쿠키 보호 시스템 설계

최향창[0] 최은복[00] 노봉남
전남대학교 전산학과[0]
전주대학교 컴퓨터 공학과[00]
(hcchoi[0], eunbog[00], bongnam)@athena.jnu.ac.kr

A Design for Cookies Protection System

Hyang-Chang Choi[0] Eun-Bog Choi[00] Bong-Nam Noh
Dept. of Computer Science, Chon-nam University
Dept. of Computer Engineering, Jeon-Ju University

요 약

현재 웹을 이용해서 수많은 정보들이 움직이고 있다. 이러한 웹에서 사용자에 대한 정보의 편의를 위하여 쿠키가 이용되고 있다. 이러한 쿠키의 가장 큰 문제점은 클라이언트 영역에 평문으로 저장되므로 쉽게 공격자에 의해 쿠키정보가 위조되어 사용될 수 있으며 쿠키에 저장되어진 정보들 또한 쉽게 공격자에 의해 노출될 수 있다. 본 논문은 쿠키를 안전하게 사용할 수 있도록 쿠키 보호 시스템에 대해서 제안한다. 쿠키를 암호화하기위한 키들을 모아놓은 쿠키 보호 키 관리 시스템을 유지하여 사용자 인증쿠키를 생성하고 이 인증쿠키를 이용해서 쿠키를 보호한다.

1. 서 론

HTTP프로토콜은 이전의 상황들을 기억하지 못하는 프로토콜이다[1]. 이러한 단점을 보안하기위한 방법이 쿠키이며 쿠키정보는 클라이언트 영역에 평문으로 저장되어진다[2]. 쿠키 정보는 쉽게 요청되어지기 때문에 공격자가 쿠키의 정보를 얻어오는 코드를 삽입하게 되면 이 쿠키에 삽입된 정보는 쉽게 노출 되고 이용되어질 수 있다.

쿠키에 대한 문제점을 해결하기 위해서는 쿠키에 대한 정보가 공격자에게 노출되지 않도록 쿠키를 요구하기 이전에 인증단계를 거치도록 하여 쿠키정보를 이용하도록 하면 되지만 이 방법만으로는 도청에 의한 쿠키정보의 노출은 막을 수 없다. 따라서 쿠키정보가 노출되었다 하더라도 보호되기 위한 쿠키의 비밀성, 쿠키정보의 위조에 대한 방어를 위한 쿠키의 무결성이 동시에 제공되어져야 한다[4].

쿠키는 웹 서비스를 사용하고자 하는 사용자의 정보를 각각의 클라이언트 영역에 저장하므로 쿠키를 암호화 시키는 키를 사용자별로 다르게 유지해도 아무 상관이 없다. 따라서 사용자가 제공하는 쿠키를 암호화 및 복호화 하는데 사용되는 쿠키 비밀키를 관리하기위한 서버를 만들고 이 서버에서 사용자의 인증쿠키를 생성한다. 이 인증쿠키를 바탕으로 웹 서비스를 제공하는 시스템이 서비스를 요청한 사용자의 쿠키를 암호화하여 보호할 사용자별 쿠키 보호키를 얻어낸다. 이 쿠키 보호키에 의해 쿠키 정보는 암호화 및 복호화 되어 웹 서비스 시스템과 웹 사용자간에 사용된다. 이러한 방법에 의해 쿠키를 보호하는 시스템이다.

본 논문의 구성은 다음과 같다. 2절에서는 쿠키를 보호하기 위한 방법에 대해 설명한다. 3절에서는 현재 안전한 쿠키[5,6]와 강화된 쿠키보호[8] 방법에 대해 살펴본다. 4절에서는 쿠키보호 시스템에 대해서 제안하고 5절에서는 제안된 방법에 대해 분석하고 6절에서 결론을 제시한다.

2. 쿠키를 보호하기 위한 방법

2.1 인증된 사용자만 쿠키 접근

쿠키는 평문으로 웹 사용자 시스템의 클라이언트 영역에 저장된다. 사용되어질 때 공격자도 쉽게 쿠키의 내용을 가져올 수 있다[9]. 따라서 클라이언트에 저장되어 있는 각각의 쿠키의 내용이 공격자에게 노출되지 않도록 쿠키가 저장되는 영역의 접근을 인증과정을 통해 쿠키를 생성한 사용자나 서비스를 제공해줄 정상적인 웹 사이트만 사용할 수 있도록 한다면 쿠키는 보호될 수 있다.

2.2 네트워크상에 이동중인 쿠키정보 암호화

쿠키 정보는 네트워크 상에서 도청 되어 공격자에 의해 재이용 될 수 있는데 쿠키의 도청을 막기위해서 TLS[7]를 사용할 수 있다. TLS에 의해서 웹 브라우져와 웹 서버 사이에 자료에 대한 흐름 자체를 암호화 하는 것이다. 이 방법에서 사용자의 인증은 TLS가 제공하는 인증 방법을 통해서도 가능하다. 하지만 클라이언트의 시스템 안에 저장되는 쿠키 정보는 평문이기 때문에 근본적인 쿠키의 취약점[8]은 보호되기 힘들다.

2.3 쿠키 데이터를 암호화하여 저장

사용자에게 쉽게 노출되어질 수 있는 쿠키 정보를 보호할 수 있는 또 다른 방법은 쿠키정보를 암호화[4]하여 저장하는 것이다. 암호화를 통해 저장한다면 쿠키 정보가 평문이 아니므로 노출되어도 암호화키를 알아내거나 암호화된 정보를 복호화 못하는 이상 이 쿠키의 정보는 무용지물이다. 하지만 이 방법만으로 사용자에 대해 신뢰를 제공하지 못한다. 또한 쿠키의 정보를 암호화 하게 되면 암 복호화 시간이 추가로 필요하다.

3. 관련연구

본 장에서는 안전한 쿠키(Secure Cookies)[5,6]와 쿠키 보호 강화 방법[8]에 대해서 고찰한다.

3.1 안전한 쿠키(Secure Cookies)

사용자의 인증과 비밀성 무결성을 제공하는 쿠키이다. 이 쿠키는 일반적인 쿠키에 암호화 기법을 적용해 쿠키를 보호한다.

3.1.1 인증 제공

사용자 인증(User Authentication)은 주소(IP)기반, 패스워드 기반, 전자서명 기반 인증이 있다.

주소기반 인증은 쿠키 정보에 주소를 저장하는 쿠키를 두어 인증하게 하는 방법으로 쿠키정보에 대한 사용이전에 주소쿠키를 통하여 상대방을 인증하고 인증되면 통신한다. 이 방법은 주소 스푸핑공격[3]을 통해서 주소를 위조할 수 있기 때문에 확실하게 안전한 인증이 될 수 없다. 둘째 패스워드기반 인증은 웹 서버의 패스워드를 클라이언트 영역에 해쉬 값으로 저장하여 쿠키를 사용하기 이전에 클라이언트 영역에 저장된 해쉬된 쿠키 값을 웹 서버가 자신의 패스워드를 해쉬하여 비교 하여 인증하는 방법이다. 사전공격(dictionary attacks)에 의해 패스워드를 알아내는 것을 막기 위해 패스워드를 해쉬하여 저장한다. 마지막으로 전자서명기반인증은 전자 서명 방식에 의해 인증하는 방법으로 만약 공개키를 알고 있다면 DSA나 RSA와 유사하게 전자서명 할 수 있는데 이와 같은 방법에 의해 인증하는 방법이다[4].

3.1.2 무결성 제공

공격자에 의해 위조된 쿠키에 의해 쿠키 정보가 웹서버에 의해 이용될 수 있으므로 쿠키 데이터에 대한 무결성 확인이 필요하다. 이러한 방법에는 공개키 기반, 비밀키 기반 무결성 확인이 있다. 공개키 기반 무결성 제공방법에는 쿠키 정보를 개인키로 다이제스트 한 쿠키를 저장해 두고 쿠키 정보를 사용하기 전에 공개키를 이용해 쿠키 정보를 다이제스트 한 결과와 비교함으로써 이상이 없는지 확인하여 무결성을 확인한다. 다른 하나인 비밀키 기반 무결성 제공방법은 웹 서버와 개인사용자간에 비밀키를 이용해 무결성을 확인한다. 쿠키 정보를 다이제스트 한 정보를 저장해 두고 쿠키를 사용하기 이전에 쿠키 정보를 다이제스트 해보고 이미 다이제스트된 쿠키데이터와 비교해 봄으로서 무결성을 확인한다.

3.1.3 비밀성 제공

중요한 쿠키 정보에 대해서 암호화 하여 쿠키로 저장함으로써 비밀성을 제공한다. 사용자가 제공한 쿠키정보가 저장되기 전에 암호화 되어 쿠키 값으로 저장되어진다. 이 쿠키 값을 도청했다 할지라도 암호화 되어있으므로 암호화를 해독하지 못하면 무용지물이 되므로 안전하다.

3.2 쿠키 보호강화

쿠키 보호를 한 단계 높이기 위해서 추가할 쿠키 보호 방법들에는 다음과 같은 것들이 있다.

3.2.1 로깅(Logging) 기법을 이용한 쿠키 불법사용 보호

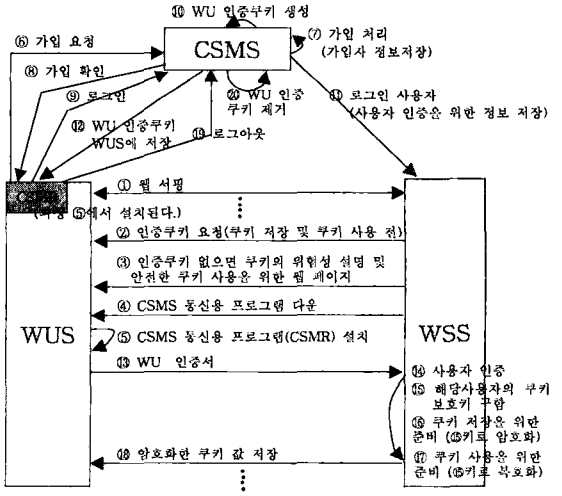
쿠키 정보는 공격자에 의해 조작되어질 수 있으므로 쿠키를 이용해서 공격자는 특정한 요청을 요구할 수 있다. 이러한 행위들은 정상적인 쿠키요구와 다르게 불 특정하게 쿠키 정보가 변화되어 정보를 요청하려 시도할 것이다. 이러한 쿠키요구에 대한 행위에 대해 판단하여 불법적으로 웹 서버에 접근하려는 침입자에 대응할 수 있다. 쿠키의 로그를 이용해 침입자의 이상행위에 대해 판단하려는 것이다. 특정한 PC에서 쿠키에 의해 요구되어지는 모든 경우에 대해서 로그정보를 유지하는 것이다.

3.2.2 쿠키 사용 전 내용 점검을 통한 보호

쿠키정보는 단순하게 사용자에 의해서 필요한 정보가 저장되어지므로 침입자에 의해 쿠키 데이터 내에 악의적인 코드가 포함될 수 있다. 따라서 쿠키의 정보를 이용하기에 앞서 쿠키의 내용에 대한 점검이 필요하다. 예를 들어 쿠키정보에 바이러스나 악의적인 스크립트를 삽입하여 공격하는 경우[8]에 대해서 쿠키가 사용되기 이전에 알아내어 조치 한 후에 쿠키정보를 이용한다면 보다 안전하게 쿠키를 사용할 수 있다.

4. 쿠키 보호시스템 설계

쿠키 보호 시스템은 크게 쿠키의 값을 보호하기 위한 키들을 관리하는 쿠키 보호키 관리 시스템(Cookie Security Key Management Systems)과 이 시스템을 이용하는 웹 서비스시스템(Web Service Systems), 이러한 웹 사이트에 접속하여 일을 처리하는 웹 사용자 시스템(Web User Systems)으로 크게 나누어 볼 수 있다. 이러한 쿠키 보호 시스템의 구조는 [그림1]과 같다. 쿠키 보호키 관리시스템에 대한 접속은 데이터의 안전을 위해 TLS[7]를 프로토콜을 사용하여 데이터를 전송 한다.



[그림1] 쿠키 보호 시스템 구조

4.1 시스템에 유지되는 정보 및 키

쿠키 보호키 관리 시스템(CSMS)에서 유지되는 사용자정보는 [표 1]과 같다. 유지하는 정보는 사용자의 기본 정보와, 쿠키를 보호화 하기위해 사용되는 비밀키, 인증 쿠키를 발행하기 위한 정보들을 유지하고 있다.

[표 1] CSMS에서 관리되는 사용자 정보

	저 장 내 용	생성시	생성	저장
(1)	CSMS 접속 ID(유일성 보증)	사용자	⑥	⑦
(2)	CSMS 접속을 위한 Password	사용자	⑥	⑦
(3)	쿠키 보호 키	사용자	⑥	⑦
(4)	일시(최근에 WU 인증쿠키 생성이나 폐기된때 시간)	CSMS	⑩,⑳	⑩,⑳
(5)	CSMS 접속 횟수(접속 종료시 기존정보에 +1)	CSMS	⑳	⑳
(6)	CSMS 접속 ID와 CS 비밀키로 암호화 한 데이터	CSMS	⑩	⑩

웹 서비스를 제공하는 시스템(WSS)에서 유지되는 사용자 정보는 [표 2]와 같다. 이 정보는 사용자의 인증쿠키의 무결성을 검사하고 웹 사용자를 인증하기 위한 기본정보를 저장한다. [표 1]의 (6)은 사용자 ID를 암호화 했으므로 유일하며 공격자가 웹 사용자의 ID를 알고 있어도 CS 비밀키를 알지 못하면 웹 사용자의 쿠키 보호키를 알아 낼 수 없도록 하기 위함이다.

[표 2] WSS에서 유지되는 사용자 정보

	저 장 내 용	생성자	생성	저장
(1)	[표 1]의 (6)	CSMS	⑪	⑫
(2)	[표 1]의 (3)	사용자	⑮	⑫
(3)	[표 1]의 (4)	CSMS	⑩,⑳	⑩,⑳
(4)	[표 1]의 (5)	CSMS	⑳	⑳

[표 3]의 WU 인증 쿠키는 로그인 한 사용자의 ID와 일치하는 사용자 정보를 찾아 [표 1]에 저장되는 (4)와 (5)를 CS 비밀키로 해쉬 한 후에 CSMS 접속 ID를 CS 비밀키로 암호화 한 데이터 붙여 생성한다.

[표 3] WUS에서 유지되는 사용자 정보

	저 장 내 용	생성자	생성	저장	폐기
(1)	WU 인증쿠키	CSMS	⑱	⑲	⑳

다음으로 [표 4]는 각각의 시스템이 유지하는 키 정보이다. CS 비밀키는 사용자 인증 쿠키를 생성하기 위해 사용되는데 이 키를 안전하게 배포하기 위해 [표 4]의 (2),(3)을 이용한 공개키 암호화 방식을 사용한다.

[표 4] 시스템별로 유지하는 키 정보

	키	생성자	관리	사용 용도
(1)	CS 비밀키	CSMS 관리자	CSMS	⑩, ⑭
(2)	WSS 공개키	WSS 관리자	CSMS	CS 비밀키 배포
(3)	WSS 개인키	WSS 관리자	WSS	

4.2 쿠키 보호 시스템 시나리오

다음은 쿠키를 사용하기 위한 각 상황별 시나리오이다.

4.2.1 쿠키 보호키 관리 시스템 미 가입 사용자 이용절차

쿠키 보호키 관리시스템의 웹 서비스 시스템들은 웹 서핑중에 쿠키를 사용하거나 저장 하려고 한다면 웹 서비스 시스템은 인증 쿠키를 요청한다. 만약에 인증쿠키가 존재하지 않으면 웹 보호키 관리 시스템에 접속 하게 할 프로그램을 다운로드 할 수 있도록 웹 페이지 화면을 제공한다. 사용자가 이 웹 페이지를 통해 프로그램을 다운 받아 설치한 후 접속하여 쿠키 보호키 관리 시스템에 가입할 수 있다. 가입에 따른 사용자 데이터의 저장 정보는 [표 1]에 나와 있다. 이 설명은 [그림1]의 ① 에서 ⑧까지를 의미한다.

4.2.2 쿠키 보호키 관리 시스템 가입 사용자 인증쿠키 획득

쿠키 보호키 관리시스템의 가입 절차가 끝났다면 다음은 인증 쿠키를 얻어 오는 과정이다. 먼저 사용자가 로그인 과정을 거치고 인증되면 이 사용자에 해당하는 인증쿠키를 쿠키 보호키 관리 시스템이 생성하여 웹 사용자 영역에 쿠키정보로 저장한다. 이렇게 저장된 인증쿠키의 생성, 저장, 폐기에 대한 시기는 [표 1]에 나와 있다. 이후에 웹 사용자의 쿠키 정보의 무결성과 사용자에 대한 인증을 제공하기 위해 값들을 [표 2]과 같이 웹 서비스 시스템에 저장한다. 이에 대한 과정은 로그인 해서 인증쿠키를 얻어내어 저장하는 과정까지인 ⑨에서 ⑫까지의 내용이다.

4.2.2 인증쿠키 획득 한 후의 쿠키 보호키 구함

쿠키 정보를 사용하려고 할때 클라이언트 영역에 저장되어있는 인증쿠키를 요구한다. 이 인증쿠키 정보에서 암호화된 CSMS 접속 사용자 ID를가지고 이에 해당하는 사용자 정보를 찾고 [표 2]에서 저장한 양식의 (3), (4)의 데이터를 같은 방법으로 해쉬해 본후 결과를 비교해 본다면 인증쿠키의 무결성을 확인해 볼 수 있다. 무결성에 이상이 없다면 이에 해당하는 쿠키 보호키를 구해 이 쿠키 보호키를 이용해 암호화 통신을 하면 안전한 통신을 할 수 있다. 지금까지의 내용은 [그림1]의 ⑬ ~ ⑱에서 보여준다.

5. 제안된 방법에 대한 고찰

안전하게 쿠키를 사용하기 위해 쿠키를 암호화하는 키 관리 서버를 두고, 이 서버에 여러 개의 웹 서비스 시스템과 웹 사용자를 가입하도록 하게하고 쿠키 보호키 관리 시스템에 사용자가 제공한 쿠키 보호키를 이용해 쿠키 정보를 암호화하여 보호하는 방법이다. 이 방법은 하나의 쿠키 보호키 관리 시스템에 여러 개의 웹 서비스 시스템과 웹 사용자를 둘 수 있다. 또한 쿠키 암호화키를 클라이언트 사용자가 결정함으로써 서로 다른 쿠키 암호화키를 유지하기 때문에 하나의 비밀키를 유지하여 암호화하는 시스템에 비해 비밀키 노출에 따른 문제를 최소화 할 수 있다.

6. 결론 및 향후 연구방향

이 방법은 쿠키 보호키 관리 시스템을 두어 쿠키를 안전하게 보호하기위한 키 관리를 별도로 함으로서 기존에 사용되고 있는 웹 서비스 제공 사이트에 쉽게 적용할 수 있다. 이 시스템은 암호화 방식을 사용해서 쿠키의 무결성, 비밀성, 사용자에 대한 인증을 제공한다. 웹 사용자 인증 쿠키는 쿠키 보호키 관리 시스템에서 종료하기 이전까지만 유효하므로 시스템을 재기동 하거나 다른 컴퓨터에서 사용하고자 한다면 쿠키 보호 키 시스템 로그인 과정을 실행해야 할 필요가 있다. 향후에는 시스템에 로깅 기법과 쿠키 내용 사전점검 방법을 적용해서 보다 강화된 쿠키보호 시스템에 대해 구현해 보고자 한다.

7. 참고문헌

[1] R. Fielding and L. Montulli, "Hypertext Transfer Protocol HTTP/1.1,"RFC2068, Jan., 1997.

[2] D. Kristol and L. Montulli, "HTTP State Management Mechanism," RFC2109, Jan, 1997.

[3] Anonymous, "리눅스 보안의 모든것", SAMS, pp.224-252, 1999.

[4] H.X. Mel and Doris Baker, "보안과 암호화 모든 것," Addison Wesley, 2001.

[5] J. Park, "A Secure-Cookie Recipe for Electronic Transactions," 1999.
http://citeseer.nj.nec.com/park99securecookie.html

[6] J. Park and R. Sandhu, " Secure Cookies on the Web," IEEE Internet Computing, 2000.

[7] E. Rescorla, "SSL and TLS," Addison-Wesley, 2001.

[8] V. Khu-smith and C. Mitchell, "Enhancing the security of cookies, ICISC, 2001.

[9] 임대호, "악성 코드에 의한 HTTP Cookie 유출 문제점 및 대책", CERTCC-KR 권고문, 2000.