쿠 키

연제영
건국대학교 컴퓨터시스템학과

Cookies

Yeon, Jea Young
Konkun University Computer System
E-mail : theexe48@nate.com

요 약

As computer technology grows, the risk of personal information leak on the internet is also increasing. A so-called "cookie" is used as one of the ways personal information leaks. A cookie offers convenience on the internet but serves as a major reason for personal information leakage at the same time. In this paper, we discuss risks and potential managements of a cookie.

1. 서론

현 시대에서 컴퓨터는 눈부신 발전을 거듭해왔으며 앞으로도 발전을 지속해 나갈 것이다. 컴퓨터 기술이 발전될수록 인터넷상에서의 개인 정보의 유출 또한 크게 증가하고 있다. 개인정보란 이름, 주민등록번호, 주소, 전화번호, ID, 비밀번호, 성별, 생일, 이메일과 같은 일반적인 인적사항에서부터 의료, 교육, 고용, 재산, 사회참여, 문화생활 등에 이르기 까지 다양한 형태를 이룬다. 이러한 개인정보 유출의 여러 방법 중 하나로서 쿠키라는 것이 사용되고 있다. 쿠키는 인터넷 사용에 편리함을 제공하는 동시에 개인정보유출의 주요 도구로서 사용되고 있는 것이다. 본 논문에서는 이러한 쿠키의 위험성과 대처방안에 대해서 살펴보도록 한다.

쿠키란 인터넷 사용자가 웹서버에 방문할 때 웹 브라우저를 통해 서버로 전송되는 텍스트 파일형태의 개인정보를 말한다. 쿠키는 컴퓨터 이용자가 웹서버에 접속했을 때 사용자의 컴퓨터로 4KB 이하의 작은 파일이 보내지는데 파일 용량이 먹다 떨어뜨린 “과자 부스러기”와 같다하여 유래된 명칭이다.[1] 이러한 쿠키는 이용자의 하드디스크에 저장되어 있다가 이용자가 해당 사이트에 접속을 할 때마다 다시 서버로 보내어진다. 또한 동일한 웹사이트 내에서 이동시에도 다시 전송될 수 있다.
쿠키의 본래 사용 목적은 웹서버가 이용자의 신원을 확인하기 위한 방법이었으나, 기업들은 이를 이용하여 개인별 방문기록, 상품구매, 취미생활 등을 기록하고 이를 통해 맞춤형 서비스를 제공하고 있다.

2. 기능 및 특징

2.1 쿠키의 기능

2.1.1 장점

쿠키는 이용자의 입장에서는 편리함과 서비스 제공자의 입장에서는 효율적인 마케팅 및 서비스 질의 향상을 가져왔다.

쿠키를 사용할 경우 사용자는 자신이 이용하는 회원제로 운영되는 웹사이트에서 다른 서비스 혹

은 다른 웹페이지를 방문할 때마다 ID와 password를 매번 입력할 필요가 없다. 서비스 제공자 입장에서는 소비자가 원하는 마케팅과 서비스를 제공할 수 있다. 쿠키에 저장된 정보와 웹서버에 저장된 데이터베이스(Database)를 이용하여 이용자가 주로 검색하는 상품, 가격 등을 분석하여 그에 맞는 개별화된 서비스를 제공할 수 있다.

2.1.2 단점

쿠키의 사용에는 여러 단점이 있다. 이용자의 계정(ID), 패스워드, 방문한 사이트 등의 정보 유출이 될 수 있으며, 또한 사상·신념등과 같은 민감한 정보들이 유출될 수 있다.[4] 컴퓨터에 저장되어진 쿠키 정보는 쉽게 복사/재사용 가능하기 때문에 집에서 사용하는 개인용 컴퓨터보다 한 대의 컴퓨터에서 여러 사람이 함께 사용하는 컴퓨터(PC방, 공공장소의 PC)일수록 더욱더 위험성이 커진다.

인터넷 전자상거래에서는 대부분의 거래 사이트에서 쿠키를 반드시 사용하게 하도록 한다. 상품이나 서비스를 구입하고자 할 때에는 상세한 개인정보가 취득된다. 이 정보는 자동적으로 데이터베이스화 된다. 기업에서는 쿠키에 저장된 정보와 웹서버에 저장된 데이터베이스(Database)를 이용하여 이용자의 의사와는 상관없이 개인정보를 취득하여 프라이버시를 침해 할 수 있다.

제3자에 의하여 쿠키로 수집된 정보를 도용당하는 경우에도 심각한 개인정보 침해를 초래 할 수 있다.[3] 정보화 사회가 발전해 가면서 이러한 프라이버시 침해 문제들이 계속 발생하고 그 사건수는 급증해 가고 있다.

2.2 쿠키의 특징

2.2.1 쿠키는 프로그램이 아니다.

쿠키의 형식은 그림 1의 텍스트(text) 파일의 형태이다. 쿠키는 하드 디스크에 저장이 되며, 윈도우 시스템 및 응용프로그램에는 영향을 주지 않는다. 윈도우 XP의 경우 기본적으로 쿠키는 \Documents and settings\사용자\Cookies에 저장된다.

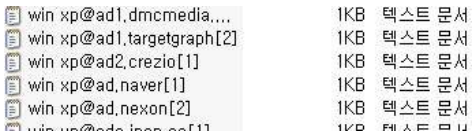

그림 1 쿠키 파일

2.2.2 쿠키에 저장되어진 정보는 사용할 수 없다.

쿠키를 이용하여 개인정보를 수집하고 이용하는 경우에는 개인정보주체의 동의를 얻어야 한다. 이에 위반하여 개인정보를 수집한 경우에는 500만원 이하의 과태료에 처한다(정보통신망법 제67조 제1항 제3조).[2] 다음은 쿠키도용 관련 기사이다.

> 제 목 : 미 쿠키 금지법 첫 발의
> 뉴스제공시각 : 2000/02/15 10:15 <전자신문>
> 웹사이트 운영자가 쿠키를 이용해 개인의 정보를 무단으로 획득하는 것을 금지하는 법안이 미국에서 처음으로 발의됐다고 미 유력 일간지
> 「USA투데이(http://www.usatoday.com)」가 보도했다.
> 이번 법을 제안한 미 상원의원 로버트 토리첼리는 『소비자들이 깜짝 놀랄 정도로 인터넷에서 개인의 정보 유출이 심각하다』며 『쿠키를 이용한 인터넷 광고업체들의 프라이버시 침해를 더 이상 방치해서는 안 된다』고 말했다.
> 한편 지난주에는 세계 최대 온라인광고대행업체 더블클릭이 쿠키기술을 사용해 개인 정보를 무단 사용했다는 이유로 프라이버시 보호기관인 EPIC(Electronic Privacy Information Center)로부터 제소 당했다.
> --- 중간생략 --
> <방은주기자 ejbang@etnews.co.kr>

2.2.3 쿠키의 용량

쿠키의 파일 크기는 4KB 이하이며, 쿠키폴더에는 약 300개의 파일이 저장된다.[5] 하나의 도메인은 쿠키의 수를 20개로 제한하고 있으며, 만약 제한된 수를 넘어 버리면 가장 적게 사용된 쿠키를 삭제하고 새로운 쿠키를 만들어 사용한다.

3. 위험성

3.1 개인 정보 침해의 위험성

쿠키에 저장된 정보는 유출될 수 있다. 쿠키의 정보가 네트워크상에 평문상태로 전송되기 때문에 보안에 취약하다. 이러한 쿠키는 사용자에 의해 쉽게 수정될 수 있고 다른 컴퓨터로 복사될 수 있다.

보안이 취약한 사이트 일 경우 쿠키정보에 개인정보가 일괄적으로 기록되는 사례가 있다. 개인의 정보보호보다는 개발자의 편의성 때문에 이렇게 처리되는 경우가 종종 있다. 다음은 쿠키의 위험성과 관련된 기사이다.

> 일부 사이트 쿠키 보안 '비상'
> [매일경제 2004-02-24 14:27] <전자신문>
> 온라인 포털 등 일부 사이트들이 '쿠키' 관리를 허술하게 해 개인정보 누출의 우려가 있는 것으로 나타났다.
> 관련업계에 따르면 일부 온라인사이트들이 서버와 PC사이의 로그인과 접속유지를 위해 자동 교환해 주는 쿠키(cookie)에 주민번호 주소 등 개인 정보를 담으면서 이를 암호화 하지 않고 일반 텍스트로 담는 방식 을 사용하면서 개인정보 누출의 우려가 제기되고 있다.
> (중간생략)
> 넷시큐어 방세중 팀장은 "쿠키 관리는 2000년대 초반에 한

차례 문제가 되면서 대부분 암호화 과정을 거치도록 하고 있지만 일부 사이트들은 아직 신경을 안 쓰는 곳도 있다"면서 "개인사용자들도 자신의 노트북이 나 PC 쿠키관리에 신경을 써야한다"고 말했다.
개인 PC에도 쿠키정보가 남아있을 경우 타인이 이를 대신 사용할 경우 개인 정보가 누출될 위험이 크다는 지적이다.
<신익수 기자>

3.2 쿠키 스니핑(Cookies Sniffing)

쿠키 스니핑은 사용자의 웹 브라우저에 있는 쿠키를 훔치거나 엿보는 해킹 기법이다.[4] 사용자가 게시판이나 쇼핑몰 등을 방문하면 웹 서버는 각종 필요한 정보를 사용자의 하드 디스크에 저장해 놓는데 여기에는 사용자가 로그인했을 때 입력한 ID나 패스워드 등 보안상 민감한 정보도 들어 있다. 이러한 정보가 저장된 파일이 쿠키이며, 쿠키 스니핑에 의하여 이것이 다른 사람의 손에 들어가게 되면 사용자는 개인 정보 유출 등의 심각한 피해를 입을 수도 있게 된다. 다음은 쿠키 스니핑 관련 기사이다.

[쿠키스니핑] 내 정보 유출,'쿠키'를 사수하라
한국일보|기사입력 2000-11-01
국내 20개 포털사이트가 해킹위험에 무방비로 노출돼 있어 개인정보가 유출될 가능성이 크다는 지적이 제기됐다. 1일 관련업계 및 한국정보보호센터에 따르면 H, N, O 등 국내 유명 포털사이트 20개가 `쿠키가로채기(스니핑)'라는 해킹 위험에 노출돼 있는 것으로 드러났다. 쿠키스니핑은 이용자가 인터넷 사이트에 접속했을 때 임시로 개인정보를 저장해 놓는 `쿠키'파일을 가로채는 해킹기법이다.
이 문제를 처음 제기한 보안컨설턴트 임대호(26)씨는 "20여개의 인터넷포털사이트와 웹메일사이트가 웹메일 본문에서 자바언어로 된 파일(자바스크립트)을 사용하거나 이용자 ID 및 비밀번호 입력 서버와 홈페이지 운영서버가 동일한 경우 해커가 가로챈 쿠키를 이용, 서버로 침투해 쉽게 이용자들의 정보를 빼내갈 수 있다"고 경고했다.
임씨는 이 같은 사실을 해당 포털사이트에 직접 실험을 통해 확인하고 경찰청 사이버테러대응센터와 한국정보보호센터에 통보했다고 밝혔다.
한국정보보호센터측도 가로챈 쿠키를 통해 웹사이트에서 이용자들의 정보를 훔칠 가능성이 있다고 보고 해당 사이트들에 대한 보안실태를 점검한 뒤 조만간 보안권고문을 발표할 계획이다.
임씨는 "사이트 운영 업체 측에서 쿠키스니핑을 막으려면 해커가 가로챈 쿠키로 침투하지 못하도록 인증서버와 홈페이지 운영서버를 다르게 지정할 것"을 권고했다. 임씨는 또 "네티즌도 웹메일 서비스를 이용할 경우 서비스 선택사항에서 `자바스크립트 허용여부'를 선택하지 말고 쿠키를 확인하는 사이트를 방문한 상태에서 다른 사이트를 동시에 검색하거나 접속하지 말라"고 당부했다.
<최연진기자>

3.3 P2P 네트워크로 쿠키값 유출

냅스터[1] 같은 프로그램으로 음악이나 파일 서비스를 받고 있는 사람들 중에 개인의 정보가 누출되는 사례가 있으며 개인 정보가 해킹된다는 것은 공공연한 사실이다.

P2P 프로그램을 통한 자료 다운로드 시 주의해야 한다. P2P 프로그램을 이용해 파일을 다운로드할 때는 악성 코드에 감염되어 있는지 보안 제품으로 검사한 후에 사용한다.

쿠키를 악용하여 개인의 특정사이트 암호와 비밀번호를 빼내가며, 개인 컴퓨터에서 복사해가는 사례도 있습니다. 다음은 P2P로 인한 쿠키값 유출 관련 기사이다.

'병주고 돈뜯은' 컴퓨터보안업체
[서울신문 : 2007-11-01 11 면]
(중간생략)
서울경찰청 사이버범죄수사대는 31일 안티바이러스 프로그램을 배포한 뒤 정상 파일을 악성코드라고 속여 돈을 가로챈 인터넷 보안업체 A사 운영자 이모(39·여)씨 등 4개 업체 관계자 8명을 특정경제범죄 가중처벌법상 사기 등 혐의로 불구속 입건했다.
A사 운영자 이씨는 2005년 3월부터 2년 동안 자사의 개인간 파일공유프로그램(P2P)과 포털사이트를 통해 396만 명에게 안티 바이러스 프로그램을 배포한 뒤 정상 파일과 쿠키(특정 사이트에 접속 시 방문기록을 컴퓨터에 저장해 재접속 때 빠른 접속을 돕기 위한 임시파일) 등을 악성코드로 진단한 뒤 126만여 명에게서 치료비 명목으로 월 3850원을 결제하도록 해 92억여 원의 부당이득을 챙긴 혐의를 받고 있다.
(중간생략)
임일영기자 argus@seoul.co.kr

3.4 IECookiesview 이용한 쿠키 공격 과정

3.4.1 IECookiesview의 특징

IECookiesView는 별도의 설치가 필요 없이 간단히 사용이 가능한 유틸리티이며, 인터넷 익스플로러에서 사용되는 쿠키의 자세한 내용을 보여준다.

쿠키의 목록과 키와 값, 적용되는 웹사이트의 도메인, 보안 여부 및 최근 사용한 날짜와 수정된 날짜, 생성된 날짜, 사용한 횟수 등을 확인할 수 있으며, 특정 키워드로 검색이 가능하여 누구나 손쉽게 사용할 수 있다. 프로그램의 주요 특징은 다음과 같다. 웹사이트 이름/생성 날짜 등의 다양한 쿠키 정보를 이용한 정렬, 웹사이트 명을 이용한 찾기, 필요 없는 쿠기의 제거, 텍스트 파일로 쿠키 저장, 클립보드로 쿠기 정보 복사, 자동으로 쿠키에 새로 고침 적용 등의 가능을 갖고 있다.

1) 냅스터(Napster) : 프로그램을 개발한 대학생 패닝(Shawn Fanning)의 별명이다. 개인이 가지고 있는 음악파일(MP3)들을 인터넷을 통해 안정적으로 공유할 수 있는 프로그램을 말한다.

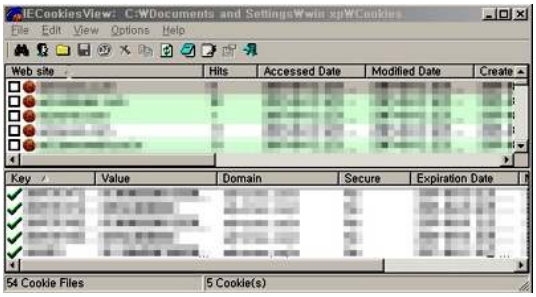

그림 2 프로그램 툴

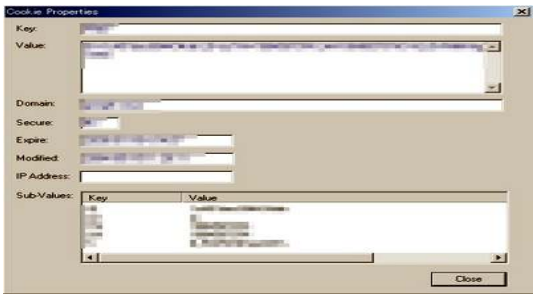

그림 3 쿠키 내용 조회

4. 대응책

4.1 쿠키 삭제(가장 손쉬운 대응책)

가장 손쉬운 대응책으로는 인터넷 익스플로러에서 인터넷 옵션을 통한 쿠키삭제이다.

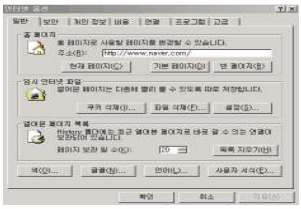

그림 4 인터넷 옵션

4.2 쿠키값 설정

그림 5

그림 6

그림7

그림5 : [인터넷 익스플로러를 실행] → [도구] → [인터넷 옵션] 선택 한다.

그림6 : [보안] → [사용자 정의 수준] 선택

그림7 : [쿠키]설정에서 [사용안함]을 선택한다. 모든 쿠키를 거부할시 등록을 요하는 서비스는 사용할 수 없다.

4.3 규칙적인 보안패치

윈도우, 리눅스 등 운영체제에서의 소프트웨어 자체의 취약점을 노리는 해킹 사례가 증가하고 있다. 주기적으로 운영체제에 보안패치를 해주는 것이 피해를 줄이는 방법이다.

4.4 CDT을 이용한 방어책

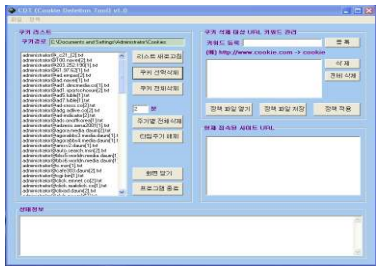

그림 8 CDT 프로그램

국가사이버안전센터에서 개발한 CDT(Cookie Deletion Tool)는 인터넷 사용 시 생성되는 쿠키파일의 자동, 수동으로 삭제하는 프로그램이다.

CDT는 웹사이트 방문 시 생성되는 쿠키를 모니터링 하여 이에 대한 삭제 수행하며, 쿠키의 전체 또는 선별 삭제를 할 수 있다. 또한 타이머 기능을 통하여 주기적 쿠키삭제 수행, 정책 설정을 통한 삭제 정책 편집 및 파일 저장을 할 수 있으며, 현재 접속한 웹사이트 목록도 볼 수 있다.[6]

즉, CDT의 주된 목적은 특정 웹사이트에 접속할 경우 해당 웹사이트 관리자가 방문자의 PC에 악성 쿠키를 생성, 개인 정보를 불법 수집하는 경우가 발생 할 수 있으므로 이를 사전에 차단하기 위함이다.

[참고문헌]

[1] 김연수,「개인정보보호」, 사이버출판사, 2001.

[2] 최경진, “쿠키의 활용과 프라이버시 보호”,「정보통신기술과 프라이버시 토론회 발제문」, http ://www.privacy.or .kr/pds/[2]cjk.hwp

[3] 최정열, "인터넷과 개인정보의 보호",「정보법학」제6권, 제1호 (2002) pp.101-159.

[4] 정준현, "개인정보 프로파일 보호를 위한 제도연구“, 개인정보침해연구 02-02, 한국정보보호진흥원

[5] David Whalen, *“Unofficial Cookie FAQ”*, http://www.cookiecentral.com

[6] 국가사이버안전센터, “CDT v1.0 사용매뉴얼.pdf & CDT_v1.0_Setup.exe”,「국정원에서 배포하는 보안 프로그램」, 2006.4

[7]국가사이버안전센터[쿠키 삭제프로그램(CDT)배포] http://www.ncsc.go.kr/
[8]관련뉴스
http://networker.jinbo.net/privacy/doc/arti2.txt
http://www.zdnet.co.kr/news/
http://news.naver.com/
http://www.hankooki.com/
http://www.seoul.co.kr/