[정보보호] ITU-T SG17 차세대 웹 서비스 정보보호 표준화 동향

개요

웹 2.0과 매시업(Mashup)과 같은 기능이 향상된 웹 기술은 월드 와이드 웹(World Wide Web) 서비스 사용에 있어서, 사용자 간의 창의력, 정보공유 및 협업을 촉진하는 것을 목표로 하는 경향이 있다. 즉, 개발자에게 효율적이고 비용절감 및 새로운 서비스를 개발과 배포가 용이하고, 다양한 소스로부터 콘텐츠 통합을 쉽고 빠르게 지원 가능하게 함으로써 차세대 웹 기술이 통신 서비스에 적용되고 있다.

그러나 차세대 웹 애플리케이션은 전통적인 웹 응용 프로그램과 같은 보안 문제가 있을 뿐만 아니라, 신 기술에 의한 특정한 위험들을 내포하고 있다. 따라서 이러한 기술로부터 발생되는 보안 위협들이 식별되어야 하며, 차세대 웹 서비스에 대한 보안 요구 사항 및 보안 기능들이 제공되어야 한다.

ITU-T SG17 Q.7(안전한 응용서비스)에서 개발되고 있는 표준권고안은 차세대 웹 기반 통신 서비스에 대한 보안 위협, 보안 요구사항, 보안 기능 그리고 보안 프레임워크를 제시한다.

차세대 웹 서비스 위협

웹 2.0 및 매시업 등과 같은 기술을 사용하여 융합 서비스를 제공하는 차세대 웹 서비스 환경에서 발생할 수 있는 위협들은 전통적인 웹 서비스 환경에서 존재하는 위협들과 차세대 웹 서비스 환경에서 발생되는 추가적인 위협으로 구분된다. 전통적 웹 서비스 환경에서의 위협들은 DoS(Denial of Service), 도청(Eavesdropping), MITB(Man in the Browser), MITM(Man in the Middle), 위장(Masqerade), 메시지 변조, 부인(Repudiation), 재공격(Replay) 등과 같은 것이 있으며, 차세대 웹 서비스 환경에서의 위협으로는 다음과 같은 것들이 제시되었다.

- **자동작업 갈취(Exploiting silent transaction)**

하나의 요청으로 일련의 동작이 자동으로 수행되는 트랜잭션을 처리하는 모든 시스템은 클라이언트에 위험하다. 일반적으로 웹 응용 프로그램은 단순히 URL 제출을 허용하는 경우에, 사용자의 승인 없이도 사전에 짜여진 세션 공격으로 공격자는 목적을 달성할 수 있다. 에이젝스(AJAX: Asynchoronous JavaScript and XML)에서 트랜잭션은 일련의 동작이 자동으로 수행된다. 그래서 사용자의 피드백 없이 페이지에 주입공격 스크립트 같은 악의적인 행위가 허가 없이 클라이언트에서 발생될 수 있다.

• **크로스 사이트 요청 위조(Cross-Site Request Forgery: CSRF)**

크로스 사이트 요청 위조 공격은 무의식적으로 취약한 웹사이트에 하나 이상의 HTTP 요청을 제출하는 이용자가 피해자가 된다. 전형적인 크로스 사이트 요청 위조 공격은 데이터 무결성을 훼손하고, 그것은 공격자에게 취약한 웹사이트에서 저장된 정보를 수정할 수 있는 능력을 제공한다.

• **크로스 사이트 스크립팅(Cross-Site Scripting : XSS)**

크로스 사이트 스크립팅은 신뢰할 수 있는 콘텐츠에 악성코드가 주입되는 공격 유형이다. 크로스 사이트 스크립팅 공격은 마치 브라우저 사용자로서 세션 쿠키를 훔치고, 접근 제한된 정보를 액세스하고, 웹 페이지의 일부를 재 작성할 수 있다. 크로스 사이트 스크립팅은 반사 크로스 사이트 스크립팅 및 저장 크로스 사이트 스크립팅으로 두 종류의 공격이 있다.

• **제이슨 하이재킹**

제이슨(JavaScript Object Notation) 하이재킹은 크로스 사이트 요청 위조 공격과 기밀성 타격 기법을 기초로 한다. 공격자는 공격 대상자의 정보를 읽을 수 있다. 제이슨은 자바스크립트로 작성되며 정보교환을 위하여, 배열과 객체의 데이터 구조에 기반을 두고 있으며, 제이슨의 배열은 제이슨 하이재킹에 직접적으로 취약점을 나타낸다.

• **파손된 자바스크립트 객체 직렬화(Malformed JavaScript Object serialization)**

자바스크립트는 객체지향 프로그래밍(OOP) 기술을 지원한다. 자바스크립트에는 여러 내장(built-in) 객체가 있으며, 새로운 객체가 쉽게 생성될 수 있는데, 프로그래머는 임의 변수에 값을 할당하고 수행할 수 있다. 공격자가 스크립트 임베디드 부분인 제목 라인에 악의적 제목을 보내면 그것을 읽는 독자는 크로스 사이트 스크립팅 공격의 피해자가 되는 것이다. 자바스크립트 객체는 데이터와 메소드를 모두 가지고 있으며, 자바스크립트 객체 직렬화의 부적절한 사용은 교묘한 패킷 주입 코드에 의해 악용되어 보안 취약점을 열어주게 된다.

• **스크립트 주입(Script injection in DOM)**

객체의 직렬화 스트림이 브라우저에 접수되면, 개발자는 DOM(Document Object Model)에 액세스하는 특정 호출을 만든다. 목표는 새로운 콘텐츠를 DOM에 'recharge' 또는 'repaint' 하는 것이다. 이것은 사용자 함수 *document.write()* 또는 *eval()* 을 호출하여 수행할 수 있다. 이러한 함수가 신뢰할 수 없는 정보 흐름에 호출되면, 브라우저는 DOM 조작 취약점에 취약하게 된다. DOM의 컨텍스트에 크로스 사이트 스크립팅을 삽입하는 공격자가 활용할 수 있는 여러 *document.*()* 호출이 있으며, 만약 그 호출이 자바 스크립트를 포함하고 있으면, 브라우저에서 실행하게 된다.

• 주입(Injection Flaws)

주입은 사용자가 제공한 데이터가 명령이나 쿼리의 일부로 인터프리터에 보내질 때 발생한다. 공격자의 악의적인 데이터는 인터프리터를 의도하지 않은 명령을 실행하거나 데이터를 변경하도록 속인다.

• 세션 하이재킹과 도용(Session hijacking and theft)

일부 웹 서비스 제공자가 서비스 요구자를 확인하기 위해 통신 중에 세션 식별자를 사용한다. 공격자는 웹 서비스 제공자와 소비자 사이의 세션을 하이잭하기 위하여 식별자 정보를 훔치고 사용할 수 있다.

• 익명 사용자 위장(Masquerade of anonymous user)

웹 기반 통신 서비스는 인증서 기반의 사용자 인증 프로세스를 실행하며, 인증서 기반의 인증프로세스는 익명 사용자에 대하여 제한성을 갖는다.

• RSS(Really Simple Syndication) 주입

RSS 주입은 RSS 피드가 악성 코드와 함께 주입되는 공격 유형이다. RSS 독자가 풍부한 콘텐츠를 화면에 표시하고 스크립트를 실행할 수 있다면, 웹 브라우저를 이용하는 것과 같은 문제가 발생된다.

• XML 메시지 주입(XML message injection and manipulation)

공격자는 XML 파서의 끝없는 루프 또는 실패를 유도하는 XML 메시지 또는 첨부 파일의 일부를 수정할 수 있다. 공격자는 또한 서비스 실패를 목적으로 재귀 요소, XPath 식, 그리고 의도되지 않는 처리를 수행하도록 관련 없는 메시지 첨부 파일을 사용할 수 있다. 이러한 공격은 일반적으로 MITM 공격 이후에 따라온다.

• 스케일러브 매시업(Scalable Mashup)

적절한 보안 정책이 순차적으로 구비되지 않은 경우 하나 이상의 소스에서 데이터를 결합하는 "매시업" 또는 웹 응용은 보안 공격에 대한 추가적인 기회를 제공한다. 매시업 애플리케이션들은 종종 임의의 타사 매시업 구성 요소를 허용한다. 만약 악성 사이트가 매시업 사용자가 자신의 매시업 구성 요소를 포함하도록 유도하고, 매시업 응용 프로그램이 충분한 보호를 제공하지 않을 경우에, 사용자와 매시업 응용 웹 사이트는 취약하다.

향후 전망

웹 서비스를 위한 기술은 계속적으로 진화하고 있다는 점은 개발자들에게 많은 어려움을 주고 있으며, 무한 경쟁의 시대를 절실히 느끼도록 하는 요인이 된다. 또한 웹 서비스의 순기능 위주의 개발 및 서비스 전개는 이미 많은 사회적 폐해를 끼치고 있다. 이러한 진화의 단계에서 사이버공간에서의 안전장치를 마련하기 위한 계획적인 접근방법이 필요하다. 폐해에 대한 대응방안으로 어떠한 것이 우선 처리대상이 되는 것을 결정하는 것도 매우 의미 있는 일이 될 것으로 사료된다. 이렇듯 웹 서비스 상에서의 취약점이 무엇인가를 지속적으로 분석하여 추적하는 것 또한 웹 서비스 정보보호를 위한 초석이 된다. ITU-T SG17 Q.7에서는 진화하는 웹 서비스 취약점 및 정보보호 요구사항 관련 표준초안을 개발 중에 있으며, 2012년 2월 회의에서 승인(Consent) 요청을 계획하고 있다.

나재훈 (한국전자통신연구원 사이버융합보안연구단 전문위원, jhnah@etri.re.kr)