키를 다른 시스템에 공개하고 개인키는 자신만이 소유한다.

③ 만일 사용자 A가 사용자 B에게 메시지 전송을 원한다면 B의 공개키를 사용해 메시지를 암호화 한다.

④ B가 암호화된 메시지를 수신하면 B의 개인키를 이용하여 메시지를 복호화 한다. B만이 B의 개인키를 소유하기 때문에 다른 어느 사용자도 메시지를 복호화 할 수 없다.

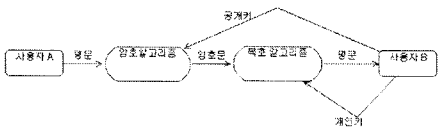

그림 1. 공개키 암호화 과정

2.2 해시 함수

메시지 인증 코드에 대한 변형이 일방향 해시 함수이다. 해시(Hash) 함수[3]는 메시지 인증 코드와 같이 다양한 크기의 메시지 M을 입력 받고 출력으로 메시지 다이제스트라고 하는 고정된 크기의 해시 코드 H(M)을 만든다. 해시 코드는 메시지의 모든 비트들의 함수이고, 에러 탐색 능력을 제공한다. 즉, 메시지에 있어서 하나의 비트 또는 비트들의 변화는 해시 코드의 변화를 가져온다. 메시지 인증을 제공하기 위해 사용되는 해시 코드의 사용 방법은 다양하다. 이에 대한 설명을 그림 2에서 보여준다

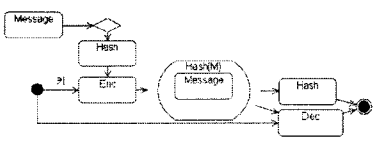

그림 2 해시 함수 사용

송신자의 개인키를 이용해 해시 코드만 공개키 방식으로 암호화 한다. 이는 오직 송신자만이 암호화된 해시 코드를 만들 수 있기 때문에 인증과 함께 전자 서명을 제공한다.

2.3 보안 서비스

웹 에서 이루어지는 메시지 전송은 사용자 입력 정보 등의 네트워크 전송 메시지가 네트워크 상에 평문 상태로 전송되기 때문에 보안에 취약하다. 네트워크 전송 메시지에 대한 보안 공격 유형은 다음과 같다.

◉방해(Interruption) : 하드웨어 파괴, 통신 두절, 파일 관리 시스템 무력화 등 시스템의 일부가 파괴되거나 사용할 수 없게 되는 가용성공격이다.

◉가로채기(Interception) : 네트워크상의 데이터를 가로채기 위한 도청, 파일 또는 프로그램의 복사 등 비인가자들의 불법적인 접근에 의한 기밀성공격이다.

◉불법수정(Modification) : 데이터 파일내의 값 변경, 프로그램의 다른 기능 수행을 위한 변조, 네트워크 전송 메시지 수정 등 비인가자들의 불법적인 변경에 의한 무결성 공격이다.

◉위조(Fabrication) : 네트워크상의 위조된 메시지 삽입, 파일에 레코드추가 등 비인가자들의 시스템에 대한 위조물 삽입에 의한 인증 공격이다.

네트워크 공격은 네트워크상에 전송되는 평문 형태의 메시지가 노출되어 수정되는 것을 말한다. 이러한 공격은 서버와 브라우저에 설치된 SSL(Secure Socket Layer)[2] 프로토콜의 사용으로 저지할 수 있다. 하지만, 이는 메시지가 네트워크상에 전송되는 동안에만 보호될 수 있다는 단점이 있다.

안전한 전송 메시지를 이용한 웹 서비스 보안 시스템을 위해서는 다음과 같은 보안 서비스의 고려사항이 되어야 된다.[4,5,6]

◉기밀성(Confidentiality)
◉인증(Authentication)
◉무결성(Integrity)
◉부인 봉쇄(Non-Repudiation)
◉액세스제어(Access Control)
◉가용성(Availability)

III. 시스템 설계

본 장에서는 안전한 네트워크 전송 메시지를

이용한 웹 서비스 보안 시스템의 구성 요소를 정의하고 안전한 메시지 전송을 위한 보안 서비스에 대해 설명한다.

안전한 네트워크 전송 메시지를 이용한 웹 서비스 보안 시스템의 구성 요소는 그림 3과 같다.

클라이언트는 웹 브라우저를 통해 웹 서버에 접속을 시도하는 개체로 자신의 공개 키 쌍을 생성하여 파일로 저장하고, 둘째, 공개키 서버에 공개키 등록 및 웹 서버 공개키를 요청하고, 웹 서버의 공개키로 사용자 요구 메시지를 암호화하여 웹 서버로 전송하는 기능을 한다. 또한 웹 서버로부터 수신된 안전한 네트워크 전송 메시지를 자신의 메시지 파일에 저장한다.

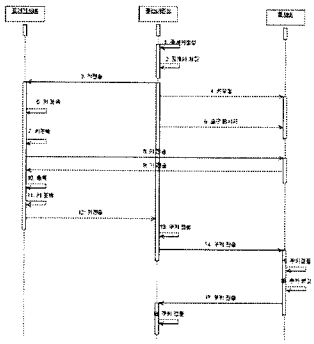

그림 3. 시스템 구성

웹 서버는 웹 서버의 데몬들을 관리하고 클라이언트 요청에 따라 공개키 서버와 연계해서 클라이언트로부터 인증이 필요한 URI 요구를 수신하면, 해당 클라이언트에게 전송하는 기능을 한다. 클라이언트로부터 암호화된 메시지를 수신하면, 기밀성, 인증, 무결성 검사를 하여 클라이언트에 대응한 안전한 네트워크 전송 메시지를 생성하여 클라이언트로 전송한다.

공개키 서버는 클라이언트 사용자 인증 메시지의 암호화를 위해 웹 서버 공개키를 클라이언트에게 분배하고, 클라이언트가 서명한 요구 메시지를 검증하기 위해 클라이언트 공개키를 웹 서버에게 분배하는 기능을 한다.

웹 서버 데몬은 웹 서버를 통해 클라이언트의 인증과 공개 키 서버간의 채널 형성을 통해 클라이언트의 키 발급 및 정보를 수신한다.

3.1 안전한 네트워크 전송 메시지 설계

기존의 클라이언트와 웹 서버 사이에서 사용되던 클라이언트 메시지 정보를 보완하여 안전한 네트워크 전송 메시지를 설계하였다. 안전한 네트워크 전송 메시지는 기밀성, 인증, 무결성 보안 서비스를 제공하기 때문에 공격자의 공격으로부터 안전하게 보호된다. 사용자 정보와 패스워드 정보를 위한 클라이언트 메시지 정보는 사용자 식별 및 인증을 위한 클라이언트 메시지 정보로 여기에 저장되는 값은 다이제스트 생성하여 웹 서버 공개키로 암호화되어 기밀성이 제공된다.

전자 서명은 해시 알고리즘(MD5)으로 클라이언트 메시지 값들(Encrypted_ID, Encrypted_Password)의 다이제스트를 생성하고, 웹 서버 개인키로 전자 서명함으로써 무결성과 인증을 제공한다.

3.2 클라이언트 메시지 보안

네트워크로 전송되는 사용자 정보가 평문으로 전송되어 안전하지 않다. 따라서 전송 메시지에도 보안 기능을 추가할 필요가 있다. 전송 메시지에 보안 서비스가 제공되어야 하며 전송 메시지는 기밀성과 인증 보안 서비스는 공개키 암호 기술과 공개키 서명 기술을 사용하여 제공되며, 무결성 보안 서비스는 해시 기술을 사용하여 제공된다. 첫째, 쿠키의 기밀성 보안 서비스는 그림 4와 같이 쿠키에 저장할 값을 웹 서버 공개키(KUw)로 암호화하여 제공한다. 암호화된 쿠키는 쿠키를 생성한 웹 서버만이 개인키(KRw)를 소유하고 복호화 할 수 있기 때문에 기밀성을 보장할 수 있다.

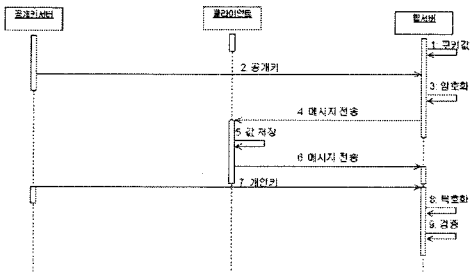

그림 4. 클라이언트 메시지 보안

쿠키 인증 보안 서비스는 클라이언트가 정당한 서버로부터 쿠키가 생성되었는지를 인증하는데

쿠키 값을 웹 서버 개인키로 전자 서명하고, 서명된 쿠키는 클라이언트에서 웹 서버 공개키로 서명 검증된다. 따라서 클라이언트는 쿠키가 정당한 서버로부터 생성되었는지를 인증할 수 있다. 또한 서버가 정당한 클라이언트로부터 수신된 쿠키인지를 인증한다.

사용자 정보를 암호화하여 저장한 쿠키를 이용한다. 사용자가 다시 접속하여 입력한 정보가 쿠키에 저장해둔 정보를 복호화한 값과 같은지 비교한다. 따라서 서버는 쿠키가 정당한 클라이언트로부터 수신되었는지를 인증할 수 있다.

정당한 서버가 생성한 쿠키인지를 인증한다. 쿠키 값을 웹 서버 개인키로 전자 서명하고, 서명된 쿠키가 다시 웹 서버로 전송되면 공개키(KUw)로 서명 검증된다. 따라서 자신이 생성한 정당한 쿠키인지를 인증한다.

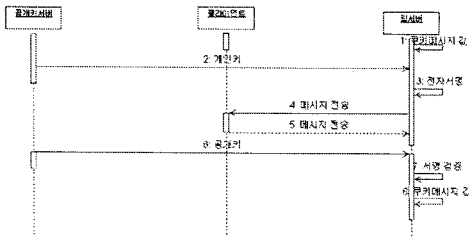

그림 5. 정당한 클라이언트 메시지 인증

쿠키의 무결성 보안 서비스는 쿠키 값을 해시 알고리즘(MD5)로 다이제스트 하여 제공한다. 쿠키에 저장해둔 다이제스트가 쿠키 값의 다이제스트와 같은지 비교하여 무결성을 검사한다.

3.3 네트워크 전송 메시지의 보안

네트워크 전송 메시지의 보안 서비스는 그림 6과 같이 메시지의 다이제스트를 생성하여 클라이언트 개인키(KRc)로 서명하고 웹 서버 공개키로 암호화하여 무결성, 인증, 기밀성 보안 서비스를 동시에 제공하도록 설계하였다. 이를 수신한 웹 서버는 개인키로 복호화하고 클라이언트 공개키(KUc)로 서명 검증하여 기밀성, 클라이언트 인증을 제공하고, 서명 검증하여 얻은 다이제스트를 원본 메시지의 다이제스트와 비교하여 무결성을 검사한다.

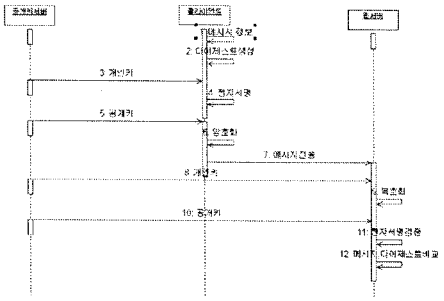

그림 6. 네트워크 전송 메시지 보안

IV. 결론

인터넷이 대중화 되어 있는 현대 사회에서 사용자의 식별 및 인증은 매우 중요한 과정이지만 사용자 식별이나 인증은 여러 가지 보안 취약점을 가지고 있는 실정이다. 이러한 문제점을 해결을 위해 본 논문에서는 안전한 네트워크 전송 메시지를 이용하여 웹 서비스 보안 시스템 연구하였다.

기존의 웹상에서 이루어지는 사용자 인증 방법에 있어 쿠키 메시지의 사용은 사용자 인증을 위해 사용되고 있지만 단순한 인증 기능 외의 보안 기능이 없다. 또한 쿠키 데이터가 평문 상태로 전송, 저장되기 때문에 보안에 취약하다.

이에 본 논문에서는 보안에 취약한 네트워크 전송 메시지에 전자 서명과 암호화에 RSA 공개키 알고리즘을 적용하고 메시지 다이제스트에 MD5 해시 알고리즘을 적용하여 기밀성, 인증, 무결성을 제공하였다. 이와 함께 네트워크 전송 메시지에도 보안 서비스를 적용하였다. 이로써 기존 네트워크 전송 메시지의 보안 취약점들을 해결하였다.

향후에는 키 관리의 다양한 방안과 장문의 문서에 대한 보안을 위한 대칭키 기반 보안서비스 설계가 요구된다.

참고문헌

[1] D. Kristol, "TTP State Management Mechanism" February 1997, RFC 2109.
http://www.ietf.org/rfc/rfc2109.txt

[2] Joon S. Park, Ravi Sandhu, and SreeLatha Ghanta, "BAC on the Web by
secure cookies" In proceedings of the IFIP WG11.3 Workshop on Database
Security, Champman & Hall, July 1999.

[3] William Stallings, "ryptography and Network Security: Principles and Practice,
Second Edition" Prentice-Hall Inc., 1999.

[4] Federal Information Processing Standards Publication. Digital Signature
Standard (DSS), 1994, FIPS PUB 186.

[5] R.L.Rivest, A.Shamir, and L.Adleman. " method for obtaining digital
signatures and public-key cryptosystems. Communications of the ACM"
21(2):120-126, 1978.

[6] R. Rivest, "he MD5 Message Digest Algorithm" April 1992, RFC 1321.
http://www.ietf.org/rfc/rfc1321.txt