情 報 保 護 學 會 誌
第23卷 第3號, 2013. 6

매쉬업 웹 정보보호 표준화 동향

나 재 훈*, 조 현 숙*

요 약

웹 기술은 계속적으로 진화하고 있다. 산업적 측면에서는 이종의 서비스들이 융합하는 것이 손쉬운 방안이 된다. 이러한 서비스들 제공에는 스마트폰의 공급이 매우 지대한 영향을 미치고 있다. 인터넷 서비스는 스마트폰 서비스를 효율적으로 제공하기 위한 진통을 격고 있다. 앱스토어에서 제공되는 앱(Application)서비스의 무차별적인 다운로드는 스마트 인터넷 환경의 위해요소로 존재하고 있다. 매쉬업 기술에 의한 보안 위협을 식별하고, 서비스에 대한 보안 요구 사항 및 기술에 대한 ITU-T SG17에서 진행되고 있는 표준화 동향을 소개한다.

Ⅰ. 서 론

매쉬업이란 용어는 두 개의 다른 곡들에서 성악과 기악 트랙을 혼합하여 탄생되는 새로운 노래의 장르를 이야기 한다. 그것은 대중음악에서 빌려온 용어 이다. 즉 음악에서와 같이 서로 다른 장르에 속하는, 종종 관련이 없는 데이터 소스로부터 소비를 위해 만들어진 콘텐트의 비정상적인 혹은 혁신적인 통합을 의미한다.

웹 기반 데이터 통합 애플리케이션의 새로운 유형은 인터넷을 기반으로 태동된 것이다. 매쉬업 이라는 용어는 제 삼의(Third party) 데이터를 부품과 같이 통합하는 방식으로부터 유래한다. 매쉬업 웹 사이트는 자신의 도메인 외부에 있는 데이터 소스에서 가져온 콘텐트와 기능을 이용하여 그 뿌리를 웹에 확산하는 특징을 갖는다.

ChicagoCrime.org 웹 사이트는 매핑 매쉬업의 아주 좋은 샘플로서, 언론에서 널리 인기를 얻은 사례가 있다. 초기 매쉬업 서비스 중의 하나로, Google 지도와 시카고 경찰 당국의 온라인 데이터베이스의 범죄 데이터를 통합(Mash)하여 정보가 제공되며, 사용자들은 매쉬업 사이트와 상호 연동을 할 수 있다. 개념과 표현이 간단하고, 범죄 데이터와 지도 데이터의 합성은 시각적으로 강력한 효과를 보인다.

매쉬업 서비스는 매핑 매쉬업, 비디오 및 사진 매쉬업, 검색과 쇼핑 매쉬업, 및 뉴스 매쉬업으로 크게 네가지로 분류가 된다[1].

매핑 매쉬업

정보 기술의 시대에 인간은 위치정보를 포함하는 사물과 활동에 관한 거대한 양의 데이터를 수집하고 있다. 위치 데이터를 기반 하는 데이터는 지도를 사용하여 그래픽으로 간단히 표시 된다. 매쉬업의 도래에 대한 가장 큰 촉매제 역할 중 하나는 구글지도 API에 대한 Google의 공개였다. 이것은 웹 개발자가 모든 종류의 데이터를 (핵 참사에서 보스턴의 카우퍼레이드(Cow-Parade)의 소에 이르기까지) 지도에 통합(Mash)할 수 있도록 수문을 열어 준 것이다. 마이크로 소프트 (Virtal Earth), 야후 (Yahoo Maps) 및 AOL (MapQuest)들의 API들도 예외 없이 이어서 그 길을 따랐다.

비디오 및 사진 매쉬업

사진 공유를 가능하게 하는 API를 제공하는 Flickr와 같은 사진 호스팅 또는 소셜네트워킹 사이트의 출현은 다양한 메시업 형태를 주도하게 된다. 콘텐츠는 이미지의 메타데이타를(사진 소유자, 사진 대상, 장소, 시간 등) 가지고 있기 때문에, 매쉬업 디자이너는 다른 정보

본 연구는 미래창조과학부의 지원을 받는 방송통신표준기술력향상사업의 일환으로 수행되었음.
* 한국전자통신연구원 사이버융합보안연구단 (jhnah@etri.re.kr, hscho@etri.re.kr)

와 메타 데이터를 통합(Mash)할 수 있다.

검색과 쇼핑 매쉬업

매쉬업이라는 용어가 나타나기 전에 검색과 쇼핑 매쉬업은 오랫동안 존재해 왔다. 웹 API 탄생이전에 BizRate, PriceGrabber, MySimon과 구글 Froogle과 같은 비교 쇼핑 도구들이 비즈니스-to-비즈니스 (B2B) 기술 정보들이나 비교 가격 데이터를 통합하는 스크린-스크래핑을 조합하여 사용했다. 매쉬업, 기타 흥미로운 웹 애플리케이션과 소비자 시장을(이베이, 아마존과 같은) 촉진하기 위하여 계획적으로 자신들의 콘텐츠를 접속하도록 API를 공개 하였다.

뉴스 매쉬업

다양한 주제에 관련된 뉴스 피드(Feed)를 보급하기 위해 2002 년부터 RSS (Really Simple Syndication)와 Atom 과 같은 신디케이션 기술이 사용되었다. 신디케이션 피드 매쉬업은 사용자의 피드를 종합하고 독자의 특정 관심사를 충족시켜주는 맞춤형 신문을 만들어 웹을 통해 표시한다.

1.1 매쉬업 구조 특징

웹 기술 발전의 주요 특징은 객체지향에서 지나 컴포넌트 기술과 서비스를 기반으로 하는 기술로 천이되었다. 서비스를 기반으로 하는 웹 기술은 SOA(Service Oriented Architecture)의 개념을 중심으로 SOAP(Simple Object Access Protocol) 프로토콜이 주요한 역할을 하였다. 수년 동안 SOA 구조에 기반한 SOAP 프로토콜이 주종을 이루었고, 차세대에 웹 서비스의 인프라를 구축하게 될 기술로 인정되어 왔다. 그러나 오랫동안 관심을 받지 못하였던 ROA (Resource Oriented Architecture) 구조가 스마트폰의 출현으로 매우 각광을 받고 있다. 이러한 방식은 주요 웹 서비스 제공자들(Amarzon, Google, Yahoo, Facebook, Twitter 등)에 의하여 이미 서비스를 제공하기 위한 기본 기술로 자리잡혀있는 상태이다. 즉 매쉬업 서비스가 많이 활성화 되면서 ROA 개념을 중심으로 REST(REpresentational State Transfer) 프로토콜 사용이 추세가 되고 있다. SOAP 프로토콜에 비하여 경량의 구조를 갖고 있어서 스마트폰과 같이 저사양의 디바이스와 다양한 플랫폼이 사용되는 환경에 적합한 것으로 평가되고 있다.

Ⅱ. 차세대 웹 서비스 위협

매쉬업과 같은 기술을 사용하여 융합 서비스를 제공하는 차세대 웹 서비스 환경은 공개주의이다. 이 공개주의는 정보보호 리스크를 발생시킨다. 매쉬업 서비스를 개발할 때에는 정보보호를 반드시 고려하여야 한다. 매쉬업에서 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 [2], 차세대 웹 서비스 환경에서의 위협으로는 다음과 같은 것들이 제시되었다 [3].

악의적 아이프레임 수행(Exploiting malicious iframe)

아이프레임은 HTML의 임베디드 콤포넌트이다. 아이프레임에 숨겨져 있는 안전하지 않는 콘텐츠가 숨겨져 있을 수 있다. 즉 상대주소로 연결되는 홈피를 바로 보여주는(Render) 동작을 사전 검토없이 수행하므로 상대 홈피에 들어있는 악성코드를 여과없이 수행하게 된다.

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 자바스크립로 작성되며 정보교환을 위하여, 배열과 객체의 데이터 구조에 기반을 두고 있으며, 제이슨의 배열은 제이슨 하이잭킹에 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 활용 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 표

시하고 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 따라 온다.

스케일러블 매쉬업(Scalable Mashup)

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

Ⅲ. 정보보호 요구사항

매쉬업 환경에서는 한 서비스에 국한된 취약점이 다수의 도메인으로 증폭되는 문제점이 있다. 그래서 타 도메인의 콤포넌트나 UI와 같은 것을 융합 할 경우에는 사전에 안전성을 검토하여야 한다. 매쉬업 웹 서비스 제공에 있어서 다음과 같은 사항을 사전에 검토하는 것이 필요하다.

전반적 보안 정책 설정 : 정보와 서비스에 대한 안전에 대한 수준을 설정하고, 받아들일 수 있는 리스크의 적정 수준에 대한 정책이 구비하여 서비스 전반적으로 리스크에 대한 체계적 대응이 필요하다.

인증, 인가 계획 수립 : 다수의 도메인에 걸친 서비스에 대한 사용자 접근에 대한 인증 메카니즘이 상호연동을 위하여 일관적으로 인증,인가를 위한 수준 유지가 필요하다.

전송계층과 응용계층 수준의 정보보호 : 전송전달 계층에서 제공되는 기밀성, 무결성등은 종단간 서비스 측면의 기밀성, 무결성 제공에 제한적이므로 응용계층 수준의 메시지 기밀성, 무결성 서비스를 제공이 필요하다.

이러한 전반적인 정보보호 점검사항에 더하여 안전하고 원활한 매쉬업 웹 서비스를 제공하기 위해서 다음과 같은 요구사항을 고려하여야 한다.

액세스 제어 : 권한이 부여된 사용자 또는 장치가 적절한 시스템 자원이나 서비스에 액세스할 수 있는지 확인이 필요하다.

인증 : 이것은 의사 소통 기관의 신원을 확인하기 위해 필요하다. 통신에 참여하는 사용자의 정체성의 유효성을 확인하고 엔티티가 가장 무도회 또는 이전 커뮤니케이션의 무단 재생을 시도가 아니라고 보증을 제공한다. 인증 기술은 액세스 제어의 일부로 필요할 수 있다.

인가 : 인가는 통신 서비스를 안전을 유지함에 있어서 중요하다. 공용 네트워크상에서 가능한 모든 종류의 공격에 대비하여 신뢰할 수 있는 제 삼자의 승인에 기반한 엄격한 인증은 필요하다.

가용성 : 네트워크 요소, 저장되는 정보 흐름, 서비스 및 네트워크에 영향을 미치는 이벤트로 인해 응용 프로그램에 적법한 액세스 권한에 대한 거부가 없다는 것을 보장한다.

통신 보안 : 정보는 권한이 부여된 엔드 포인트 사이에 흐름을 보장한다. 통신 보안은 이러한 엔드 포인트 사이의 흐름 정보가 우회되지 않고 또 가로 채임을 당하지 않았다는 것을 보장한다.

데이터 기밀 :이는, 네트워크 서비스에 의하여 전송, 처리 또는 저장 하는 데이터를 대상으로 비 허가된 접근, 또는 보기에 대하여 보호가 필요하다.

데이터 무결성 : 데이터 무결성은 데이터의 정확성을 보장한다. 데이터에 대하여 허가 받지 않은 공격에 대한 표시를 제공하며, 수정, 삭제, 및 복제에 대하여 보호된다.

효율 보증 : 전송 또는 액세스 작업을 지연하지 않고 실시간 통신 서비스를 효율적으로 적용하기 위해서, 웹 기반 보안 통신 서비스 스킴들은 경량화 되어야 한다.

부인방지 : 개인 또는 엔티티들의 데이터에 대한 특정 작업을 수행함에 대하여 부인을 방지하기 위한 수단

제공이 필요하다.

프라이버시 : 개인이나 단체는 자신과 관련된 정보가 누구에게 수집되고 저장될 수 있는지에 대하여 제어할 수 있는 개개인의 권리를 보장하여야 한다.

안전한 장치의 원격 백업 : 장치가 원격 서버로부터 시스템 형상정보를 안전하게 저장 및 검색을 하는 수단 제공이 필요하다. 이러한 형상정보에는 사용자의 개인정보가 포함될 수 있으므로 안전한 처리가 필요하다.

안전한 사용자 관리 : 익명 사용자의 경우, 통신 서비스의 사용이 공개 개인 정보로 추가적인 등록 절차 없이도 가능 하여야 한다. 그럼에도 불구하고, 정보가 입증되어야 한다.

키 관리 분리 : 웹 기반 통신 서비스로부터 키 관리를 분리하여, 개인키와 관계없이 웹이 통신 서비스를 공유할 수 있도록 하여야 한다.

신뢰 서비스 : 인증 모델에 참여하는 모든 개체는 데이터와 블록 부인을 전송할 수 있다. 따라서 웹 기반 통신 서비스가 제공되어야 한다.

사용자 인증 : 웹 기반 통신 서비스 환경에서 모바일 장치만을 인증이 수행된 경우, 모바일 기기 사용자 인증이 요구된다. 이것은 이동 통신 환경에서 매우 중요한 인증 프로세스로 제안된다.

Ⅳ. 결 론

웹 기술이 표준화 과정 없이 산업기술로 적용되는 진보적 진행을 하고 있다. 개발자들은 자사의 경쟁력을 높이기 위하여 특화된 기술을 제공하고자 표준 협상을 회피하는 사례가 빈번하다. REST 기술의 출현(2000)은 오래되었다. 그동안 SOA 구조의 SOAP 프로토콜의 그늘에 있다가 스마트폰과 매쉬업의 출현으로 프로토콜의 경량화의 추세에 힘입어 각광을 받고 있다.

그러나 산업의 주도로 개발된 기술들은 체계화된 표준 개발을 뒤로 하고 사업성만을 목표로 달려가고 있다. 이러한 점에서 시스템 및 서비스의 상호운용을 위하여 그리고 향후의 기술개발과 상존을 위하여 기초를 마련하여야 한다고 조심스럽게 제언을 한다. ITU-T SG17 Q.7에서는 현재 안전한 매쉬업 서비스 제공을 위한 프레임워크를 위한 국제적 공통표준을 만드는 작업이 진행 중에 있으며 많은 참여를 기대한다.

참고문헌

[1] Mashups: The new breed of Web app http://www.ibm.com/developerworks/xml/library/x-mashups/index.html

[2] ITU-T Recommendation X.1143 (2006), *Security architecture for message security in mobile web services.*

[3] X.Suppl.17: ITU-T X.1143-Supplement on *threats and security objectives for enhanced web-bsed telecommunication services*

〈著者紹介〉

나 재 훈 (Jae Hoon Nah)
정회원

1985년 2월: 중앙대학교 컴퓨터공학과 졸업
1987년 2월: 중앙대학교 컴퓨터공학과 석사
2005년 2월: 한국외국어대학교 전자정보공학과 박사
1987년 ~현재 : 한국전자통신연구원 사이버보안연구단 전문위원/책임연구원
2011년~현대: 한국정보보학회 부회장
2011년~2012년:한국정보보호학회 학회지편집위원장
<관심분야> IPv6/MIPv6, P2P, IPTV, 매쉬업 보안

조 현 숙 (Hyun Sook Cho)
정회원

1979년 2월: 전남대학교 수학교육과 졸업
1989년 2월: 충북대학교 컴퓨터과학과 석사
2001년 2월: 충북대학교 컴퓨터과학과 박사
1982년~현재 : 한국전자통신연구원 사이버보안연구단 단장/책임연구원
<관심분야> 암호학, 보안 프로토콜, 네트워크 보안