

웹스토리지와 보안

윤수지* 송신예* 이슬** 이현진* 백종호***

◆ 목 차 ◆

- | | |
|--------------------------|-----------------|
| 1. 서론 | 4. 웹스토리지 활용의 예 |
| 2. 웹스토리지 이전의 유사 기능, '쿠키' | 5. 웹스토리지는 안전한가? |
| 3. 웹스토리지 정의와 특징 | 6. 결론 |

1. 서론

2014년 10월 28일, W3C(World WideWeb Consortium)는 새로운 웹표준안으로 HTML5으로 확정했다고 발표했다. 이에 따라 인터넷에 접속해서 웹을 사용하는 모든 전세계 이용자들은 어쩌면 자신도 모르는 사이에 HTML5를 사용할 수 밖에 없게 되었다. 하지만, 기존에 사용하던 HTML4에서 HTML5로 바뀌면서 사용자가 인식할 만큼 혁신적인 변화가 있었다고는 볼 수 없다. 다만, 기능적으로 구역요소를 나누는 블록요소가 div로 대체되었다는 것, 플러그인이 없이도 멀티미디어를 재생할 수 있게 되었다는 점은 프론트엔드 개발자나 디자이너들이 구현하기 편하도록 변화되었다고 볼 수 있다.

그런데 주목할 만한 혁신적인 변화가 없는 가운데 사람들의 이목을 이끈 것으로 '웹스토리지'라는 추가적인 저장소가 생겼다는 점이다. 이러한 웹스토리지를 통해 웹 사용자들은 좀 더 자신에게 맞는 옷을 입듯이 자신의 웹 사용 행동 패턴에 따라 편하게 웹을 사용할 수 있게 되었다. 예를 들어, 자신이 자주 들어가는 웹사이트의 비밀번호가 미리 저장되어 있어서 '자주 기억을 못해내는 비밀번호를 입력하지 않아도 바로 사용할 수 있다는 것'과 '인터넷 쇼핑몰에서 쇼핑카트에 들어가지 않아도 쇼핑몰에서 둘러보았던 옷들을 다시 볼 수 있다 것' 등이 있다. 하지만 비전문가

로 볼 수 있는 일반 사용자는 웹스토리지의 발전에 대해 크게 느끼고 있지 못하고 있는 실정이다. 그저 '웹 사용이 점점 편해지네!' 정도로만 인지하고 있는 정도로 볼 수 있다. 설령 웹스토리지에 대해 조금이라도 알고 있다 할지라도 HTML5가 생겨남으로 발전된 웹스토리지의 장점만 알고 있을 뿐이다.

동전의 양면이 있듯 HTML4의 기능을 보완해서 나온 HTML5의 웹스토리지 일지라도 안전하지 못한 위험 요소들은 항상 내재하고 있다. 자세하게 웹을 모르는 비전문가들이 새롭게 등장한 웹스토리지에 대한 안전성, 웹스토리지를 통한 개인정보의 노출위험 등을 인지하지 못하는 것이 당연한 일일 수도 있지만, 새롭게 바뀐 웹표준안에 따라 안전하고 실용적인 웹을 사용해야 할 권리는 있다고 생각된다. 비전문가들은 한번도 HTML5와 웹스토리지에 관한 내용을 들어보지 못해 자신도 모르는 사이에 웹 상의 중요한 개인정보들을 안전하지 못한 저장소에 저장하기도 하고 때로는 나의 개인정보들이 어느곳에 저장되는지 잘 모르는 경우도 많다. 따라서, 비전문가들도 안전하고 효율적이게 웹을 사용하기 위해 새롭게 채택된 HTML5의 웹스토리지에 대해 정확한 이해를 돕고 이를 통해 어떻게 더 안전하고 효율적인 웹을 사용할 수 있도록 하기 위해 본 기고문을 작성하고자 한다.

2. 웹스토리지 이전의 유사 기능, '쿠키'

새롭게 채택된 HTML5에 웹스토리지가 왜 생겨났을까? 하는 질문을 해본다. HTML5의 웹스토리지가

* 서울여자대학교 멀티미디어학과
** 서울여자대학교 콘텐츠디자인학과
*** 서울여자대학교 멀티미디어학과 조교수

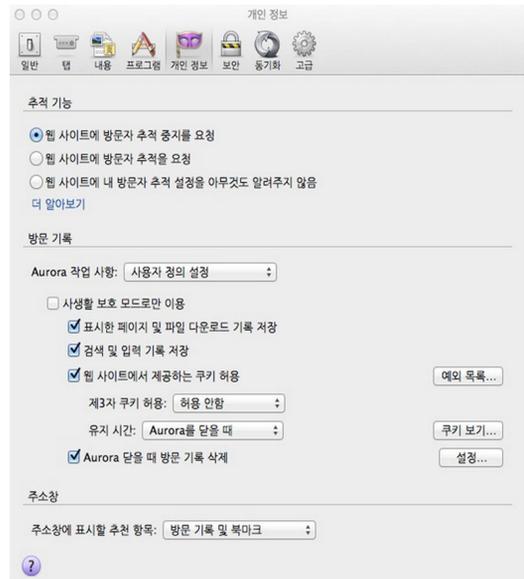
생겨나기 전에, HTML4에서 ‘쿠키’라는 것이 있었다. 쿠키는 1994년 넷스케이프에서 일하던 루 몬톨리가 쇼핑몰을 위한 서비스를 개발하는 과정에서, 넷스케이프 사이트에 방문한 사람이 처음 온 사람인지 확인을 위해 개발하게 되었다. 그 이후 쿠키는 사용자의 다양한 활동들을 알려주는 용도로 사용되었다. 사용자가 ‘팝업창을 다시 보지 않는다.’ 는 단추에 체크한 사실 같은 것을 쿠키가 기억해 편리하게 웹을 사용할 수 있도록 도와주었다. 쿠키는 그림1에서 보는 바와 같이 웹사이트(서버)와 내 컴퓨터가 텍스트 파일(.txt)의 형태의 쪽지이다. 쿠키를 주고받으며 대화를 한다.



(그림 1) 쿠키의 모습

사용자는 웹사이트 브라우저 별로 쿠키를 설정할 수 있다. 쿠키를 설정한다는 것은 사용자가 선택한 A라는 특정 사이트에서 행동한 모든 것들을 추적할 수 있는 파일(.txt)를 A사이트의 서버에 보낼 것인지에 대한 선택하는 개념으로 볼 수 있다. 그림2에서 보는 바와 가티 각 브라우저의 설정에 들어가 쿠키를 설정할 수 있는데, A라는 웹사이트에서 쿠키를 한번 설정하게 되면 그 이후부터 사용자 컴퓨터의 모든 웹 요청과 쿠키정보, 즉 해당 사이트에서의 사용자 행동의 모든 패턴정보가 A사이트의 서버로 전송된다. 이러한 쿠키는 사이트 당 20개, 용량은 4KB로 정해져 있고 쿠키의 데이터를 로컬 저장소에 연속적으로 저장하는 것이 아니라 만료 일자를 저장해야하기 때문에 보존 기간이 한정적이었다. 웹브라우저가 많은 발전을 이루기 전에는 사용자의 행동과 사이트의 서버와의 대화가 로컬 저장소에 저장될 수 있었다. 하지만 모바일 앱, 하이브리드앱 및 웹앱 등 모바일 환경에서 웹이 상호적으로 발전됨에 따라 HTML5가 정식 웹표준안으로 채택되기 직전부터 웹 브라우저의 성능이 빠르

게 증가하게 되었고 이에 따라 브라우저에서 구동할 수 있는 웹 어플리케이션 사이트들은 높은 수준의 성능을 보여주었다. 이런 이유로 4KB라는 제한적인 쿠키의 용량으로 많은 정보를 로컬에 어떻게 저장할 수 있겠는가라는 논의를 낳게 되었다. 초기의 로컬 저장소였던 쿠키는 제한적인 갯수와 용량은 급속하게 발전하는 웹에서 치명적인 단점으로 대두되었다. 예를 들어, 구글이 ‘구글 드라이브’와 같은 데이터 저장이 핵심인 기능을 포함하는 웹앱을 만들려고 시도했으나 용량의 한계가 있는 쿠키로는 구현이 불가능했다. 따라서, 구글을 비롯한 많은 웹 브라우저 제조사들이 새 로운 HTML 표준안 제정 시 웹을 위한 저장소를 만들 것을 제안하였으며, 이에 따라 HTML5 초기의 저장소 규격을 만들게 되었다.



(그림 2) 웹브라우저 설정에 포함된 쿠키를 차단하는 기능

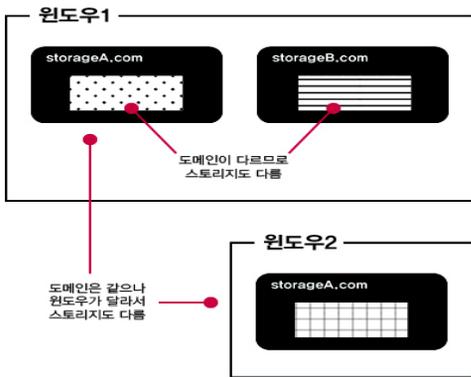
3. 웹스토리지 정의와 특징

구글과 그 외의 브라우저 제조사들이 웹이 발전됨에 따라 쿠키보다 더 큰 규격의 저장소가 필요하다는 의견을 같이해 새로운 웹표준안 추진시 새롭게 탄생된 것이 바로 ‘웹스토리지’이다.

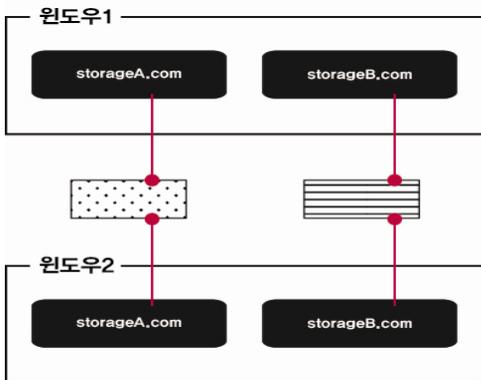
	Internet Explorer	Firefox	Safari	Chrome	Opera
Two versions back	6.0	3.0	3.2	3.0	10.1
Previous version	7.0	3.5	4.0	4.0	10.5
Current	8.0	3.6	5.0	5.0	10.6
Near Future (2010)	9.0	4.0	5.*	6.0	7.0
Future (2011 or later)	9.0	4.0	5.*	7.0	10.7

(그림 3) 브라우저 지원현황

웹스토리지란 인터넷 익스플로어, 크롬 등의 브라우저를 이용하여 데이터를 서버로 보내지 않고서도 클라이언트 측에 데이터를 영구적으로 저장할 수 있는 기술이다. 데이터에 ‘키’와 ‘값’이라는 두 속성을 부여하여 한 쌍으로 묶고, 키를 기반으로 저장된 데이터를 찾아내는 방식을 사용하고 있다. 이를 통해, 웹스토리지는 단순 문자열을 넘어 스크립트 객체 정보를 저장할 수 있게 되었다. 웹스토리지는 크게 생존기간과 접근가능 범위에 따라 로컬스토리지, 세션스토리지로 나눌 수 있으며, 그림4와 그림5에서 각각 보여진다.



(그림 4) 세션 스토리지



(그림 5) 로컬 스토리지

로컬 스토리지와 세션스토리지는 그림4와 그림5에서 보는 바와 같이 모두 도메인마다 따로 생성된다. 로컬 스토리지는 새로 생성된 윈도우에서도 같은 도메인이라면 같은 스토리지를 사용해 직접 지우지 않고서는 삭제되지 않는다. 저장한 데이터를 명시적으로 지우지 않는 이상 영구적으로 보관한다. 세션 스토리지는 데이터가 브라우저 종료시까지만 존재하고 새로 생성된 윈도우와 기존의 윈도우의 세션 스토리지는 서로 영향을 주지 않는다.

4. 웹스토리지 활용의 예

이러한 웹스토리지의 활용범위는 무궁무진한데, 인지하지 못하고 사용자들이 웹을 이용할 때 자주 경험할 수 있었다.

하나, 구글 - 대표적으로 지메일과 구글 드라이브

팀 프로젝트를 하거나 큰 저장소가 필요할 때 대부분 사용자들은 ‘구글 드라이브’를 사용한다. 앞서 언급한바와 같이, 구글은 누구보다 적극적으로 HTML5를 수용했고 HTML5의 다양한 기능들을 사이트에 접목시켰다. 지메일과 구글 드라이브는 온라인상에서 로드시켜왔던 메일 혹은 데이터들을 오프라인 상에서도 이용할 수 있도록 하였다. 이는 온라인상의 정보들을 클라이언트 측의 웹 스토리지에 저장을 함으로써 오프라인 상에서는 이를 꺼내오기만 하여 이전의 것을 열람하거나 이용하려면 굳이 사용자가 온라인 환경일 필요는 없게 되었다. 또한 대용량 데이터들을 웹 스토리지에 저장을 함으로써 로드되는 시간을 단축시키고자 했다.

또한, Chrome에서 로그인상태에서 로그아웃을 했음에도 불구하고 Chrome웹에서는 북마크, 방문기록, 설정 등과 같은 웹의 기본사항들이 그대로 보존이 되어있다. 이는 대부분의 로컬자원이 OS의 사용자별 어플리케이션 데이터 공간에 저장되기 때문인데, 예를 들어 윈도우 XP의 경우 어플리케이션 데이터가 저장되는 경로가 'C:\Documents and Settings\사용자계정\Local Settings\Application Data' 이 공간이며, 이 디렉터리 하위에 있는 각 브라우저 별 폴더에 로컬자원이

저장된다. 참고로, 윈도우에서 'C:\Documents and Settings\사용자계정'의 경로는 %userprofile%로 대체 된다.

(크롬 북마크 위치: C:\Users\사용자계정\AppData\Local\Google\Chrome\User Data\Default)

웹의 기본사항들이 로컬스토리지에 저장되는 만큼 오프라인 상태에서 앱을 사용했을 때도 (오프라인 상태에서 크롬 북마크 추가 등) 앱 이용이 가능하다. 이는 로컬에 저장되어 있던 데이터들을 온라인으로 연결될 때 가져와 싱크를 맞춰줌으로써 가능하다.

둘, 페이스북 이용

페이스북은 대용량의 미디어 파일들과 수많은 사용자들의 데이터를 보관하는 사이트이다. 그렇기 때문에 로컬 스토리지를 이용해 많은 데이터들을 저장해놓고 오프라인 상에서 이용이 가능해진다. 또한 페이스북 역시 구글처럼 대용량의 데이터들을 서버와의 통신 없이 로컬 스토리지에서 가져오기만 하면 된다. 따라서, 로드되는 시간을 단축할 수 있다.

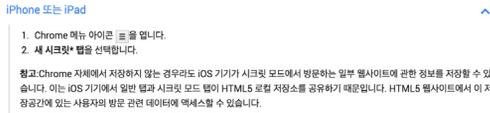


[그림 6] 오프라인시 웹스토리지를 이용하는 모습

5. 웹스토리지는 안전한가?

웹스토리지의 사용을 통해 사용자는 편리함을 느끼기도 하지만 이렇게 변한 웹을 사용할 때마다 자신의 행동 패턴이 다 저장되는 것 같아 불안감을 느끼기도 한다. 일부 사용자들은 검색 기록을 주기적으로 지우기도 하지만 그 기록이 컴퓨터의 어느 저장소에서 어떻게 지워지는지 알 수 없어 불편함을 느낀다. 도대체 이러한 개인적인 정보들은 어디에 저장되고 사용자가 어떻게 지울 수 있을까? 사용자들이 정보들을 지웠다고 하더라도 깨끗하게 지워진 것일까? 아니면 웹의 어느 곳에 남아있어 다시 불러올 수도 있는 것인가? 앞서 언급하바와 같이 웹스토리지가 생겨나기 이전에는 브라우저에서 구동할 수 있는 웹 어플리케이션 사이트들은 높은 수준의 성능을 가지고 있지만 한계를 들어낸 쿠키 저장소의 크기 때문에 많은 웹의 기능들을 구현하기 힘들었다. 이러한 두드러진 단점이 있어, 용량의 제한이 없는 웹스토리지가 생겨났고 이제 많은 웹 어플리케이션들이 사용자의 정보를 객체화해 로컬스토리지에 저장한다. 그렇다면, 개인정보가 스크립트 언어로 저장되고 있는 로컬스토리지가 안전한가?

일반적으로 로컬 스토리지에 데이터들을 저장할 때, 암호화 되어있지 않는 평문으로 적어야 한다. 평문으로 적힌 키값은 XSS (크로스 사이트 스크립팅 -Cross Site Scripting) 공격에 취약하다. XSS 공격은 로컬스토리지에서 데이터들을 꺼내 읽을 수 있다. 다시 말하자면, XSS는 자바스크립트 언어로 로컬스토리지에 접근해 스크립트로 언어로 저장된 데이터들을 읽어낼 수 있다. 그러므로 중요한 개인정보 사항들은 절대로 로컬스토리지에 저장해 놓지 말아야한다. 하지만 웹스토리지를 사용한 많은 웹 어플리케이션들은 편하게 저장하기 위해 사용자의 많은 정보들을 로컬 스토리지에 저장한 것을 흔히 발견할 수 있다. 예를 들어, 크롬을 사용할 때 사용자가 크롬 브라우저에서 로그아웃했다고 하더라도 로그인이 되어 있는 사이트 북마크 했다면 그 사이트에 접근할 수 있다.



(그림 7) 구글 시크릿 모드 설명1

이와 같은 접근 해결을 위해 크롬 설정에 들어가 보면 그림7에서 보는 바와 같은 안내문을 발견할 수 있으며, 아이폰과 아이패드를 사용하는 경우, 크롬에 방문한 페이지 및 다운로드 기록이 저장되는 것을 원하지 않는 경우 웹을 시크릿 모드로 탐색하는 방법에 대해 안내해주는 글이다. ‘iOS 기기에서 일반 탭과 시크릿 모드 탭이 HTML5 로컬 저장소를 공유하기 때문입니다’라고 직접 명시한다. 이 안내문을 다시 웹스토리지의 정의와 관련하여 쉽게 해석해 보면, ‘크롬 웹서버에 사용자의 정보들이 저장되는 것이 아니라, 서버에 직접 데이터들을 전송하지 않아도 정보를 클라이언트 쪽에 저장하는 웹스토리지’가 있다. 이 웹스토리지를 통해 정보들이 로컬 저장소에 저장되었고 애플기기(iphone, ipad)들은 이 로컬 저장소를 공유하고 있다. 그러므로 만약 사용자의 크롬 브라우저 사용 행태를 알고 싶다면 로컬 저장소를 방문해라’ 라고 해석 할 수 있다. 사용자가 자신의 크롬 브라우저 사용 행태를 하나하나 추적할 수 있는 정보를 삭제하고 싶다면, 크롬 브라우저의 로컬저장소를 찾아 삭제하면 된다. 하지만 대부분 사이트가 웹의 데이터를 로컬/세션 스토리지 중 어느 곳에 저장해놓았다고 명시해두지도 않았고 심지어 여전히 쿠키에 저장되는 경우도 있어 사용자는 주기적으로 웹의 설정 페이지에 들어가 자신의 데이터 기록들을 지워야만 한다. 만약 자신의 개인정보를 더욱 안전하게 관리하면서 효율적으로 웹 사용을 원하는 사용자라면 웹 데이터 저장소를 웹스토리지가 아닌 쿠키로 전환할 필요가 있다. 쿠키는 크기가 작지만 외부의 공격이 쿠키에 들어올 때, 데이터들을 보안플래그(secure/httponly)로 보호할 수 있기 때문이다. 보안플래그 중 secure는 민감한 세션 토크들을 항상 암호화된 상태에서 주고받을 수 있는 것을 의미하고 httponly는 어떤 스크립트 언어로든 쿠키에 접근을 못하게 하는 것이다. 따라서, XSS공격이나 외부 악성 코드로부터 안전성을 지킬 수 있다. 스크립트

언어를 통해 데이터가 저장되어 공격을 쉽게 받을 수 있는 웹스토리지 보다 훨씬 안전하다.

6. 결론

웹 기술의 급속한 발전에 따라 사용자의 다양한 이용 행태에 보다 최적화된 서비스를 제공하고자 기존 쿠키가 지내고 있는 저장소 용량의 단점을 해결하고 보다 다양한 사용자의 웹이용 행태의 저장이 가능한 웹스토리지가 새롭게 등장하여 최근에는 많은 웹 어플리케이션에서 이용되고 있다. 하지만, 여러 가지 장점에도 불구하고 사용자들은 개인정보 유출의 불안감과 걱정을 갖고 있어 웹스토리지를 이용하는 많은 웹사이트에서 이러한 문제점을 해소하기 위해 비전문가인 사용자들에 보다 알기 쉽게 이해할 수 있는 수준으로 웹스토리지를 설명하고 개인정보 유출을 방지하는 방법에 대해 적극적으로 알리기 시작했다. 예를 들어, 구글은 사용자를 인증하고, 로그인 자격 증명의 허위 사용을 방지하며, 무단 액세스로부터 사용자 데이터를 보호하기 위해 보안 쿠키를 사용한다. 또한 그림8에서 보는 바와 같이 시크릿 모드를 제공하여 시크릿 모드를 사용할 경우, 인터넷 사용 기록과 다운로드 기록이 저장되지 않고 이 창에서 생성된 쿠키들은 창을 닫음과 동시에 삭제가 되게 하였다.

시크릿 모드 및 게스트 모드 자세히 알아보기

참고: 현재 게스트 모드는 Chrome의 일부 버전에서만 지원됩니다.

시크릿 모드 및 게스트 모드 모두 임시 브라우저 모드이지만 기본적인 차이점이 있습니다.

- 시크릿 모드: 컴퓨터에 인터넷 사용기록과 쿠키를 남기지 않지만, 여전히 기존 방문 기록, 북마크, 비밀번호, 자동완성 데이터 및 기타 Chrome 설정 등을 볼 수 있습니다.

- 게스트 모드: 게스트 모드 상태에 있는 사용자는 컴퓨터에 인터넷 사용기록 또는 쿠키를 남기지 않습니다. 또한 컴퓨터 소유자의 Chrome 프로파일을 보거나 수정할 수 없습니다.

중요: 시크릿 모드와 게스트 모드 모두 웹에서 나옴을 숨길 수 없습니다. 방문하는 웹사이트, 직원, 또는 서비스 제공업체는 여전히 탐색 활동을 볼 수 있습니다.

시크릿 및 게스트 모드에 저장되는 사항에 대한 자세한 정보는 [Chrome 개인정보취급방침](#) 안을 병문하세요.

(그림 8) 구글 시크릿 모드 설명2

이를 통해 구글은 사용자 추적에 의한 보안 문제를 예방 할 수 있게 도와주었다. 하지만 여전히 ‘기존 방문기록, 북마크, 비밀번호 등’ 여러 정보들을 볼 수 있다. 브라우저 입장에서 웹 어플리케이션을 통해 사용자가 웹의 편리하고 멋진 기능들을 사용할 수 있게끔 발전시켰다고 볼 수 있다. 하지만 편리할 수록

사용자는 자신의 개인정보를 보호받지 못하므로 이러한 웹을 사용할 때 피할수 없는 혼란스러움을 느낄 수밖에 없다. 따라서, 사용자는 급속히 발전하는 웹의 기능을 안전하고 효율적으로 사용하기 위해서 개인적으로 노력이 요구되는 실정이다. 하지만 이러한 사용자의 작지만 적극적인 노력이 있다면 더욱 발전하고 다양하고 효과적인 웹 어플리케이션에 발맞추어 보다 편안한 마음으로 안전하게 사용할 수 있지 않을까 기대해 본다.

참 고 문 헌

- [1] <http://ko.wikipedia.org/wiki/HTML5>
- [2] http://navercast.naver.com/contents.nhn?rid=122&contents_id=50994
- [3] <http://www.hacking-tutorial.com/tips-and-trick/how-to-delete-browser-cookies-cache-and-history/#sthash.Y44WN8kU.dpbs>
- [4] <http://ryuseunghyun.tistory.com/2749>
- [5] <http://croute.me/419>
- [6] http://navercast.naver.com/contents.nhn?rid=122&contents_id=50994
- [7] <http://caniuse.com/>
- [8] <https://support.google.com/chrome/answer/95464>

● 저 자 소개 ●



윤 수 지

2012년-현재 서울여자대학교 멀티미디어학과 재학 중
관심분야 : 웹프로그래밍, 안드로이드 프로그래밍, 아두이노 프로그래밍



송 신 예

2012년-현재 서울여자대학교 멀티미디어학과 재학 중
관심분야 : 웹프로그래밍, 서버프로그래밍



이 솔

2012년-현재 서울여자대학교 콘텐츠디자인학과 재학 중
관심분야 : 웹프로그래밍, 서버프로그래밍



이 현 진

2012년-현재 서울여자대학교 멀티미디어학과 재학 중
관심분야 : 웹프로그래밍, 서버프로그래밍



백 종 호

1994년 중앙대학교 전기공학과 공학사
1997년 중앙대학교 전기공학과 공학석사
2007년 중앙대학교 전자전기공학부 공학박사
1997년-2011년 전자부품연구원 모바일단말연구센터 센터장
2011년-현재 서울여자대학교 멀티미디어학과 조교수
관심분야 : 차세대 방송통신 시스템, 차세대 영상시스템, 소프트웨어 테스트