모바일 환경을 위한 웹 애플리케이션 서비스의 세션 관리 개선방안

김영훈* ,박용석*

*정보보호대학원, 세종사이버대학교

Improved Session Management for Mobile Workflow in Web Application Service

Young-hun Kim* ,Yongsuk Park*

*The Graduate School of Info Security. Sejong Cyber University

E-mail : roadak1984@gmail.com, yongspark@sjcu.ac.kr

요 약

스마트 단말기의 대중화로 모바일을 통한 업무 처리가 선호되고 있다. 모바일 기기를 통한 인터넷 접속 비율도 2012년 9월 기준으로 PC 대비 30%에 이르고 있다. 모바일 시대에 나타나는 사이버 보안 위협의 특징은 기존의 인터넷에서 발생되는 보안 위협이 모바일 환경에서도 그대로 재현된다는 점이다.

웹 애플리케이션 보안 연구 기관인 OWASP (The Open Web Application Security Project)가 경고하는 세션 관리의 취약점은 앞으로 모바일 환경에서도 대비해야 하는 이슈이다. 하지만 모바일과 데스크탑 컴퓨터의 세션 관리 환경은 크게 다르다. 본 학술지는 모바일 환경에 맞게 개선된 세션 관리 방식을 제안한다.

ABSTRACT

It is preferred to the popularization of smart device business processes through mobile. The ratio of Internet access via mobile devices is reached 30% of PC in September 2012. It is reproduced in a mobile environment that security threats arising from the Internet. that is the characteristics of cyber security threats appearing on the mobile era.

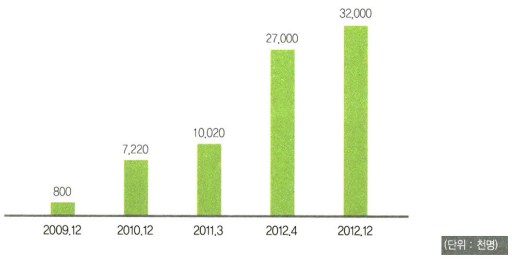
Web Application Service security research firm OWASP (The Open Web Application Security Project) issued Session Management threat. That threat will be reproduced in the mobile environment. But Mobile is significantly different from Desktop Computer about Session Management environment. This proceeding proposes a improved Session Management method in Mobile environment.

키워드

모바일 보안, 웹 애플리케이션 서비스, 세션 관리, OWASP

Ⅰ. 서 론

일반폰보다 월등히 뛰어난 성능을 가진 스마트폰으로 등장으로 인해 모바일 단말기는 규모면에서 빠르게 증가하고 있다. 스마트폰 가입자 수는 2009년 9월 80만 명에서 2012년 12월에 3200만 명으로 늘어났다. 스마트폰과 같은 모바일 기기의 대중화로 많은 사람들이 휴대용 단말기로 인터넷에 편리하게 접근하고 있다. [1]



[출처 : 방송통신위원회, 유·무선 가입자 통계현황, 무선 트래픽 이용현황, 2013. 1]

도표 1. 스마트폰 가입자 수 추이

스마트폰 이용 확산은 시간과 장소에 구애받지 않고 무선 인터넷을 활용할 수 있게 해주어 기존 인터넷 사이트의 환경도 모바일 환경 변화에 맞춰 변화되고 있다. PC 환경에서 제공하는 인터넷 서비스가 모바일 환경으로 전환되면서 PC 환경의 보안 위협이 스마트폰 환경에서도 나타날 것으로 예상된다.[2]

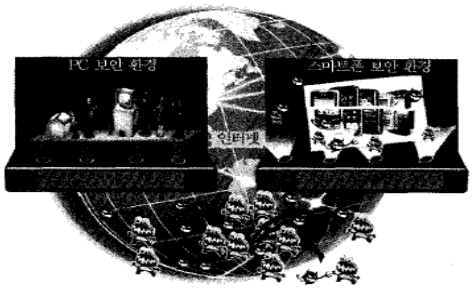


그림 1. PC와 스마트폰의 환경 차이

특히 인터넷의 기반인 HTTP는 매번 서버에 접속했다가 연결을 끊는 과정을 반복하는 상태 비유지 프로토콜이기 때문에 사용자의 상태 정보를 유지하지 않는다. 그래서 웹 어플리케이션 서비스는 개별 사용자들의 접속을 유지하기 위해 세션을 사용한다. 세션은 사용자 인증 정보의 유지하기 위해 클라이언트에 공유되므로 공격자가 악용할 수 있다.[3]

본 논문은 웹 어플리케이션 서비스에서 가장 기본적으로 보안이 보장되어야 하는 세션의 관리 방식을 검토하고 모바일 환경에 맞게 개선하는 방안을 제안한다.

II. 관련연구

2.1 SSL 세션 관리

OWASP (Open Web Application Security Project)는 인터넷을 구성하는 웹 어플리케이션 취약점에 대한 연구와 그 결과를 제공하는 권위 있는 기관이다. OWASP는 3년 마다 웹 어플리케이션에서 발생하는 특정 카테고리의 취약점들을 중심으로 즉시 개선이 필요한 취약점 리스트를 소개한다.[4]

이 중 'A2 – 인증 및 세션 관리 취약점'은 세션 토큰이 적절히 보호되지 못해서 패스워드나 세션 키, 그리고 세션쿠키 등이 공격자에게 악용되어 인증을 우회하고 다른 사용자로 가장하여 접속할 수 있는 취약성이다. [4]

OWASP는 네트워크 Sniffing으로 세션이 도용되는 취약점을 방지하기 위해 암호화 채널(SSL)을 통해 Session ID를 보호하는 방식을 제안한다. SSL은 전송 중의 자격증명을 보호하기 위한 효과적인 방법으로 널리 활용할 수 있다.[5]

A1 – 인젝션
A2 – 인증 및 세션 관리 취약점
A3 – 크로스 사이트 스크립팅 (XSS)
A4 – 취약한 직접 객체 참조
A5 – 보안 설정 오류
A6 – 민감 데이터 노출
A7 – 기능 수준의 접근 통제 누락
A8 – 크로스 사이트 요청 변조 (CSRF)
A9 – 알려진 취약점이 있는 컴포넌트 사용
A10 – 검증되지 않은 리다이렉트 및 포워드

도표 2. OWASP Top 10 (2013)

2.2 세션 암호화

세션을 생성할 때 사용자 인증정보와 함께 생성된 세션을 강력한 암호 알고리즘으로 암호화하여 저장함으로써 유효성을 강화할 수 있다. 공격자가 세션의 암호화 코드를 본다 해도 값을 변경할 수 없도록 인증 정보도 같이 암호화하여 분석하지 못하게 제안하였다.[6]

2.3 세션 변조 차단

인트라넷 시스템에서 세션 생성과 검증 부분에 고유 식별자로 IP주소를 이용한 변조 차단 알고리즘이 제안되었다. 패스워드 검증이 통과된 접속자 PC IP주소를 포함하여 세션을 생성한다. 세션이 생성될 때마다 접속자 IP주소를 저장함으로써 최근 IP주소를 유지하고 이를 통해 동시에 한명만 로그인하여 사용할 수 있게 보장하였다. [7]

III. 본 론

3.1 기존 연구의 한계

기존 연구는 인증에 성공한 세션을 암호화하거나, 인트라넷에서 할당된 고정 IP를 고유한 식별자로 사용하여 취약점을 해결하는 방안을 제시하고 있다.

그러나 SSL은 데이터 전송 중간지점에서 해당 Session ID를 변조하는 것을 방지해 줄 뿐이다. 공격자는 클라이언트에서 XSS공격 등으로 세션 정보를 가로채어 Session Hijacking 공격을 할 수 있다.

세션 암호화 방식은 암호화된 세션을 그대로 도용하면 다른 IP의 컴퓨터에서 공격자가 인증된 사용자로 위장할 수 있다.

세션 변조 차단 방식으로 생성된 세션은 평문으로 노출되므로 공격자가 변조하여 정상적인 작업으로 간주되게 악용될 수 있다. 또한 무선 네트워크 환경의 유동 IP를 고유한 식별자로 활용할 수 없다.

기존의 연구는 인트라넷을 기반으로 하는 고정 IP와 데스크탑 컴퓨터의 고성능을 가정하고 있다. 이에 반해 모바일 환경은 무선 네트워크를 활용하는 유동IP이며 휴대용 단말기로써의 성능 한계도 존재한다. 그러므로 모바일 고유 식별자를 이용하는 효율적인 세션 관리가 필요하다.

3.2 모바일 고유 식별자 IMEI

IMEI(International Mobile Station Equipment Identity)는 국제적으로 유일하게 부여된 식별번호이며 15자리 숫자로 구성되어 있다. 15자리 하드웨어번호는 GSM(Global System for Mobile Communications) 표준에서 제조업체에 의해서 단말기 하드웨어 제작시 할당되며, 이 번호는 형식 승인 코드, 최종 조합 코드 및 일련 번호를 포함하고 있다. 이를 통해 3G/4G 이동 단말기가 서로를 고유하게 식별한다.[8]

정보	TAC	SNR	spare
크기	8 bits	6 bits	0 or 1 bit
* TAC : Type Allocation Code			
* SNR : Serial Number			

도표 3. IMEI의 구조

OWASP Mobile Security Project에서도 IMEI를 모바일 웹 세션에서 활용하는 아이디어가 논의되고 있다.[9][10]

현실적으로 모바일 웹 세션은 보안을 위해 HW Reset이나 Session Timeout, Logout 등의 이벤트에 대해 기존 세션 무효화를 보장해야 하므로 IMEI를 활용한 세션 관리가 오히려 적합하다.

3.3 ISeM 세션 관리 방식

본 논문에서는 모바일 고유 식별자인 IMEI를 활용하는 세션 관리 방식인 ISeM(IMEI based Session Management)을 제안한다. 모바일 시대에는 휴대용 단말기를 기반으로 하는 모바일 환경 세션 관리가 필요하다. 모바일은 3G/4G와 Wifi를 기반으로 통신하므로 네트워크 환경에 따라 변하는 IP가 아닌 별도의 고유 식별자로 세션을 관리해야 한다.

모바일 단말기의 고유 식별자인 IMEI와 서버 시스템 시간은 모바일 환경에서 세션 관리에 활용하기 적합하다. 식별 토큰이 매 접근마다 최신 시스템 시간으로 갱신된다면, 공격자는 네트워크 스니핑으로 수집된 이전 식별 토큰을 도용하기 힘들다. 또한 서버에서 HTTP요청마다 IMEI를 검증한다면, 공격자가 XSS 공격으로 세션을 탈취해도 소용이 없다. 이러면 공격자가 개입한 시점에서 식별 토큰의 상태가 바뀌므로 보안을 강화할 수 있다. 공격자가 송신한 시점에서 식별 토큰을 탈취해도 시스템 시간으로 갱신되었기에 재활용할 수 없다. 공격자가 수신한 시점에서 식별 토큰을 탈취해도 IMEI로 재검증하므로 잘못된 접근으로 세션은 무효화된다.

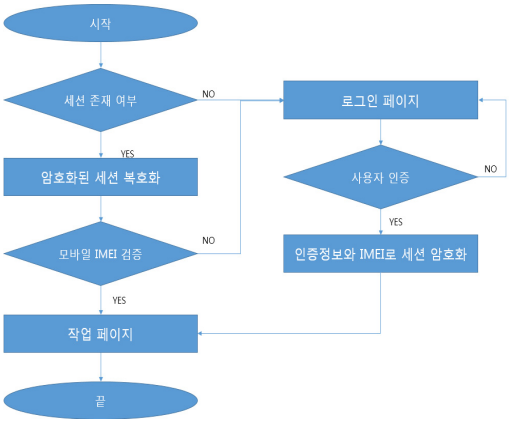


그림 2. ISeM 방안 시스템 흐름도

Ⅳ. 결 론

모바일 환경에서 인터넷 접근은 더욱 증가하고 있다. HTTP는 상태 비유지 프로토콜이기 때문에 접속자 정보를 유지하기 위해 세션이 필요하다. 이런 세션 관리는 웹 어플리케이션 서비스의 취약점 중 하나이다.

모바일 환경에서 고유 식별 번호인 IMEI를 활용해서 생성한 세션은 차후 더욱 확대될 모바일 인터넷 보안에 큰 도움을 줄 수 있다.

참고문헌

[1] 국가정보원, "국가정보보호백서", 2013.
[2] KISA, "국내 모바일 환경에서의 신규취약점 발굴 및 분석방법연구", 2012.11.
[3] The Internet Society, "Hypertext Transfer Protocol - HTTP/1.1", 1999.7.
[4] OWASP, "OWASP Top 10", 2013.6., https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[5] The Internet Society, "HTTP over TLS - HTTPS", 2000., http://www.ietf.org/rfc/rfc2818.txt
[6] 홍성민(경북대학교), "사용자 인증과 파라미터 암호화를 이용한 웹 공격 차단 알고리즘", 2007.
[7] 김종섭(고려대학원), "웹 어플리케이션에서 인증과 세션 취약점 개선방안에 관한 연구", 2005.
[8] 3GPP, “Numbering, Addressing and Identification, TS 23.003 V7.9.0", 2009.
[9] OWASP, "Mobile Security Project", 2011.11., https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_Ten_Mobile_Risks
[10] OWASP "OWASP Top 10 Mobile Risk", 2011.11., http://www.slideshare.net/JackMannino/owasp-top-10-mobile-risks