情 報 保 護 學 會 誌
第22卷 第2號, 2012. 4

매시업 웹 정보보호 표준화 동향

나 재 훈*, 조 현 숙*

요 약

웹 2.0과 차세대 웹 기반의 서비스 환경에서는 다양한 보안 요구 사항을 가진 이기종 서비스들이 컨버전스 서비스를 제공하기 위해 결합된다. 차세대 웹 기반 애플리케이션은 전통적인 웹 애플리케이션이 갖고 있는 보안 문제 뿐만 아니라, 자신의 특정한 세트의 보안 위협을 갖고 있다. ITU-T SG17에서 진행되고 있는 매시업 기술에 의한 보안 위협을 식별하고, 서비스에 대한 보안 요구 사항 및 기술에 대한 표준화 동향을 소개한다.

Ⅰ. 서 론

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

매시업은 본래 두 개의 다른 곡들에서 성악과 기악 트랙을 혼합하여 탄생되는 새로운 노래이다. 그것은 대중음악에서 빌려온 용어 이다. 즉 음악에서와 같이 서로 다른 장르에 속하는, 종종 관련이 전혀없는 데이터 소스로부터 소비를 위해 만들어진 컨텐츠의 비정상적인 혹은 혁신적인 통합이다.

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

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

1.1 매핑 매시업

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. 매시 업의 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.

1.2 비디오 및 사진 매시업

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, 매시업 디자이너는 다른 정보와 메타 데이터를 통합(Mash)할 수 있다.

본 연구는 방송통신위원회 및 정보통신기술협회의 표준개발지원사업(2012-PK10-008:유무선 환경의 이종 웹 정보보호 표준개발)의 일환으로 수행되었습니다.

* 한국전자통신연구원 사이버융합보안연구단(jhnah@etri.re.kr, hscho@etri.re.kr)

1.3 검색과 쇼핑 매시업

매시업이라는 용어가 나타나기 전에 검색과 쇼핑 매시업은 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. 매시업, 기타 흥미로운 웹 애플리케이션과 소비자 시장을(이베이, 아마존과 같은) 촉진하기 위하여 계획적으로 자신들의 콘텐츠를 접속하도록 API를 공개 하였다.

1.4 뉴스 매시업

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

Ⅱ. 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[2], 차세대 웹 서비스 환경에서의 위협으로는 다음과 같은 것들이 제시되었다[3].

2.1 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.

2.2 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.

2.3 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.

2.4 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.

2.5 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, 프로그

래머는 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.

2.6 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.

2.7 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.

2.8 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.

2.9 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.

2.10 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.

2.11 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.

2.12 스케일러블 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.

Ⅲ. 정보보호 요구사항

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.

〔표 1〕 위협요인과 보안요구사항간의 상관관계

위협요인	보안요구사항	엔티티
Exploiting Silent Transaction	키관리 분리 안전한 사용자관리 안전한 장치의 원격 백업	ISP, Provider, Device
Cross-Site Request Forgery	인증 데이터 기밀성 데이터 무결성 부인방지	User Device, Provider, ISP Provider, ISP User
Cross-Site Scripting (XSS)	안전한 사용자 관리 인증	ISP, Provider User, Device
제이슨 하이제킹	신뢰 서비스 통신보안 인가	ISP ISP ISP, Provider, Device
파손된 자바스크립트 객체 직렬화	인증 무결성 안전한 사용자 관리	User, Device All objects ISP, Provider
스크립트 주입	접근제어 인가	User, ISP ISP, Provider, Device
주입 (Injection Flaws)	신뢰 서비스	ISP, Provider
세션 하이제킹 도용	접근제어 인증	User, ISP User
익명 사용자 위장	사용자 인증 접근제어	User, User, Device
XML 메시지 주입	인증 기밀성 무결성 부인방지	All objects All objects All objects All objects
서비스 거부 (Denial of service)	가용성 액세스 제어 프라이버시 효율 보증	ISP, Provider ISP User All objects
Eavesdropping	데이터 기밀성	All objects
Man in the browser	인증 데이터 기밀성 데이터 무결성	All objects All objects All objects
Man in the middle attack	인증 데이터 기밀성 데이터 무결성	All objects All objects All objects
Masquerade	Mutual-Authentication	User
Modification of message	데이터 기밀성 데이터 무결성	All objects User, Provider
Non-repudiation attack	부인방지 인증	User, Provider User, Device
Replay	부인방지 통신보안	All objects User, ISP, Provider
RSS 주입	인증 기밀성 무결성	User, Device All objects All objects
Scalable Mashups Attack	인증	All objects

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. 위협요인과 보안요구사항간의 상관관계

본 절에서는 매시웹 서비스 환경에서 위협과 요구사항간의 관계성과, 또 네트워크의 객체와의 관련성을 [표 1]에 나타내었다.

Ⅴ. 결 론

웹 서비스를 위한 기술은 계속적으로 진화하고 있다는 점은 개발자들에게 많은 어려움을 주고 있으며, 무한 경쟁의 시대를 절실히 느끼도록 하는 요인이 된다. 또한 웹 서비스의 다양한 기능으로 말미암아 상호 호환이 안되는 문제가 존재한다. 이러한 문제는 각 업체가 자사의 사업성을 높이기 위한 경쟁구도로 진행하고 있어서 서비스들이 화합하지 못하는 이유가 된다. 그러므로 어떤 웹 사이트에서는 제공되는 서비스가 다른 웹 사이트에서는 제공되지 않아서 이용자들에게 혼선을 주는 원인이 되고 있으며, 또한 서비스 공급자들도 웹 브라워저별로 서버 구축을 하여야 하는 문제점도 존재한다. Web2.0의 개방, 참여와 공유의 정신이 기술의 상호배타성으로 인하여 단순 구호에 그치는 우려가 발생하게 된다.

이러한 웹 기술의 발전 단계에서 정보보호 또한 동일한 문제를 갖고 있다. 사용자들의 안전한 서비스를 위하여 계획적인 접근방법이 필요하다. 정보보호에 있어서 어떠한 것이 우선 처리대상이 되는 것을 결정하는 것도 매우 의미 있는 일이 될 것으로 사료되며, ITU-T SG17 Q.7에서는 현재 웹 위협과 보안 요구사항에 대한 국제적 공통표준을 만드는 작업이 진행 중에 있다.

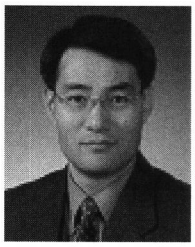
참고문헌

[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] ITU-T draft Recommendation X.1144 (TD2653), *Threats and security requirements for enhanced web based telecommunication service.*

〈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 사이버융합보안연구단 전문위원/책임연구원
<관심분야> IPv6/MIPv6, P2P, IPTV, 웹메시업 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 사이버융합보안연구단 단장/책임연구원
<관심분야> 암호학, 보안 프로토콜, 네트워크 보안