제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

HTML5의 안전하지 않는 모바일 웹 어플리케이션에 대한 고찰

정훈영*, 서희석*
*한국기술교육대학교 컴퓨터공학부
e-mail:gost12@kut.ac.kr

A Study on Unsafe Mobile Web Application of HTML5

Hoon-Young Jung*, Hee-Suk Seo*
*Dept of Computer Science & Engineering, Korea University of Technology and Education

요 약

현재 인터넷의 최대의 관심사는 HTML5의 등장으로 인한 Web Page의 변화이다. 다양한 분야에서 영향을 미칠 것으로 최근 들어 급격히 무선 네트워크 사용률이 증가한 스마트폰에서도 Web Application이 등장하고 있다. 하지만 Web Application은 Native Application보다 소스 보안에 대해 매우 취약하며 본 연구에서는 이에 대한 분석과 보안을 위해 요구되는 HTML5 기능에 대해 언급한다.

1. 서 론

HTML이란 Hyper Text Markup Language의 약어로 Web 문서를 제작하기 위해 사용되는 Web Programming Language의 한 종류이다. 모든 Web 문서는 HTML을 기본적으로 사용하여 구현된 것이다. 현재 사용 중인 HTML은 HTML4로서 W3C에서 만들고 있는 차세대 Web 표준안인 HTML5는 HTML4 환경에서는 구현이 불가능했었던 다양한 기능이 추가된다. ActiveX를 비롯한 Flash, Camera, GPS 등 인터넷 환경에서는 사용하기 위해선 특별한 프로그램을 설치해야만 하거나 또는 구현이 불가능했다. 이러한 기능을 웹 문서로 제작할 수 있는 HTML5는 차세대 웹 서비스 개발의 주요 기술로서 각광받고 있다. HTML5는 W3C를 제외한 운영체제로 유명한 M사, 웹 브라우저 개발회사인 M사, O사, 각종 다양한 분야에서 활약 중이며 특히 근래 스마트폰으로 유명해진 A사나 G사 및 관련 웹 브라우저 업계가 참여한다.

이처럼 차세대 웹 표준안이자 관련 웹 브라우저 업계가 참여하여 개발을 진행한 HTML5는 최근 스마트폰을 이용한 무선 인터넷 사용률이 급증하면서 적지 않는 영향을 미치기 시작했다. 기존 Native Application에서 Web Application 으로의 변화가 조금씩 시작되고 있는 것이 그 이유다. 기존 방식의 Native Application의 경우 배포나 패치 등으로 인해 변경되었을 경우 각각의 단말기가 전부 재설치나 패치 파일을 이용하여 버전을 업그레이드해야만 했다. 하지만 Web Application의 경우 Server만 업그레이드하면 단말기에는 업그레이드작업 없이 즉시 최신버전으로 사용가능하다. 이는 문제점이나 버그, 개선사항을 위한 업그레이드 시에도 Server에서 업그레이드하는 것만으로도 해당 Web Application에 접속하는 모든 단말기가 업그레이드된 효과를 얻을 수 있다는 뜻이다. 이러한 이점은 기존 Native Application에 큰 영향을 미쳤다. 회사에서는 이러한 이점을 적용한 HTML5에 기반을 둔 Web Application을 찾기 시작하고, 각종 Application 개발회사들은 HTML5에 기반을 둔 Web Application에 대한 준비하고 있다.

하지만 HTML5에 몇 가지 강력한 기능들이 추가됨에 따라 웹 프로그래밍의 패러다임이 변화할 것이라는 호들갑에도 불구하고 실제로는 Web상에서 Native Application의 퍼포먼스를 아직까지 따라가지 못하고 있다. HTML5의 강력한 성능에도 불구하고 그것이 모든 문제를 해결할 수는 없다. HTML5에 추가된 매력적인 기능들로 인해 Web Application이 Native Application의 강력한 경쟁자로 부상하고 있으나, 보안문제, Local Data Storage의 한계, 동기화 문제 등으로 아직까지는 기대에 미치지 못한 부분도 적지 않다.

2. HTML5 기반의 Web Application

Web Application은 작년부터 대중에게 멀리 알려져 현재는 많은 사람들이 사용하고 있다. 국내 검색엔진으로 유명한 N사나 D사 등 Web Application을 스마트폰용으로 개발하여 배포중이다. Web Application이란 중요 부분의 소스를 Web Server에서 실시간으로 전송받아 실행하는 Application으로서 현대 사회에서 많은 이들이 사용하는

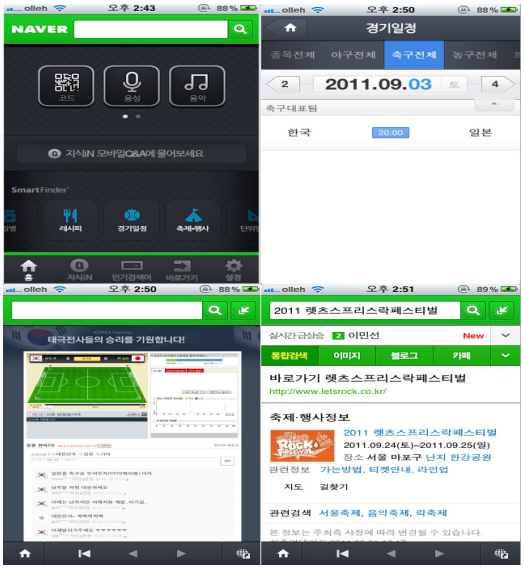
스마트폰의 무선 인터넷 사용률 급증에 따라 이를 착안하여 각종 통신사, Application 개발사에서 현재 개발이 한창 진행 중이다.

아래 [그림 1]은 HTML5기반의 Web Application 중 하나이다. 보는 거와 같이 개인정보를 입력하고 HTML5의 새로운 기능인 카메라를 이용하여 즉석에서 사진도 촬영하여 첨부가 가능하다. Save를 누를 경우 Web Server로 즉시 전송한다.

[그림 1] HTML5 기반의 Mobile Web Application

스마트폰 무선 인터넷 사용률 증가와 더불어 같이 상승하는 분야가 있다. 몇 년 전에도 온라인 게임은 PC의 전유물이나 다름없었으나, 최근 스마트폰을 이용한 온라인 게임이나 소셜 네트워크 게임이 상당히 출시되고 있다. 이미 상당한 인기와 중독성으로 상승세를 펼치고 있는 중이다. 이러한 방식의 게임들이 Native Application보다 업그레이드, 관리 등 편리한 Web Application으로 출시될 확률이 높다. 갑자기 게임 얘기가 나온 이유는 개인정보와 관련이 깊기 때문이다. PC에서 온라인 게임을 하기 위해서는 해당 관련 게임에 회원가입이 필수다. 물론 카페나 이메일, 기타 서비스를 이용하기 위해서도 회원가입은 필수다. 마찬가지로 스마트폰 또한 서비스를 이용하기 위해서는 굳이 PC를 거치지 않고서도 Web Application에서 회원가입을 진행할 수 있다. 하지만 스마트폰을 이용하여 Web Application에서 회원가입 시 사용되는 중요 소스가 악의적인 의도를 가진 사용자에게 공개되거나 서비스 이용 중에 관련 중요 소스가 유출되어 이를 이용하여 보안상 취약점을 발견 및 부당한 이득을 취할 경우 심각한 문제가 될 수 있다. 물론 소스가 공개된다고 무조건 문제가 발생하는 것은 아니다.

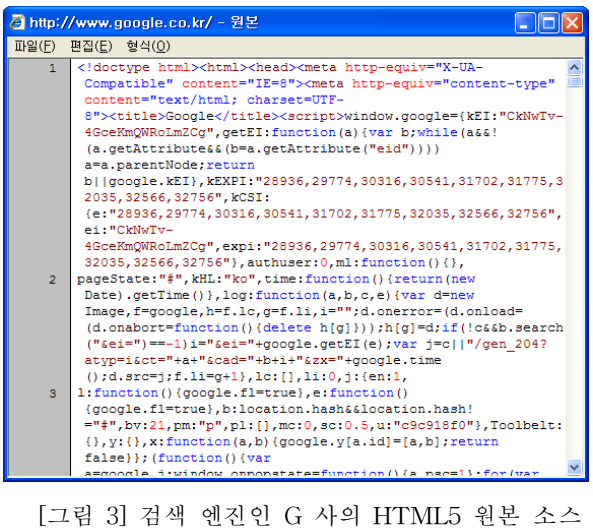
또한 Web Application이 위와 같은 단점만 존재하지는 않는다. 아래 [그림 2]처럼 일상생활에서 매우 유용한 정보를 제공해 준다. Web Application을 통해 자신의 주변 위치 정보나 내비게이션, 스포츠 중계, 일정, 이메일 등 다양한 분야에서 활용이 가능하다. 물론 스마트폰에 설치된 브라우저를 통해 위의 기능들을 사용할 수 있으나 이처럼 Web Application을 이용할 경우 스마트폰에 최적화되어 사용자가 편히 쓸 수 있게 제공해준다.



[그림 2] 국내 유명사이트의 Web Application

3. Web Application의 드러난 소스

인터넷에서 웹서핑을 할 때 클라이언트 측면에서의 근본적인 문제는 사용자가 서버에서 동작하는 Web Page의 소스를 확인할 수 있다는 점이다. Web Application의 경우 브라우저를 뛰어난 툴로 디버깅하면 소스를 확인하거나 남용하기에 어려움이 없다.



[그림 3] 검색 엔진인 G 사의 HTML5 원본 소스

Firebug와 같은 Javascript Debugger를 사용하면 소셜 네트워크 서비스 중 하나인 F 웹페이지나 유명한 검색 사이트인 G 웹페이지 같은 사이트가 어떻게 동작하는지, 호기심이 많거나 관련 업종으로 종사하는 사람은 누구든지

Breakpoint들을 삽입해 놓고 소스를 볼 수 있다.([그림 3] 참고) 이로 인해 웹사이트의 디버깅과 동작방식을 쉽게 이해할 수 있게 되지만 "보안"의 관점에서는 바라볼 경우 이러한 문제는 매우 치명적이다.(참고로 첫 번째 줄의 <!doctype html>은 HTML5 임을 뜻하는 태그이다.)

또한 Firebug를 비롯하여 브라우저 디버깅 툴을 사용하면 특정 변수의 값을 원하는 대로 조작할 수 있다. 즉, 브라우저가 지구상에 위치해 있는 위도와 경도값 등 위치 변수를 쉽게 편집해서 주위의 지인들에게 위치를 속일 수 있다. Web Application이 제공하는 모든 기능들 역시 수정될 수 있다. Web 환경은 일반적인 Native Application에서 보다 쉽게 조작이 가능하다. Native Application의 경우 컴파일 되어 배포되기 때문에 전문가가 아닌 이상 소스를 해독하는데 어려움이 많기 때문이다.

물론 공개된 소스로 인한 보안문제가 발생하는 데에는 한계가 있으며, G사의 Web Toolkit과 같은 JavaScript Tool은 표준 컴파일러만큼이나 복잡한 툴들의 출력 결과는 측량하기가 어렵다.

보안상의 위험은 어플리케이션의 특징에 달려있다. 위도와 경도값을 편집해서 지인들에게 내 위치를 지구의 반대편에서 체크인한 것처럼 보이게 만들 수 있다. 만약 누군가 위치 조작에 의해 특정 장소의 Mayor로서의 권한을 취득하고 이것이 돈과 관련이 된다면 더욱 악용될 확률이 높아지고 수법은 훨씬 더 복잡해진다. 이러한 이유로 중요한 데이터를 수집을 위해 HTML5를 활용한 Web Application들은 아직까지는 보안에 문제점이 적지 않다.

```
var w    = 680;
var h    = 260;

w+=document.body.scrollLeft
h+=document.body.scrollTop

var leftpos=w
var toppos=h
document.getElementById("loadingBar").style.left=w
document.getElementById("loadingBar").style.top=h

function staticize(){
        w2=document.body.scrollLeft+leftpos
        h2=document.body.scrollTop+toppos
        document.getElementById
("loadingBar").style.left=w2
        document.getElementById
("loadingBar").style.top=h2
}
//언어변경
function langChange(vl){
        document.languageForm.target = "_self";
```

[그림 4] 모든 소스를 보여주는 HTML

4. 결 론

작년까지는 Cloud Service나 비슷한 서비스에도 대중은 크게 반응하지 않았다. 대부분은 사람들은 USB나 외장하드 등 휴대용 메모리를 애용했기 때문이다. 하지만 올해 들어 개인 Web Hard, Cloud Service를 이용한 동기화 등 각각의 컴퓨터에 설치하는 것보다 웹을 이용한 편리함에 많은 이들이 Web 관련 서비스를 이용하고 있다. 또한 HTML5의 등장이 다가옴에 따라 Web에 대한 관심은 앞으로도 계속 고조될 것이다. 이러한 Web 동향을 살펴볼 경우 경제적인 면에서나 시간적인 면에서 기존 사용하던 방식의 Native Application보다 단점보다 장점이 더욱 많은 Web Application이 각광받을 것이다. 하지만 설치가 필요하지 않는 Web Application은 사용자가 특정 툴을 사용할 경우 Web Browser에게 전송되던 소스를 특정 툴로 전송하여 Web Application의 소스가 출력된다. 물론 PHP, JSP와 같이 서버에서 컴파일 작업을 거쳐 오는 소스의 경우 큰 문제점이 없지만 HTML의 경우 원본 소스가 그대로 전송되어 보안에 치명적인 문제점을 야기한다. 이러한 이유로 PHP나 JSP와 같이 컴파일 작업을 거친 후의 결과만 출력해주는 새로운 기능이 있다면 이러한 문제는 상당 부분에서 해결될 것이다.

해킹대회의 문제 중 하나인 웹 해킹은 자주 출제가 되고 있다. 소스가 드러난 HTML 소스를 확인하여 해킹하는 것과 PHP, JSP 등의 웹 페이지의 전체 소스가 확인이 불가능한 웹페이지 해킹 두 가지 방식이 대부분이다. 이 두 방식 중 해킹성공률은 후자 쪽이 현저히 적다. 이러한 결과는 소스가 숨겨졌을 때 보안성이 높아진 것을 의미한다. 이를 보아 새로이 표준화 작업이 진행 중인 HTML5가 [그림 4]와 같이 웹페이지의 소스 전체가 드러나게 될 경우 보안상 문제가 있을 수밖에 없다. 하지만 HTML5가 PHP, JSP와 같이 컴파일 연산을 통해 표시된 웹페이지 결과만 소스가 보이도록 한다면 HTML5는 PHP, JSP와 큰 차이가 없어 사람들로부터 버려질 기능이 될지도 모른다.

본 논문에서 제안하는 HTML5의 새로운 기능은 특별한 태그를 이용한 Hybrid Web Programming Language를 위한 기능이다. HTML은 인터프린터 방식의 성향을 지닌다. 이러한 방식을 이용한 장점으로는 PHP, JSP보다 높은 인식성과 빠른 속도를 자랑한다. 하지만 본 논문에서 제기한 것처럼 소스 보안에 대한 치명적인 문제가 있다. 하지만 모든 소스가 이러한 단점을 불러오지는 않는다. 요점은 Web Page의 중요한 부분만 보이지 않는다면 이 문제는 상당 부분 해결이 가능하다는 의미이다. 하지만 이를 위해서는 언급한 것처럼 새로운 기능이 필요하다.

만일 특정 태그를 입력하여 해당 태그 범위 안에 있는 소스만 컴파일이 된다면, Web Page의 소스가 공개된다하더라도 원본 소스는 알려지지 않는다. 이로 인해 발생될 이점은 보안성은 우수해지면서 속도측면에서도 큰 차이가 없다. Web Page의 핵심기능이 담긴 소스 등은 PHP, JSP와 같이 컴파일 처리가 되어 연산결과만 소스로 보여주고 알려져도 의미 없는 일반적인 소스는 전부 기존 HTML4 방식처럼 인터프린터 형식으로 처리되도록 한다.

[그림 5] 컴파일 기능이 추가된 예

위의 [그림 5]은 설명을 돕기 위해 <HTMLCOM> 이라는 가상의 태그를 이용하여 만들었다. <HTMLCOM> 태그는 해당 범위 안에 위치한 소스는 PHP, JSP와 같이 연산처리 이후 해당 결과만 소스로 출력되도록 하는 역할을 담당한다.

위와 같은 새로운 기능의 태그를 도입한 홈페이지를 개설할 경우 보안성은 매우 높아질 것이며, 국내의 IT 보안에서 없어선 안 될 새로운 기능으로 등장할 가능성도 엿보인다.

개인정보 유출, Web Page를 통한 Database Server 해킹 등의 사건들을 방지하기 위해서는 예방이 최선이다. 이러한 예방을 위해선 Web Page의 소스부터 안전하게 관리해야 될 필요성이 있다. 본 논문은 이러한 관점에서 바라보고, Web Page 소스의 중요성을 높이 삼아 이를 위한 새로운 보안기능이 추가된 태그를 제시하였다. PHP, JSP처럼 모든 소스를 컴파일 하는 방식이 아닌 만큼 본래 HTML의 속도와 PHP, JSP와 같은 우수한 보안성을 지닌 이러한 기능을 가진 방식으로 이와 같은 태그의 필요성은 충분하다.

참고문헌

[1] “2010년 인터넷이용실태조사”, 한국인터넷진흥원, 2010. 9.

[2] “스마트폰이용실태조사”, 한국인터넷진흥원, 2010년 제1차 인터넷이슈 기획조사, 2010. 7.

[3] “모바일 인터넷 및 스마트폰 보안 기술”, 김기영, 강동호, 개방형컴퓨터통신연구회, 제36권 1호

[4] “[김광현의 IT 집중분석] 스마트폰 ‘공짜 앱’ 통해 개인정보 줄줄 샌다.”, 한국경제, http://news.nate.com/view/20100802n05938

[5] “[스마트폰보안] ‘악성코드보다 위험한 모바일 앱’”, 유호선, http://www.ciobiz.co.kr

[6] “차세대 모바일 웹 애플리케이션 표준화 동향”, 전종홍, 이승윤, 전자통신동향 분석, 제25권, 2010(2).

[7] “안전한 웹 서비스를 위한 웹 어플리케이션 공격 유형 및 대응 방안 분석”, 이용호, 박명수, 윤준, 윤정원, 정보보호학회지, 제14권, 제4호, 2004. 8

[8] “하이브리드 모바일 애플리케이션 플랫폼, HyWAI”, 이승윤, 전종홍, 이원석, 한국정보과학회지, 제28권, 제6호, 2010. 06.

[9] “차세대 모바일 웹 애플리케이션 표준화 동향”, 전종홍, 이승윤, 전자통신동향분석, 제25권, 제1호, 2010. 02.

[10] “웹 애플리케이션 취약점 분석 시스템”, 이동건, 이민수, 조상현, 차성덕, 2008년 가을 학술발표논문집 Vol.35, No.2(D), 2008.

[11] W3C, Working Draft, HTML5, http://www.w3.org/TR/html5/