제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

모바일 환경에서 GPS 위치정보를 이용한 인증 보안 강화

한근석*
*고려대학교 컴퓨터정보통신대학원 컴퓨터정보통신공학과
e-mail:mosaic79@korea.ac.kr

Enhancement of Authentication Security Using GPS Location Information in Mobile Environment

KeunSeok Han*
*Graduate School of Computer Information & Communication, Korea University

요 약

모바일 네트워크 고도화 및 네트워크와 단말기의 비약적인 발전으로 모바일 기기의 보급이 확산되고, 시장의 경쟁 본격화에 따른 개방형 플랫폼 증가와 애플리케이션 및 모바일 웹의 활성화가 이뤄지고 있다. 또한 모바일 환경에서의 개발이 표준화 되어가면서 제작 및 배포가 용이해지고 있다. 이러한 환경적인 영향으로 모바일 웹 및 어플리케이션에 대한 보안 위협은 더욱 가중되고 있으며 공격의 규모 및 피해가 증가될 것으로 예상된다. 본 논문에서는 이러한 모바일 환경에서 인증 보안을 강화하기 위해 인증 서비스에 위치정보를 활용하는 방안을 제안하고 개인별로 특화된 인증에 관련된 LBS(Location-Based Service)를 제공할 수 있는 시스템을 구현한다. 이 시스템의 구현을 통해 사용자 위치에 따라 인증 유효성 여부를 체크함으로써 현재의 인증시스템에서 신뢰성과 유효성을 추가적으로 확보 할 수 있음을 증명하고 구체적인 활용 방안을 제안한다.

1. 서론

모바일 인터넷 가입자 수가 세계적으로 최근 급속히 증가 하고 있으며 모바일 데이터 트래픽은 가입자 수 증가세를 훨씬 넘어설 것으로 전망되고 있다. Ovum의 자료에 따르면 전 세계 모바일 인터넷 가입자 수는 연평균 50%의 성장률을 보이며, 2008년 1억8천만 명 규모에서 2014년에는 2008년 대비1024%인 20억 명 수준으로 증가할 것으로 예측하고 있다. 이러한 모바일 인터넷 가입자 수의 증가와 함께 무선 데이터 트래픽도 급격히 증가할 것으로 예측되고 있다. Cisco는 4G의 보급과 함께 전세계 모바일 트래픽이 2013년까지 연평균 131%의 증가율로 증가하여 2008년 대비 66배까지 증가할 것으로 예상하고 있다[1]. 이러한 모바일 데이터 트래픽의 급격한 증가에 따라 보안 위협 또한 급격히 증가하는 추세이다.

모바일 인터넷의 응용서비스는 일반적으로 스마트폰, 스마트패드, PDA 등과 같은 다양한 모바일 기기를 대상으로 하기 때문에 단말 특성에 적합한 컨텐츠나 비즈니스 모델을 제공하게 된다[2]. 인증프로세스 역시 모바일 환경 특성에 맞게 구성되는데 입력장치의 제약과 인터넷 접속 환경의 잦은 변경 등으로 인해 PC와 같은 유선장치의 인증보다 단순화된 방식으로 제공되고 있는 실정이다. 이러한 모바일 환경의 변화는 단순화 특성과 보안성 확보에 대한 조율을 필요로 하게 된다.

스마트폰은 전세계적으로 모바일 장치 시장에서 가장 빠르게 성장하고 있다. 모바일 통계기관인 가트너(Gartner, Inc.)에 따르면 2010년 모바일 기기의 판매량은 16억대에 이르며 스마트폰의 판매량은 전년대비 72% 성장했다고 한다[3]. 스마트폰이 가진 즉각적인 정보접근 및 통신의 편리성과 더불어 네트워크의 발전으로 스마트폰의 폭발적인 성장을 가지고 온 것이다. 하지만 스마트폰 등의 모바일 기기에 웹브라우징 기능이 추가가 되면서 모바일 웹기반의 해킹 및 감염이 확산될 가능성이 커지게 되었다. 또한 웹서비스에서 개방형 플랫폼 및 오픈소스의 활용이 증가함에 따라 상대적인 보안 위험성 증가하게 되었다. 본 논문에서는 모바일 환경에서 웹기반의 인증보안을 강화할수 있는 방법에 대해 제안하였으며 웹서비스에서 인증의 보안을 지키기 위해 사용하고 있는 방안들을 소개하고 보다 강화된 인증시스템의 설계 및 구현을 통해 이를 증명하도록 한다.

2. 웹기반의 인증 보안방안 및 문제점

1) OTP (One Time Password)

사용자가 인증을 받고자 할 때마다 매번 새로운 비밀번호가 자동으로 생성되는 보안 시스템으로, 한번 사용하고

버리는 일회용 비밀번호를 말한다. 최근 고도화 되고 있는 해킹, 패스워드 유출과 같은 위험의 증가로 정보보호 기능이 위험에 노출되고 있다. 키로깅(Key-Logging), 스니핑(Sniffing), 피싱(Phishing) 등 비밀번호 탈취를 위한 여러 방법들이 존재하고 있고 이를 방어하기 위한 방화벽 등 네트워크 보안이 이루어지고 있으나 아이디와 비밀번호가 노출되면 결국은 인증의 실패를 가져오게 된다. 따라서 OTP 시스템은 인증방식으로 더욱 부각되고 있다[4].

2) ActiveX

우리나라는 전자정부(E-Gov), 포털(Portal), 전자상거래(E-Commerce), 금융(Internet Banking) 등 웹을 통한 다양한 온라인 서비스를 제공하고 있으며, 이러한 온라인 서비스 제공시 정적인 HTML의 스크립트방식을 탈피하여 이용자들에게 보다 확장된 대화형의 동적인 서비스 제공을 위해 Microsoft사에서 개발한 ActiveX 기술을 사용하고 있다[5]. 하지만 크로스웹 브라우징문제, 취약점을 이용한 악성프로그램 배포 등의 문제로 ActiveX 사용을 지양하고 있는 실정이다.

3) IP보안

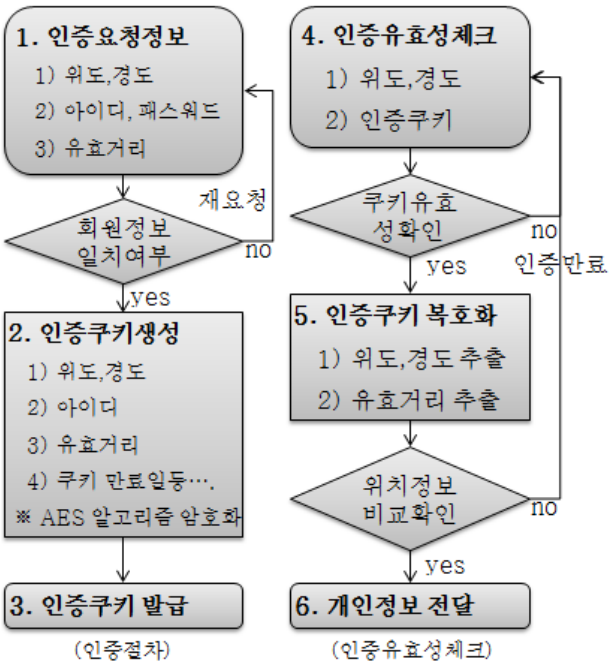
IP주소정보의 사용범위를 사용자의 인터넷 접속환경에 단계별로 설정할 수 있도록 하여 타인이 로그인 권한을 가로채어 부정하게 사용하는 것을 방지하는, 사용성 및 보안성이 강화된 로그인 상태 관리 서비스다. IP보안 서비스 제공 업체에 따라 제한 단계에 차이가 있지만 보통 아래와 같은 단계로 나누어 제한된다.

1단계: IP의 C클래스까지 제한
2단계: 최근 로그인 IP주소와 동일하지 않을 경우 제한
3단계: 로그인 시점의 IP주소와 다를 경우 인증만료

서론에서도 잠시 언급했듯이 모바일 기기에 웹브라우징 서비스가 기본으로 탑재됨에 따라 무선 환경에서도 웹기반의 해킹에 노출될 수밖에 없다. OTP와 같은 경우는 패스워드의 입력시점에 보안은 확보할 수 있으나 OTP인증 이후의 인증 쿠키정보의 보안까지 확보할 수 없다. 그래서 주요 포털에서는 추가적으로 IP정보를 사용하여 인증쿠키의 재사용에 대한 유효성을 검증하고 있다. 하지만 모바일 환경에서는 기기의 이동에 따라 IP정보가 수시로 바뀌게 되므로 IP 정보만으로는 인증정보의 유효성을 확보 할 수 없게 된다.

3. 위치정보를 활용한 인증보안 방안

모바일 환경일 경우 기존의 인증시스템과 같이 사용자가 로그인 시점의 IP주소로 인증쿠키의 유효성을 체크하게 되면 사용자의 이동에 따라 IP가 변하는 시점에 인증쿠키의 유효성이 만료되어 재로그인이 필요하게 된다. 그래서 모바일 환경일 경우에는 IP정보를 대신하여 위치정보를 수신하는 방법으로 이 문제를 해결하고자 한다. 최초 로그인 시점에 아이디, 패스워드 정보와 함께 위치 정보 및 유효거리를 수신하여 인증쿠키를 생성할 때 위치정보를 함께 암호화하여 사용자의 브라우저에 설정한다. 추후 쿠키를 통한 인증정보 확인 요청시 기존에 발급한 인증쿠키 정보와 새로운 위치정보를 받은 후 인증쿠키를 복호화하여 저장된 위치정보와 새로운 위치정보를 비교하여 인증 유효성을 체크한다. 최초 로그인시 저장된 위치정보 값에서 100m, 1km, 10km 등의 거리정보를 사용하여 인증쿠키의 유효성을 단계별로 보장할 수 있다. (그림 3)은 인증시스템의 흐름도이며 인증쿠키는 AES알고리즘으로 암호화되어 인증시스템에서만 암복호화 할 수 있도록 구성한다. 인증쿠키 복호화 이후 위치정보의 비교는 쿠키에 포함된 위치정보와 현재의 위치정보와의 거리를 Haversine Formula 수식[6]을 통해 계산하여 로그인시 입력된 유효거리 이내에 있을 경우에만 유효하다고 판단하여 개인정보를 확인해준다.



(그림 1) 인증시스템

4. 인증 시스템의 설계 및 구현

4.1 구현환경

본 시스템은 Java 언어를 이용하였으며 Spring프레임워크 기반으로 구성하였다. 암호화 방식은 AES알고리즘을 사용하였고 로그인시점의 위치정보와 인증확인시점의 위치정보간 거리계산은 Haversine Formula을 이용하였다. 추가적인 상세 환경은 <표 1>에서 정의하였다.

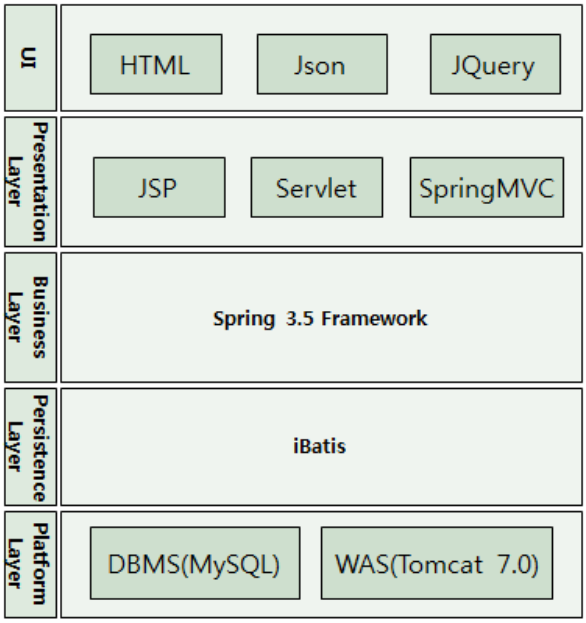
<표 1> 시스템 개발환경 및 사용기술

개발환경	적용기술
WAS	Apche Tomcat 7.0
Database	MySql v5.5
Framework	Spring, ibatis

개발언어	Java
인증쿠키 암호화 방식	AES 알고리즘
위치간 거리계산	Haversine Formula 수식

4.2 시스템구조

웹 서비스의 시스템 구조는 Presentation Layer에서 SpringMVC 사용하였고 Jsp, Ajax를 이용하여 보완하였다. Business Layer에서 Spring 3.5 프레임워크를 이용하여 bean객체를 관리하였으며 ibatis프레임워크를 이용하여 Persistence Layer를 구성하였다. 전체적인 시스템 구조는 (그림 2)와 같다.



(그림 2) 웹 서비스의 시스템 구조

4.3 구현

기존의 인증시스템과는 달리 (그림 3)에서처럼 인증 요청 정보를 받는 화면에서 아이디, 패스워드 정보이외에 위치 정보와 유효거리가 필요하다. 파라미터 전송은 보안성 확보를 위해 SSL방식의 전송이나 RSA 공개키 암호 방식이 필수적이다. 클라이언트에서 위치정보추출이 가능한 브라우저 여부를 확인하고 위치정보 사용 동의 절차를 거친 뒤 요청된 모든 파라미터를 송신한다. 서버는 가입여부와 비밀번호 일치여부를 체크하고 (그림 4)의 변수 값과 같이 개인정보 나열 값을 AES방식으로 암호화하여 인증쿠키에 설정한 후 (그림 3)의 개인정보 조회화면을 보여준다.

(그림 3) 로그인시도 및 개인정보 조회화면 예

원문:
7:mosaic79:126.977969:37.566535:1:SUCCESS
AES암호화값:
OvyRRVPpWrPxUKrVvWiMqF5DNNQvYSG8sru
ZFv0Ph0dxF0nt6f4kWT5qG8KKQvVU

(그림 4) AES 암호화값

인증이 정상적으로 완료된 이후 인증 쿠키 값을 이용한 유효성 체크가 필요하다. 이를 위해서 우선 브라우저에 설정되어있는 인증쿠키와 함께 현재의 위치정보를 가지고 온다. 쿠키만료일을 체크하고 AES알고리즘을 이용해 쿠키 정보를 복호화 하여 로그인 성공여부를 확인한 후 로그인 시점의 위치정보 및 유효거리를 추출한다. 그리고 (그림 5)에서 기술한 Haversine Formula 소스코드을 통해 현재의 위치정보와 쿠키에 포함된 위치의 거리를 계산한다. 계산된 거리가 설정된 유효거리 100m, 1km를 벗어나지 않을 경우에만 인증쿠키의 유효성을 확보 할 수 있다.

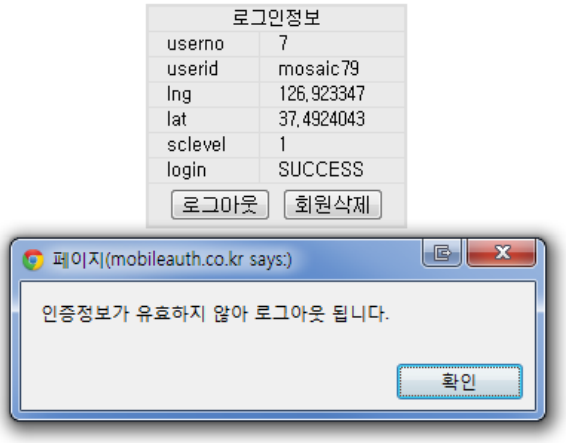
```
public static double distance(double lat1,
double lon1,double lat2,double lon2,char unit) {
double theta = lon1 - lon2;
double dist = Math.sin(deg2rad(lat1))
* Math.sin(deg2rad(lat2))
+ Math.cos(deg2rad(lat1)) * Math.cos(deg2rad(lat2))
* Math.cos(deg2rad(theta));
dist = Math.acos(dist);
dist = rad2deg(dist);
dist = dist * 60 * 1.1515;
if (unit == 'K') {
dist = dist * 1.609344;
} else if (unit == 'N') {
dist = dist * 0.8684;
}
return (dist);
}
```

(그림 5) Haversine Formula 수식

마지막으로 개인정보 조회 화면은 호출될 때마다 인증쿠키의 유효성을 확인하게 되는데 위와 같은 유효성체크 과정을 모두 거친 후 인증정보가 유효하지 않을 경우 (그림 6)의 메시지를 보여주며 자동으로 로그아웃된다.

4.4 시스템 검증

시스템의 검증을 위해 (그림 7)의 A지점에서 유효거리를 100m로 설정한 이후 로그인한다. 그리고 XSS(Cross-site scripting)공격[7] 등으로 인해 인증쿠키가 노출되었을 경우를 가정하며 인증쿠키정보를 추출한다. 우선, B지점까지의 위치정보를 랜덤하게 추출하고 위에서 추출한 쿠키정보를 헤더에 설정하여 인증 유효성 체크가 가능한 개인정



(그림 6) 인증만료화면

보 조회 페이지를 호출하였다. 이 경우 인증이 정상적으로 처리되어 개인정보 조회페이지가 호출됨을 확인할 수 있었다. 다음으로 유효거리 100m를 벗어난 C지점에서 위치정보와 추출된 인증쿠키를 이용하여 로그인 검증 값을 확인해 보았다. 해당 위치에서되지 않음을 확인할 수 있었다.

(그림 7) 로그인 검증지점

4.5 구현 시스템의 문제점 및 해결방안

현재 시스템에서 구현되지는 않았지만 인증쿠키 정보를 획득한 이후에 무작위의 위치정보를 입력하여 권한을 획득하기 위한 brute force 공격이 이루어질 가능성이 있다. 이 공격을 방어하기 위해 같은 인증쿠키로 짧은 시간에 많은 요청이 올 경우에 해당쿠키를 만료시키는 방법을 사용할 수 있다. 공격규모에 따라 유동적으로 시간당 허용 요청 값을 조절한다면 효과적인 방어가 가능할 것이다. 또한, 보안성을 확보하기 위해서는 인증요청시점에서 위치정보의 노출여부가 매우 중요하다. 그러므로 파라미터의 전송시 암호화 처리를 위해 SSL 인증서 설치 또는 RSA 공개키 암호화 방식을 이용하여 해결해야 한다.

GPS 위치정보의 오차에 따라 원하는 지점에서의 인증이 정확하게 이루어지지 않을 가능성이 존재한다. 따라서 현재 시스템에서는 포함되지 않았지만 보안성 확보를 위해 위치정보의 보정작업이 필수적으로 고려되어야 한다.

5. 결론

본 논문에서는 무선 환경 일 경우 인증정보가 노출되었을 경우 IP보안을 대체하여 위치정보를 사용하여 위치정보에 대한 유효성을 체크하여 사용자를 보호할 수 있음을 확인하였다. 이러한 보안방식은 위치정보를 활용하여 시, 군, 구 혹은 특정 버스노선 등에서만 인증정보를 유효하게 가져갈 수 있도록 구성 가능하다. 그리고 강화된 인증을 위해 로그인 후 위치정보를 등록하여 특정지점에서만 인증이 가능하도록 구현할 수 있으며 이러한 방식을 사용할 경우 아이디와 비밀번호가 노출된 경우에도 사전에 등록된 위치정보를 알지 못하면 인증이 불가능하므로 기존 인증에 비해 강화된 보안성을 확보할 수 있다. 또한 본 시스템에 시간정보를 추가한다면 물리적으로 이동할 수 있는 거리 혹은 사용자가 직접 설정한 시간당 거리 정보 이내에 있는 경우에만 인증 유효성을 확보해주는 방식으로 보다 유연하게 구성 할 수 있다.

참고문헌

[1] 전종홍, 이승윤, “차세대 모바일 웹 애플리케이션 표준화 동향”, 전자통신동향분석 제 25권 제1호, 2010. 2.

[2] 김수형, 장철수, 노명찬, 김중배, “모바일 환경 적응 시스템을 위한 보안 서비스 구조 설계 및 구현” 한국정보과학회 제31권 제1호(A), 2004. 4.

[3] Gartner, Inc, http://www.gartner.com

[4] 김대진, 최홍섭, “OTP를 이용한 IPTV콘텐츠 보호 및 인증 시스템 설계” 한국콘텐츠학회논문지 제 9권 제8호, 2009. 8.

[5] 박성용, 문종섭, “보안 인증을 통한 ActiveX Control 보안 관리 모델에 관한 연구” 정보보호학회지 제 19권 제6호, 2009. 12.

[6] Haversine formula, http://en.wikipedia.org/wiki/Haversine_formula

[7] Cross-site scripting, http://en.wikipedia.org/wiki/Cross-site_scripting

한 근 석
2006년 한국항공대학교 컴퓨터공학과 졸업 (학사)
2009년~현재 고려대학교 컴퓨터정보통신대학원 컴퓨터 정보통신공학과(석사)