웹 서비스 환경에서 작동하는 SOAP 메시지 접근제어를 위한 방화벽 설계

박수진O 김운용 최영근
광운대학교 컴퓨터과학과
{mos27O, wykim, ygchoi}@kw.ac.kr

Design of a Firewall to restrict SOAP message in WebService Environment

Sujin ParkO Wonyong Kim Yougkeun Choi
Dept. of Computer Science, Kwangwoon University

요 약

기존의 인터넷 환경에서는 내부 자원들을 보호하기 위하여 인터넷과 같은 외부 네트워크와 내부 네트워크 사이에 방화벽을 설치하고 내부 네트워크에 존재하는 정보와 자원들에 대한 트래픽을 사전에 방어 하거나, SSL, TLS, IPSec 과 같은 보안 프로토콜을 사용함으로써 신뢰할 수 있는 통신을 제공하여 왔다. 그러나 최근 HTTP와 XML이라는 플랫폼 독립적인 업계 표준을 사용하는 웹 서비스의 등장과 더불어서 기존의 보안 시스템으로는 웹 서비스 보안문제를 완전히 해결해 줄 수 없게 되었다. 이는 웹 서비스의 전송 프로토콜이 HTTP를 사용함으로써, 전송되는 SOAP 메시지가 기존의 방화벽과 같은 보안 시스템에 영향을 받지 않기 때문이다. 이에 본 논문에서는 웹 서비스 환경에서 SOAP 메시지 전송에 대해 액세스를 제한하는 방화벽을 제안 및 설계 한다.

1. 서 론

웹 서비스의 기본 사상은 플랫폼과 언어에 관계없이 RPC(Remote Procedure Call)를 가능하게 하자는데서 출발하며, 다양한 업계 표준 기술을 사용하여 웹을 통해 사용자나 다른 서비스에게 제공하기 위한 오픈 스탠더드 이다[5]. 이는 인터넷상의 애플리케이션들이 어떤 표준화된 인터페이스를 통해서 서로 간의 기능을 공유할 수 있게 함으로써 내용 중심의 공유에서 한 단계 진화된 기능 중심의 공유로 인터넷 이용 환경을 한층 발전시키는 역할을 하였다[6]. 이러한 웹 서비스의 활발한 움직임은 플랫폼 독립적인 XML의 활성화를 가져왔으나, 본질적으로 해결해야 할 보안 문제가 남아있다.

웹 서비스는 근본적으로 요청자와 웹 서비스 상호간의 SOAP 메시지 교환이라고 볼 수 있기 때문에 가장 기본적인 보안은 XML, 즉 SOAP 메시지 보안부터 시작해야 한다. 이러한 관점에서 W3C에서는 보안을 고려한 XML 스팩들을 기반으로 하여 SOAP 메시지 보안을 기술한 WS-Security를 발표하였다[9]. 이러한 보안 스팩들은 SOAP 메시지의 기밀성, 무결성, 인증, 부인방지 등의 기능을 제공하며, 웹 서비스 환경의 보안성을 한층 강화시켰다.

WS-Security는 기존의 네트워크 계층 보안 사양들과 함께 사용되는 호환성을 지니고 있다. 방화벽이 웹 서비스에 적용될 때는 IP 블러킹으로 허용되지 않는 접근을 차단한다. 이는 요청자가 불특정한 웹 서비스인 경우에는 적용이 어렵다는 단점이 있다.

이에 본 논문에서는 방화벽에서 요청자에 대한 인증을 하여 인증된 메시지에 보안토큰을 발행함으로써 인증된 메시지와 인증되지 않은 메시지를 구별하고, 후에 인증되지 않은 메시지가 방화벽을 통과하려고 하면 이를 차단하는 웹 서비스 환경에 기반한 방화벽을 제안한다.

본 논문 2장에서는 WS-Security를 사용한 웹 서비스 인증 방법을 간단히 알아보고, 3장에서는 제안하고자하는 웹 서비스 환경에서의 방화벽의 구성과 동작원리에 대해 알아보고, 4장에서는 결론을 맺는다.

2. WS-Security 인증 방식

인터넷을 통해서 계좌이체를 제공하는 웹 서비스가 존재한다고 가정하자. 고객 A가 계좌이체 서비스를 이용하기 위해서는 자신이 계좌의 정당한 주인임을 입증하는 과정이 필요하다. 고객 A는 웹 서비스를 요청하기 위한 SOAP 메시지를 작성한다. SOAP 메시지 작성시 <Header>의 <binaryLicense>엘리먼트 안에 X.509 인증서를 포함시킨다. 고객 A는 자신의 개인키를 사용하여 디지털 인증서를 암호화하여 함께 보냄으로써, 메시지를 보낸 사람이 틀림없이 자신이라는 것을 알 수 있게 한다. 서버인증도 같은 절차를 사용하여 이루어진다.

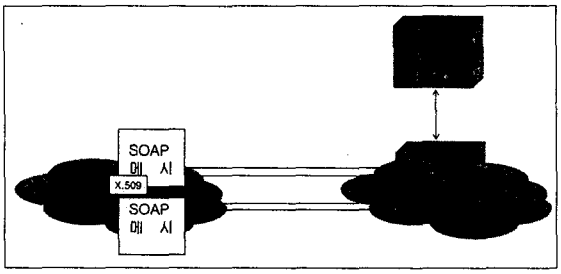

그림 1. WS-Security 인증 구성도

그림 2는 기존의 인증 방식의 구성도이다. 유효한 X.509 인증서를 가지고 있는 SOAP 메시지는 웹 서비스에 도달한다. 웹 서비스는 X.509 인증서가 첨부된 SOAP 메시지를 상호인증한다. 인증이 올바르게 이루어지면 웹 서비스에서는 요청을 수행하며 그렇지 않으면 거부한다. 이러한 방법에서는 인증서를 가지고 있지 않거나, 위조된 인증서를 가지고 있는 SOAP 메시지도 방화벽을 통과하여 웹 서비스에 도달한다. 방화벽에 IP 블러킹을 사용한 SOAP 메시지 차단 방법이 존재하지만 이는 요청자가 불특정 웹 서비스인 경우에 적용이 어렵다. 웹 서비스는 서비스를 실행함과 동시에 SOAP 메시지에 대한 인증을 담당해야 하는 부담을 안고 있다.

3. 웹 서비스 환경의 방화벽

본 논문에서 제공하는 방화벽은 크게 두 가지 역할을 담당한다. 첫째는 방화벽에서 인증의 역할을 담당한다는 것과 둘째는 인증이 된 메시지와 그렇지 않은 메시지를 분류하여 인증된 메시지는 웹 서비스와 통신을 가능하게 하며, 그렇지 않은 메시지는 차단하는 것이다.

3.1 인증 시스템 구성도

본 논문에서는 방화벽에서 SOAP 메시지를 인증하여 인증된 SOAP 메시지만을 웹 서비스에 전달하고 인증되지 않은 SOAP 메시지는 웹 서비스에 전달되지 못하도록 차단한다. 웹 서비스는 요청에 대한 실행만 담당하며 인증을 위한 알고리즘과 합의는 필요치 않다.

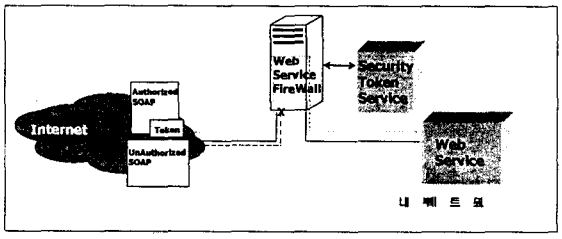

그림 2. 인증 시스템 구성도

그림 2은 인증 방화벽 구성도이다. WS-Security를 사용한 인증과의 차이점은, 기존에는 웹 서비스에서 수행하던 인증의 과정을 그림 2에서는 방화벽에서 수행하고 있다는 것이다. 인터넷에는 X.509와 같은 인증서를 가지고 있는 요청자와 위조된 인증서를 가지고 있거나 인증서를 가지고 있지 않은 요청자가 존재한다. 두 요청자는 웹 서비스에 서비스를 요청한다. 이 요청 메시지는 방화벽에서 Security Token Service와의 통신을 통하여 인증이 이루어진다. 이때 정상적인 인증이 이루어진 메시지는 방화벽으로부터 소유증명토큰을 제공 받는다. 후에 SOAP 메시지의 <Header> 엘리먼트에 방화벽에서 지정한 소유증명토큰이 있다면 인증의 과정은 끝난 것으로 간주되며 웹 서비스와의 직접통신이 가능해진다.

이 방화벽은 웹 서비스에게 인증 절차에 관한 부분을 대신해줌으로써 인증에 관한 웹 서비스의 절차를 생략 가능하게 해준다.

3.2 동작원리와 구성요소

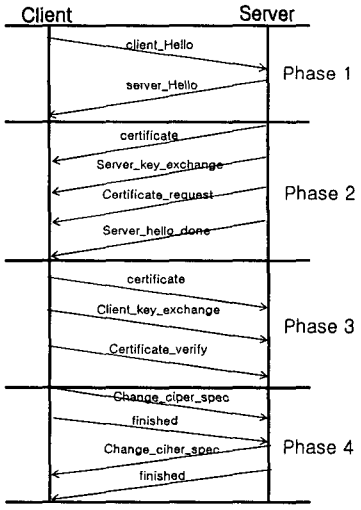

그림 3. 동작 방식

그림 3은 <WS-Secureconversation>과 X.509 인증서를 이용한 인증 시스템의 동작 방식을 나타낸다. 1단계에서 클라이언트는 서버에게 X.509 인증서를 요청한다. 2단계에서 서버는 클라이언트에게 자신의 인증서를 전송해준다. 3단계에서 클라이언트는 서버의 X.509 인증서에 담겨 있는 공개키를 이용해 임의의 난수를 암호화해 서버에게 전달한다. 4단계에서 서버는 자신의 비밀키를 이용해 클라이언트가 보낸 난수를 복호화시키고 그 값을 클라이언트에게 보내 클라이언트가 자신이 암호화한 값과 같은지 확인하면 인증의 절차는 끝난다.

일반적인 웹 서비스의 경우에는 웹 서비스의

서버에서 이러한 과정을 담당하지만 본 논문에서는 방화벽이 이러한 절차를 대신한다. 클라이언트에서 인증서 요청 메시지가 왔을 때 방화벽은 이를 서버에게 전달하지 않고 대신 방화벽이 직접 위의 2~4단계의 작업을 수행한다. 작업을 마쳐서 인증의 과정이 끝나면 방화벽은 더 이상 메시지에 관여하지 않고 클라이언트와 서버간의 메시지가 직접 전달 될 수 있도록 한다.

3.3 메시지 허용 차단

인증이 끝난 후에 방화벽은 소유증명토큰을 발행한다. 소유증명토큰은 클라이언트가 서버와 정식 인증절차를 밟았다는 것을 증명해주는 토큰으로, 이후 클라이언트의 SOAP 메시지 Header 부분에는 직접 통신이 끝날 때까지 항상 이 토큰이 포함된다.

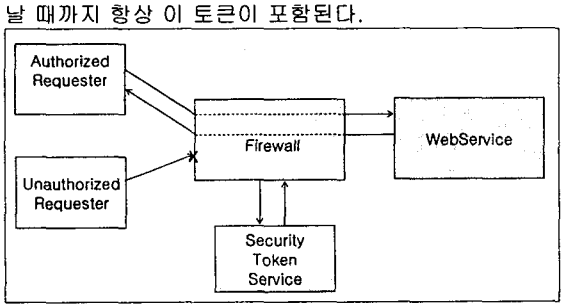

그림 4. 메시지 허용 차단

그림 4는 소유증명토큰을 가지고 있는 인증된 요청자가 방화벽을 통과하여 웹 서비스와 통신하는 모습과, 인증되지 않은 요청자가 방화벽에서 차단당하는 모습을 도식화한 것이다. 방화벽은 클라이언트로부터 온 SOAP 메시지의 헤더 부분을 검사하여, 소유증명 토큰이 있는 메시지는 인증의 과정을 생략하고 웹 서비스 서버에게 전달한다. 그리고 소유증명 토큰이 없는 SOAP 메시지는 차단한다.

3.4 비교

기존의 웹 서비스 인증은 웹 서비스 서버에서 이루어졌다. 인증이 이루어지기 위해서 웹 서비스자체에 인증에 관한 메커니즘과 그에 관한 합의된 알고리즘이 필요했다. 웹 서비스는 서비스의 실행과 동시에 보안에 관한 사항까지 제공해야 하는 부담을 안고 있었다. 또한 요청을 받는 메시지마다 인증을 거쳐야 했기 때문에 속도와 효율적인 면에서 제약이 있었다. 이에 본 논문에서는 방화벽에서 웹 서비스 인증에 대한 부분을 담당하도록 하여, 웹 서비스가 성능 향상된 서비스를 제공할 수 있도록 한다.

4. 결론 및 향후 연구방향

본 논문에서는 웹 서비스 환경에서 작동하는 방화벽을 제안하였다. SOAP 메시지는 항상 방화벽을 거쳐야 하며, 인증서의 소유증명을 통해서 확인되지 않은 메시지는 내부 네트워크에 존재하는 웹 서비스에 도달하지 못한다. 이는 웹 서비스에게 보안에 관한 부담을 덜어줌으로써 보다 향상된 서비스를 제공할 수 있게 하였다.

더 나아가 웹 서비스 환경에서 작동하는 방화벽과 현재 사용되고 있는 방화벽과의 호환성 문제, 인증을 함으로써 발생하는 속도와 성능상의 문제 등은 앞으로 더 연구해야 할 과제이다.

참고 문헌

[1] http://www-903.ibm.com/developerworks/kr/webservices/library/ws-secmap.html, 웹 서비스 세계에서의 보안, IBM, 2003.

[2] http://kiie.org/iemagazine/9_2/ieforum.html 소프트웨어개발 및 배포방식의 변화 " 웹서비스", ie매거진, 2002

[3] http://home.postech.a.kr/~hiro/cs499/0320_pki.html

[4] http://www.microsoft.com/korea/msdn/library/dnglobspec/html/ws-secureconversation.asp, 웹 서비스 보안 통신 언어, 2002

[5] Blake Dournaee," XML-Security" ,McGraw-Hill, 2002

[6] Ben Galbraith, Whitney Hankison, Andre Hiotis, Murali Janakiraman, Prasad D.V, Ravi Trivedi, David Whitney, " Professional Web Services Security", Wrox Press, 2002

[7] 이한수, " 웹 서비스 실전 프로그래밍" 한빛미디 어㈜, 2002

[8] 정지훈, " 웹 서비스" 한빛미디어㈜, 2002

[9] 이해규, 이상수, 김문규, " 웹 서비스 보안" 한국정보처리학회지 제 9 권 제 4 호, 2002.7