웹 환경에서 쿠키 재전송 공격에 대한 탐지기법

이재식*, 박지수**1), 손진곤*
*한국방송통신대학교 대학원 정보과학과
**경기대학교 교양학부
e-mail:iics4u@knou.ac.kr

Detection Techniques against Cookie Replay Attack in Web Environment

Jae Sik Yi*, JiSu Park**, Jin Gon Shon*
*Dept. of Computer Science, Graduate School, Korea National Open University
**Division of General Studies, Kyonggi University

요 약

웹 3.0 시대를 맞으면서 인터넷과 PC의 발전은 웹 서비스 이용을 대폭 증가시켰고, 이러한 웹 환경에서 이용자가 인증 절차를 거치지 않고 임의로 접속하는 공격을 방어하기 위한 정보보호 대책이 중요하다. 쿠키는 웹사이트에 접속 시 웹 서버가 한번 발행하면 이후 이용자의 웹페이지 이동마다 인증 절차를 거쳐야 하는 번거로움을 간단하게 하는 편리한 수단이다. 그러나 공격자가 쿠키를 스니핑하여 웹페이지를 새로 고침 하는 공격으로 인증 절차를 우회하여 정상 이용자로 가장하는 위험이 있다.

본 논문은 이용자의 정상 로그인 시의 쿠키 등을 해시 함수로 암호화한 값을 데이터베이스에 저장하였다가 쿠키 재전송 공격이 의심되는 이벤트가 발생하면 현재 웹브라우저의 쿠키 등을 해시 함수로 암호화한 값과 서로 비교함으로써 쿠키 재전송 공격을 탐지하는 기법을 제안한다.

1. 서론

웹 3.0 시대의 환경에서 HTTP 쿠키는 인터넷 이용자가 웹브라우저로 웹사이트에 접속할 때 웹 서버에 의해 이용자의 PC에 자동으로 만들어진다. 쿠키는 이용자의 아이디, 패스워드를 비롯한 검색한 콘텐츠, IP 주소 및 세션아이디 등의 다양한 정보를 담고 있는 일종의 임시 정보파일이다. 쿠키는 이용자가 웹사이트에 접속할 때 아이디와 패스워드를 입력하여 한번 인증을 받으면 일정시간 동안 다른 웹페이지들을 이동할 때마다 다시 인증을 하지 않아도 되는 편리한 수단이다[1, 2].

또한 웹 환경에서는 다양한 취약성을 노린 공격들이 있으며, 인증을 우회하기 위한 패스워드 무차별 공격, 불충분한 인증 절차 공격, XSS(Cross Site Script) 공격 및 변조 공격이 있다. 쿠키는 공격자가 스니핑하여 웹 서버에 재전송함으로써 정상적인 인증 절차를 거치지 않고 정상 이용자로 가장하는 수단으로 악용될 위험이 있다.

공격자는 이용자의 컴퓨터를 악성 코드로 감염시킬 수 있고 악성 코드로 쿠키는 공격자에게 유출될 수 있다[2, 3]. 따라서 쿠키 재전송 공격에 대한 방어를 위하여 쿠키 재전송 공격에 대한 탐지기법들이 연구되었다. 그러나 인위적인 사용자 토큰 발행과 콜백 페이지를 생성하고 공격 탐지를 위해 정상 이용자의 웹페이지 이동마다 사용자 토큰을 비교하여 프로세스가 복잡하다[8, 9]. 이는 다양한 웹 공격의 위협이 많은 환경에서 긴 탐지 시간으로 공격 후에 방어가 될 수도 있어 위험하다.

본 논문은 웹서버에서 정상 로그인 시의 쿠키 중 중요한 정보 값들을 해시 암호화해서 데이터베이스에 저장해 둔다. 다음에 공격자가 쿠키를 스니핑하여 재전송 공격을 하면 현재 웹브라우저 쿠키 정보의 해시 값과 데이터베이스에 저장된 이용자 쿠키의 정보 해시 값을 비교해서 다르면 쿠키 재전송 공격으로 의심하여 탐지하는 기법을 제안한다.

2. 관련 연구

2.1 이용자 인증 관련 웹공격의 종류

이용자가 웹서버에 접속하기 위해서는 웹브라우저의 주소창에 URL을 입력하고 요청하며, 웹 서비스를 이용하면서 많은 정보들이 송·수신된다. 웹 환경에서 전송되는 정보들을 공격자가 도청하여 악의적으로 변조함으로써 웹 공격이 시작되며, 이용자 관련 공격 방법들은 <표 1>과 같다[3, 4].

<표 1> 웹 환경에서 이용자 관련 공격 방법들

서비스	공격 형태	사용프로토콜	공격 효과
인증	무차별 공격	Brute Force Attack	사용자 계정 획득
	불충분한 인증	URL Attack	관리자 권한 획득
	취약한 비밀	브루트 포스	패스워드 해킹

1) 교신저자

	번호 이용		
인가	자격증명/세션 예측	Session Hijacking	세션 공격
	불충분한 인가	Network Sniffer	디렉터리 접근 및 세션 공격
	세션 고정	HTTP request	쿠키 고정을 겨냥한 공격
Client 측 공격	컨텐츠 스푸핑	Contents Spoofing	허위 컨텐츠 제공
	XSS	Cross-site Scripting	URL에 내장된 코드 에코

2.2 사용자 인증에서 보안 강화 기법

재전송 공격에 안전한 싱글 사인온 인증 시스템을 위해 인증 서버는 인증정보 생성에 사용될 임시 값(Random Nonce) 및 원타임 패스워드(OTP)를 생성하였다[5]. 서버 접속 시 사용자 인증시스템인 강화 커버로스(kerberos)는 인증기법으로 사용자 정보 외에 보안환경의 기본 정보로 사용자 IP 주소를 사용하였다[6].

웹서버에서는 사용자의 인증 정보를 텍스트 파일이 아닌 해시함수로 암호화된 값을 저장하고 클라이언트에서도 해시함수로 암호화된 값을 전송하여 서로 비교한다[7].

2.3 쿠키 재전송 공격 및 탐지 기법

쿠키 재전송 공격에 대한 탐지 기법은 웹서버의 로그인 페이지에서 이용자가 정상 로그인 시 쿠키 및 인위적으로 생성한 사용자 토큰을 정적 배열 리스트란 데이터 구조에 저장해 둔다[8, 9].

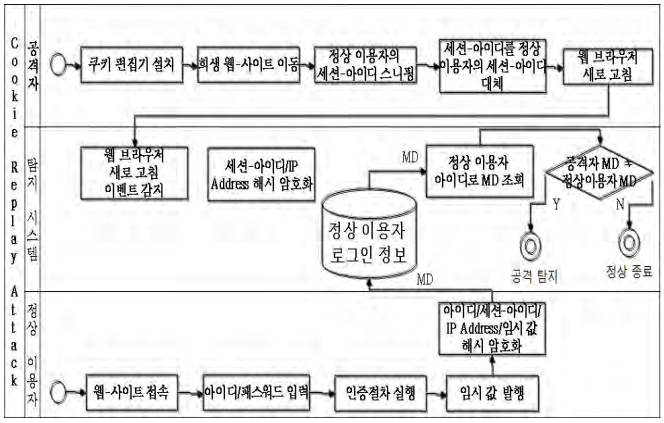
정상 이용자가 웹페이지를 이동할 때 마다 쿠키 정보가 스니핑 되어 쿠키 재전송 공격을 의심하여 정적 배열 리스트에서 사용자의 사용자 토큰이 저장된 인덱스 번호를 암호화하여 웹페이지로 전송한다. 공격자가 로그인 않은 경우의 공격으로 공격된 웹페이지에 세션정보가 존재하면 인위적으로 만들어진 콜백 페이지로 이동시키고 세션에 사용자 토큰을 저장한다. 다시 로그인 페이지로 이동시켜 공격된 웹페이지의 사용자 토큰과 콜백 페이지의 사용자 토큰을 비교하여 같으면 정상 이용자로 만약 다르면 공격자로 판단한다[8, 9].

이 탐지 기법에서는 웹페이지가 쿠키 재전송 공격이라면 사용자가 정상 로그인 시에 발행된 사용자 토큰을 공격자가 가지고 있지 않는 점을 이용했다.

3. 쿠키 재전송 공격에 대한 탐지 기법

3.1 쿠키 재전송 공격 및 탐지 프로세스 개요

이용자의 정상적인 로그인과 공격자가 쿠키 재전송 공격을 실행한 후에 공격을 탐지하는 전반적인 프로세스는 (그림 1)과 같다.



(그림 1) 쿠키 재전송 공격에 대한 탐지 프로세스

정상 이용자는 아이디/패스워드 등 자신의 인증 정보를 사용하여 인증 절차를 거쳐 웹사이트에 접속하게 된다. 이때 정상 로그인 시의 쿠키 정보를 해시 암호화하여 데이터베이스에 저장하였다가 공격자가 정상 이용자의 쿠키를 스니핑 한 후 쿠키 재전송 공격이 시도되는 이벤트 발생이 감지되면 탐지 시스템이 작동된다, 웹브라우저의 쿠키 등을 해시 암호화한 값과 데이터베이스에 저장된 정상 이용자의 쿠키 등의 해시 암호화 값을 서로 비교하여 만약 두 값이 다르면 쿠키 재전송 공격으로 의심하여 탐지하는 기법이다.

3.2 쿠키 재전송 공격 및 탐지 시나리오

쿠키 재전송 공격 및 탐지 시나리오는 로그인 절차, 공격 절차, 탐지 절차로 나눈다.

로그인 절차는 다음과 같다.

1) 정상 이용자가 공격대상 웹사이트에서 정상적으로 로그인 절차를 거친다.
2) 정상 이용자가 로그인에 성공한다.
3). 정상 이용자의 로그인 정보를 해시 암호화 시 사용할 솔트로 임시 값을 발행한다.
4) 정상 이용자의 쿠키 정보 중 세션아이디, IP 주소 및 임시 값을 해시 함수를 이용하여 암호화 한다.
5) 해시 함수 암호화 값(MD)을 이용자 아이디를 기본 키로 데이터베이스의 이용자 로그인 이력 테이블에 저장한다.

공격 절차는 다음과 같다.

1) 공격자가 정상 이용자의 쿠키 정보를 스니핑하기 위해 인터넷에서 쿠키 편집 프로그램을 다운로드 받아 공격자 PC에서 작동하게 한다.
2) 웹브라우저에서 공격대상 웹사이트로 이동한다.
3) 쿠키 편집 프로그램을 실행시켜 정상 사용자의 로그인에 사용된 쿠키를 스니핑 한다.
4) 스니핑 된 정상 이용자의 쿠키로 웹브라우저의 url을

편집한다(또는 쿠키 에디터를 이용하여 쿠키를 스니핑 된 쿠키로 대체한다).

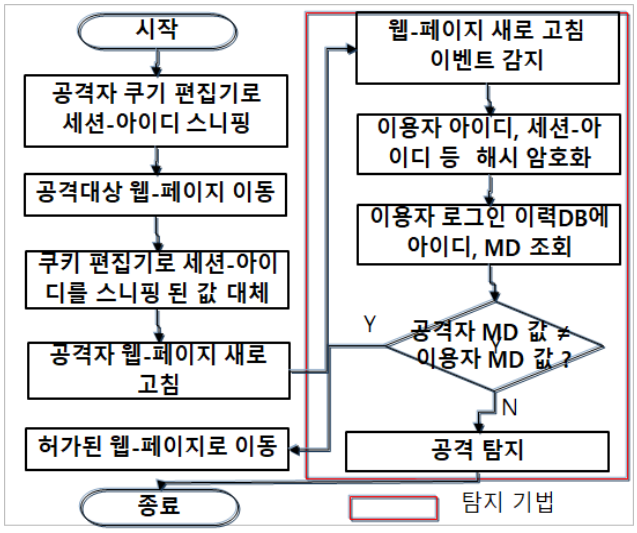
5) 공격을 위해 웹브라우저를 새로 고침 한다.

공격 탐지 절차는 다음과 같다.

1) 공격대상 웹브라우저에서 공격을 위한 새로 고침 이벤트가 감지된다.
2) 웹브라우저의 쿠키 정보 중 세션아이디, IP 주소를 해시 함수를 이용하여 암호화 한다.
3) 데이터베이스의 이용자 로그인 이력 테이블에서 이용자 아이디를 PK로 해시 함수 값을 조회한다.
4) 웹브라우저의 해시 함수 MD와 데이터베이스의 해시 함수 MD를 비교한다.
5) 만약 두 MD가 다르면 쿠키 재전송 공격으로 공격자의 공격을 탐지한다.

공격자는 쿠키 편집 프로그램을 이용하여 정상 이용자의 쿠키를 스니핑 하지만 웹사이트에 접속한 PC의 IP 주소가 다르고 정상 이용자에게 발행된 임시 값을 가지고 있지 않아 다른 입력 값이 사용된 해시 함수의 MD는 다르게 된다.

쿠키 재전송 공격 및 탐지 시나리오를 나타내는 순서도는 (그림 2)와 같다.



(그림 2) 쿠키 재전송 공격 및 탐지 순서도

4. 검증

4.1 쿠키 재전송 공격 탐지 프로세스 비교

쿠키 재전송 공격에 대한 탐지 여부는 각자의 기법으로 관련 연구기법과 제안 기법 모두 탐지하는 것으로 판단되고 검증의 초점이 아니어서, 다양한 웹 공격 위협이 많은 요즘 환경에서 보다 중요한 탐지 시간을 검증 대상으로 하였다.

검증을 위하여 정상 이용자가 로그인 후 웹페이지 이동은 10회로, 공격자의 공격은 3회 시도로 가정하였다.

쿠키 재전송 공격에 대한 탐지와 관련한 검증 방법으로 탐지 프로세스를 준비와 탐지로 구분하고 제안 기법과 관련연구 기법에서의 프로세스를 순서대로 나열한 후 해당 여부를 두 기법에 표시하였으며, 결과는 <표 2>와 같다.

<표 2> 탐지 프로세스 비교

탐지 프로세스		제안 기법	관련 기법
준비	로그인 시 세션/사용자 토큰 발행	X	○
	인덱스 번호/임시 값 발행	○	○
	세션/사용자 토큰 해시 암호화	X	○
	인덱스 번호 양방향 암호화	X	○
	쿠키 해시 암호화	○	X
	탐지 파라미터 저장	DB 테이블	배열 리스트
	콜백 페이지 생성	X	○
	웹페이지 이동	○	○
	웹페이지 이동 시 인덱스 번호 전송	X	○
	로그인 페이지 인덱스 번호 복호화	X	○
	로그인 페이지 사용자 토큰 조회	X	○
	로그인 페이지 사용자 토큰 비교	X	○
탐지	공격자 쿠키 변조 및 공격	○	○
	공격 기법	주소창에 변조 쿠키를 URL에 입력	웹페이지 새로 고침
	세션정보 유무 검사	X	○
	콜백 페이지 이동	X	○
	세션에 콜백 페이지 url 저장	X	○
	로그인 페이지 이동	X	○
	탐지 기법	세션 URL = 콜백 URL	현재 쿠키 ≠ DB 쿠키
	공격 여부 판단	○	○
	이용자 정상 로그인 시 쿠키 조회	DB 테이블	배열 리스트

4.2 검증 결과

쿠키 재전송 공격에 대한 탐지 프로세스를 비교한 결과 준비 과정에서 이용자의 정상 로그인 시 쿠키 정보를 저장하는 프로세스와 인위적인 인덱스 번호나 임시 값을 사용하는 점은 제안기법과 관련 연구 기법이 사용하는 데이터 구조만 다를 뿐 모두 발생하였다. 반면에 인위적인 세

션 토큰, 사용자 토큰 및 콜백 페이지를 만들어 웹페이지 이동마다 공격 여부를 탐지하기 위해 네트워크를 사용하여 해당 파라미터들을 통신하며 비교하는 프로세스는 관련 연구에서만 있었다.

또한 웹페이지의 주소창에 URL을 입력하거나 쿠키 에디터를 이용 후 웹페이지의 새로 고침 이벤트 발생 시 공격자의 공격인지를 구별하기 위해 쿠키나 임의의 다른 값을 비교하는 프로세스는 같았다.

공격 탐지를 위한 준비 과정에서 검증결과 중 관련 연구 기법을 수식으로 표현하면 다음과 같다.

$$T[p] = T[ti]\times 3 + T[te]\times 3 + T[cs] + T[cp] + \sum_{i=1}^{i=10} (T[pm]\times T[im]) + T[id] + T[tr] + T[tc]$$

.....수식 1

제안 기법을 수식으로 표현하면 다음과 같다.

$$T[p] = T[ti] + T[ce] + T[cs] + \sum_{i=1}^{i=10} T[pm]$$

.....수식 2

공격 탐지 과정에서 검증결과 중 관련 연구 기법을 수식으로 표현하면 다음과 같다.

$$T[d] = \sum_{i=1}^{i=3} (T[cf] + T[ra] + T[sc] + T[pm]\times 2 + T[us] + T[ad])$$

.....수식 3

제안 기법을 수식으로 표현하면 다음과 같다.

$$T[d] = \sum_{i=1}^{i=3} (T[cf] + T[ra] + T[ce] + T[cr] + T[ad])$$

.....수식 4

수식에서 사용된 기호에 대한 설명은 <표 3>과 같다.

<표 3> 수식에서 사용된 기호

기호	설명
T(ti)	토큰/인덱스 발행시간
T(te)	토큰/인덱스 암호화 시간
T(cs)	토큰/쿠키 저장시간
T(cp)	콜백 페이지 생성시간
T(pm)	정상 이용자의 웹페이지 이동시간
T(im)	웹페이지 이동시 인덱스 번호 전송시간
T(id)	토큰/인덱스 복호화 시간
T(tr)	사용자 토큰 조회시간
T(tc)	사용자 토큰 비교시간
T(ce)	로그인/웹페이지 쿠키 암호화 시간
T(cf)	공격자의 쿠키 변조시간
T(ra)	쿠키 재전송 공격시간
T(sc)	사용자 토큰 값 비교시간
T(us)	세션에 콜백 페이지 url 저장
T(ad)	공격 판단시간
T(cr)	DB 테이블 쿠키 조회시간

공격 탐지를 위한 준비 과정과 탐지 과정에서 수식 1부터 4까지의 관련 연구 기법과 제안기법을 비교해보면 수식의 항목 수나 발생 횟수로 보아 관련 연구 기법에 비해 제안기법이 시간이 작음을 알 수 있다.

5. 결론

쿠키 재전송 공격에 대한 탐지 프로세스는 관련 연구 기법에 비해 제안 기법이 인위적으로 세션, 사용자 토큰 및 콜백 웹페이지를 만들지 않는 등 상당히 간단하다. 또한 공격 탐지 준비 과정과 탐지 과정에서 수식 1부터 수식 4까지의 비교에서 탐지 시간도 제안기법이 더 빠른 것으로 판단된다.

인터넷과 관련 기술이 발전한 웹 환경에서 정보보호 위협인 공격을 탐지하는 시간은 매우 중요하다.

본 논문의 제안 기법이 쿠키 재전송 공격을 더 빨리 탐지하는데 활용될 수 있기를 바라며, 다른 쿠키 재전송 공격의 경우와 방어 기법도 고려한 탐지 기법을 계속 연구할 것이다.

참고문헌

[1] 위키 백과, Google 검색, “인터넷 쿠키, 세션, Cookie Replay Attack”, url : http://www.wikipedia.com, https://www.google.com/

[2] 네이버 지식백과, 블로그, “인터넷 쿠키, 세션, 재전송 공격, 순서번호”, url : https://terms.naver.com, https://blog.naver.com

[3] 서진원, 서희석, 곽진, “웹서비스 공격정보 분류 방법 연구”, 한국정보과학회 논문지, 한국시뮬레이션학회논문지, 19(3), 99-108., 2010.9.

[4] OWASP, “Category : OWASP Top Ten Project”, 2017, https://www.owasp.org

[5] 김현진, 이임영, “재전송 공격에 안전하고 개선된 Single Sign-On 인증 시스템에 관한 연구”, 정보보호학회 논문지, 769-780(12 pages), 2014. 10

[6] 황희태, "안전한 서버 접속을 위한 이용자 인증 기법", 단국대학교 대학원 석사학위 논문, 2008.

[7] 이규안, “개인정보보호 강화를 위한 인증방법의 개선 방안 연구”, 한국전자통신학회 학술대회지, 제6권 제2호, pp.460-463, 2012. 11

[8] 원종선, 박지수, 손진곤, “웹 어플리케이션에서 세션 상태 기반의 쿠키 재전송 공격 방어 기법”, 정보처리학회 논문지, 컴퓨터 및 통신 시스템, 제4권 제1호, pp.31-36, 2015.

[9] 원종선, “웹 어플리케이션에서 쿠키 재전송 공격에 대한 방어 알고리즘”, 한국방송통신대학교 대학원 석사학위 논문, 2015.