특집 12

웹 2.0과 정보보호기술

목 차

한 정 란
(협성대학교)

1. 서 론

컴퓨팅 환경의 패러다임이 변하면서 인터넷 정보와 서비스는 복잡하고 다양해지고 있고 시공을 초월하여 다양한 네트워크 기기를 통해 정보에 접속하여 정보자산이 유출될 가능성이 높아지고 있다. 클라우드컴퓨팅[1]으로 개인이나 기업의 중요한 정보가 저장된 서버의 공격으로 정보자산이 유출되는 보안 침해 사고의 위험성이 커져 정보 보호의 중요성을 인식하고 있다.

서비스 제공자의 일방적인 정보의 전달이 아닌 사용자의 참여와 개방 및 공유의 특성을 갖는 웹 2.0 환경이 열리면서 개인의 기호나 성향에 따라 맞춤 정보를 제공하는 등의 사용자의 요구사항에 맞게 개인화 서비스를 제공하고 있다. 개인의 다양한 신상정보나 기호나 거래 정보에 따른 맞춤 서비스를 제공하면서 개인 정보의 노출이나 도용의 위험성이 더 커지고 있다. 정보의 홍수 속에 정보를 신속하고 간편하게 생성하고 유통하여 인터넷에서 공유하면서 사이버 테러나 개인 정보가 유출되는 정보 역기능 문제가 야기되어 웹 2.0 환경에서 사이버 범죄나 개인 정보보호가 중요한 이슈가 되고 있다.

2008년 정보보호진흥원의 정보보호실태조사(개인편)에 따르면 정보보호의 중요성을 인식하는 응답자가 98.2%(매우중요 59.9%, 중요한편 38.3%)를 차지했고 개인정보보호의 경우 99.3%(매우 중요 71.8%, 중요한편 27.5%)가 중요하다고 응답해 정보보호의 중요성을 공감하고 있다. 정보보호 관련 최신 정보를 수집하거나 대책을 마련하는 이용자는 30.2%에 불과하고 2007년에 비해 0.6%가 감소하여 중요성은 인식하지만 대책 마련이 미비함을 확인할 수 있다.

많은 기업이 정보보호를 위해 솔루션 기반의 보안인프라의 구현이나 외부보안 전문 업체에 의존하고, 정보 보호를 위한 보안 산업이 투자 대비 ROI 산출이 쉽지 않아 보안인프라 투자가 미비하고 사고 후의 경험으로 보완하고 있는 실정이다.

1) 클라우드 컴퓨팅은 인터넷을 기반으로 전 세계에 존재하는 각종 컴퓨터 자원들을 가상화 기술로 통합하여 언제 어디서나 사용자가 원하는 서비스를 사용할 수 있는 시스템이다. 이용자들이 별도의 소프트웨어를 설치하지 않아도 이용할 수 있고, 웹, PC, 모바일로 연결해 언제 어디서나 온라인에 접속할 수 있다.

웹 2.0 기업 입장에서 비즈니스의 영속성을 보장하기 위해 정보보호를 위한 각종 보안 시스템을 구축하는 것이 필요하다. 본 연구에서는 웹 2.0 환경에서 지능화되고 고도화되는 사이버 테러로부터 정보 자산을 보호하기 위해 보안 문제의 취약성을 분석하고 그 해결방안을 제시하고자 한다. 2장에서는 웹 2.0에서 전반적으로 보안에 유의해야 될 기술을 고려하고 3장에서는 웹 2.0 환경에서 정보 보호를 위해 취약한 부분을 분석한다. 4장에서는 웹 2.0에서 보안 문제를 해결하기 위한 방안을 제시하고 5장에서는 웹 2.0에서 개인 정보보호 기술 현황을 설명하고 6장에서 결론을 기술한다.

2. 웹 2.0과 기술

사용자의 참여와 정보의 공유 및 개방의 특성을 갖는 웹 2.0[2]은 웹을 사용하는 사용자가 웹에 적극적으로 정보와 지식을 생산하고 그것을 다른 사용자들과 공유하고 개방하는 열린 공간의 참여 웹이라 할 수 있다. 기존의 웹을 웹 1.0이라 하는데 사용자가 컨텐츠를 제작하여 수정하거나 제거할 수 없는 서비스인데 반해 웹 2.0에서는 사용자가 원하는 대로 자료를 활용할 수 있고 사용자가 나름대로 컨텐츠나 자료를 생성해서 홈페이지나 블로그에 게시할 수 있다. 블로그를 통해 UCC(user created content)가 등장하고 자연스럽게 사용자의 참여를 유도하는 웹으로 변화하고 있다.

과거 인터넷 사업자가 웹에 정보를 생산하고 관리하던 것과는 달리 사용자가 직접 컨텐츠를 생산하는 UCC와 집단 지성(collective intelligence)을 통해 다양한 컨텐츠를 만들어 내고 있다. 사용자가 만든 컨텐츠가 서비스 업체의 플랫폼을 통해 인터넷을 이용하는 다른 사용자에게 공유되어 기존 웹보다 컨텐츠 제공자가 악의적인 목적으로 악용될 가능성이 높고 검증되지 않은 정보의 공개로 인해 프라이버시를 침해할 수 있다. 특히 웹 2.0 서비스의 경우 Ajax 기술로 자바스크립트의 사용이 많아지면서 정보를 유출하는 보안 위협이 증가하고 있고 공격자가 특정 사이트에 악성코드를 삽입하는 삽입(injection) 공격에 취약성을 드러내고 있다. 소셜 네트워크 서비스[3]의 확산으로 이용자 간에 신뢰관계를 형성하면서 개인정보가 노출되고 연쇄적인 해킹을 초래할 수도 있다.

웹 2.0 사이트의 경우 서비스를 개발할 때부터 정보 보호에 기반을 둔 모델을 설계해야 하고 보안을 고려해 설계해야 서비스를 중단하는 피해를 막을 수 있고 신뢰할 수 있는 안전한 서비스를 제공할 수 있다.

웹 2.0의 적용 기술 중 정보자원이 유출될 위험을 안고 있는 기술들로는 Ajax(Asynchronous JavaScript and XML), RSS, Open API (Application Program Interface), SOAP (Simple Object Access Protocol) 등이 있다.

Ajax는 자바스크립트와 XML을 조합하여 각각의 장점을 살려 풍부하고 세련된 사용자 인터페이스를 가진 인터넷 서비스를 실현할 수 있는 웹 애플리케이션을 개발하기 위한 기술들을 말한다. Ajax는 JavaScript를 기본으로 동적이고 풍부한 화면을 구성하기 위해 여러 기술들을 조합하는 것이다. 웹 2.0 이전에는 서버측 프로그래밍이 중심이 되어 웹 서버로부터 응답을 받아서 웹 페이지를 표시하므로 속도가 느린 단점이 있고 서버로부터 웹 페이지를 받아 웹 서비스 화면이 전환되었는데 Ajax를 사용하여 화면이 전환되지 않는 동적 인터넷 서비스가 가능하다.

RSS는 Really Simple Syndication, Rich Site Summary 혹은 RDF(Resource Description

2) 웹 2.0에 관한 내용은 "웹 2.0 서비스 모델의 특징 및 전망"[1]에서 발췌하여 정리한 것이다.

3) 소셜 네트워크 서비스(social network service)는 커뮤니티형 인터넷 서비스로 회원들 간에 친구를 소개하거나 사이트에서 공통된 목적을 가진 사람들과 만남을 갖는 등의 목적으로 개설된 서비스이다.

Framework) Site Summary의 약칭이다. RSS와 Atom은 웹사이트의 컨텐츠 제목이나 내용 정보를 XML로 정의한 메타 데이터 포맷으로 뉴스나 블로그 등의 업데이트가 자주 일어나는 웹 사이트에서 컨텐츠의 업데이트 정보를 사용자에게 자동적으로 쉽게 전송하는데 사용하고 있다. 사용자는 서로 다른 사이트에 접속하지 않고 RSS 리더기를 통해 새로운 정보를 전송받아 최신 정보를 볼 수 있다.

Open API는 애플리케이션 개발을 위한 인터페이스로 특정 프로그램의 기능을 다른 프로그램에서 활용하여 사용할 수 있도록 표준화된 인터페이스를 공개하는 것이다. 웹 2.0 사이트에서 제공하는 웹 서비스들을 모듈화시킨 API를 공개하고 있고 다른 서비스를 만들 때 활용할 수 있도록 한다. 웹 2.0의 새로운 웹 비즈니스를 시작할 경우 여러 다양한 Open API를 매쉬업[4]하여 새로운 서비스를 만들어 낼 수 있다.

웹 2.0에서는 SOAP과 같은 기술을 사용하여 웹 서비스를 제공한다. SOAP은 메시지 관련 프로토콜로 웹 서비스가 인터넷 상에서 어떤 방식으로 통신해야하는지 규정하고 있다. SOAP은 마이크로소프트사와 IBM사에 의해 빠르게 보급되고 있는 표준으로 클라이언트의 작업 요청과 시스템의 응답을 XML 문자열로 구성하고 전송 프로토콜로 HTTP를 사용한다.

3. 웹 2.0 정보 보호 취약성

웹 2.0은 사용자 중심의 웹으로 많은 장점이 있지만 보안상의 문제점을 안고 있다. 2010년 OWASP(Open Web Application Security Project)[8]의 보안 취약점에서 1위는 삽입(injection)이고 2위는 XSS(Cross-site scripting)이다. 웹 2.0에서 발생할 수 있는 보안 취약점을 삽입과 XSS를 중심으로 분석하고자 한다.

웹 애플리케이션이 외부 시스템이나 운영체제에 접근할 때 입력받은 내용을 그대로 전달하는데 악의적인 명령어를 삽입하여 입력받은 명령어를 실행함으로써 보안상의 문제를 초래할 수 있다. 웹 2.0 환경에서 삽입공격으로 RSS/Atom과 Xpath 및 SQL 질의 삽입 공격 등이 발생할 수 있다. Ajax에서 XSS 공격의 스크립트 삽입과 관련된 취약성이 있고, WSDL(Web Services Definition Language) 스캐닝 문제를 안고 있다.

삽입 공격부터 살펴보면 RSS/Atom 삽입은 악의적인 자바스크립트를 삽입한 RSS 피드가 리드되면서 소프트웨어를 설치하거나 쿠키의 정보를 획득할 수 있다. 특히 피드가 다른 블로그로 이동하면서 웜처럼 퍼져나갈 수 있는 특징이 있다.

웹 2.0 사이트의 경우 XML 기술을 많이 사용하여 Xpath 삽입 공격의 가능성이 높다. Xpath는 XML 문서의 쿼리를 위한 것으로 XML문서 구조를 통해 경로 상에 지정한 구문으로 항목을 배치하거나 처리하는 언어이다. 웹서비스의 SOAP 메시지를 이용해 Xpath 삽입공격을 시도할 수 있다.

웹 애플리케이션은 사용자가 동적으로 SQL 질의를 생성하므로 웹 애플리케이션을 조작하여 SQL 질의를 URL이나 폼 필드에 입력하여 비인가된 사용자가 입력 취약성을 악용하여 DB 정보에 접근할 수 있다.

웹 애플리케이션이 사용자의 브라우저를 공격하는 수단으로 사용되는 XSS는 악의적인 자바스크립트 코드가 사용자의 브라우저에 실행되면서 정보를 유출시키는 것이다. 웹 2.0 사이트의 경우 Ajax를 사용하면서 XSS 백도어 쉘과 같은 공격으로 클라이언트의 정보가 유출될 수 있다. 악의적인 링크를 만들어 사용자가 방문하도록 유도하거나 DOM(Document Object Model)을

4) 매쉬업(Mushup)은 웹 사이트나 웹 애플리케이션을 구축할 때 기존에 만들어진 기술들을 조합하여 구축하는 것으로 개방되어 있는 웹 서비스나 데이터 소스를 조합하여 독자적인 컨텐츠나 서비스를 만드는 방법으로 웹 서비스 API를 통해 구현한다.

조작하거나 쿠키를 제어해 정보를 유출하게 된다. Ajax는 비동기 통신 방식으로 사용자가 모르게 XML HTTP의 Request object를 사용해 클라이언트 콜을 실행하면서 쿠키를 재전송하는데 이를 이용하여 정보를 유출한다. 또한, 클라이언트 코드를 분석하여 공격자가 코드를 수정하거나 비슷하게 작동하는 새로운 애플리케이션을 만들 수 있고, 입력 값 검증 취약점을 지닌 소스코드를 분석하여 조작된 인자를 보내는 애플리케이션을 제작하거나 우회하는 공격을 시도할 수 있다. 웹 서비스를 요청하여 누출되어진 HTML 소스 코드를 통해 Ajax로 처리되는 소스코드를 수집하고 분석하여 웹 2.0 환경의 서버나 Open API를 제공하는 웹서비스 서버에 접근한 후 취약한 서버 페이지를 찾아 악성 코드를 삽입한다. 사용자가 악성코드에 감염된 페이지를 요청할 때 사용자의 아이디와 비밀번호 등의 정보를 자동으로 획득하게 된다.

웹 2.0 환경에서 웹 서비스는 다중 서버에서 운영되고 웹페이지와 정보가 동적으로 생성되어 기존의 솔루션으로 한계가 있다. 웹 방화벽 같은 보안 솔루션이 인터넷상의 모든 서버에 적용될 수 없고 현재의 보안 솔루션이 중간 단계에서 검사하므로 사용자는 위험한 사이트에 노출될 가능성이 높아지고 있다[2]. WSDL은 웹 서비스 기술언어로 XML로 기술한다. 웹 서비스의 구체적 내용을 기술하고 있어 서비스 제공 장소, 서비스 메시지 포맷, 프로토콜 등을 나타내므로 정보가 노출될 경우 큰 문제를 유발할 수 있다. WSDL 파일을 보호하고 제한적으로 접근을 허용해야 한다.

웹 2.0에서 UCC는 동영상 부분이 많이 활용되고 있고 보안 취약성이 감지되는 영역이다. 애플리케이션 취약성에 의한 공격이 중요한 보안 이슈가 되고 동영상 UCC의 대부분이 기존 방송이나 광고 등을 편집하여 저작권 침해가 심각하다. 게시판의 취약성이나 컨텐츠의 업로드/다운로드 과정의 취약성 및 동영상 플레이어 설치를 이용한 시스템이나 DB의 공격이 보안을 위협하고 있다. 그림 파일이나 동영상 파일에 악성코드를 삽입하여 재생하지 않더라도 웹페이지를 열어보는 것으로 감염되는 경우도 있다.

4. 웹 2.0 보안 문제 해결 방안

웹 2.0 환경에서 발생하는 삽입 공격과 XSS의 취약성을 중심으로 보안 취약성 문제를 해결하는 방안을 모색하고자 한다. 삽입 공격의 경우 RSS/Atom과 Xpath 및 SQL 질의 삽입이 있다.

RSS 피드삽입공격[4]을 극복하려면, 악의적인 스크립트나 태그가 삽입된 비정상적인 피드들을 효과적으로 탐지해야 한다. 피드 내부에 스크립트가 삽입되어 있는지 탐지하는 스크립트 탐지 과정을 통해 악의적인 스크립트를 차단한다. HTML 태그 중 정상적인 태그만 삽입되었는지 분류하여 정상 피드일 경우 리더 애플리케이션에 전달된다. 마지막으로 피드 내용중 정상적인 HTML 태그 규칙들과 비교하여 정상피드를 탐지하는 과정이 필요하다.

웹 2.0 사이트의 경우 XML 문서 접근을 위한 Xpath 삽입 공격[5]에는 확인우회와 XML 문서 구조 추출이 포함된다. Xpath 삽입을 차단하기 위해 입력값 검증을 수행하는데 클라이언트와 서버측 모두에서 입력된 값에 대해 검증을 수행한다. Xpath의 조작된 질의에 대해 대응하는 것이 중요한데 사용자의 입력에 대해서 반드시 문자열 필터링을 적용하여 허용가능한 매개변수를 이용하여 Xpath 문장이 만들어질 수 있도록 하여 Xpath 취약성을 극복할 수 있다.

SQL 질의를 URL이나 폼 필드에 입력하여 비인가된 사용자가 입력 취약성을 악용하여 DB 정보에 접근하는 것을 예방해야 한다. 예방 방법은 DB관리자 계정으로 DB에 바로 연결하지 말고 입력 폼으로 사용자의 입력을 받을 때, 사용자의 입력 내용에 대해 특수문자나 예외문자에 대한

사전 처리를 수행하는 것이다. DB에 접근할 수 있는 SQL 질의 문자를 제거하여 DB로의 접근을 통제해야 하고 저장 프로시저를 이용하는 것도 하나의 예방 방법이라 할 수 있다.

XSS는 가장 널리 알려져 있고 치명적인 웹 애플리케이션 보안 문제로 모든 입력데이터의 화이트 리스트 검증 조합과 모든 출력 데이터의 암호화로 방어할 수 있다. 검증은 공격을 탐지하게 하고 암호화는 브라우저에 악의적인 스크립트 삽입을 예방하는데 사용된다. 입력값 검증은 허용 가능한 입력 값의 리스트인 화이트리스트와 허용 불가능한 입력 값의 리스트인 블랙리스트 검증이 있는데 모든 가능한 공격 항목을 명세할 수 없어 대부분의 검증은 화이트리스트방식을 이용한다. 사용자가 입력가능한 문자만 정해놓고 그 문자열이 아닌 경우 모두 필터링하는 방식이다.

XSS의 Ajax 보안 취약점을 고려하여 HTTPS, SSL 같은 암호화 기법을 통한 프로토콜을 이용할 수 있고 웹서비스의 메소드 암호화 기법을 통해 웹서비스를 보호할 수 있다. HTTPS는 데이터를 보호하기 위해 소켓 통신에서 일반 텍스트를 이용하는 대신에, SSL(Secure Socket Layer)이나 TLS(Transport Layer Security) 프로토콜을 통해 세션 데이터를 암호화한다. SSL은 넷스케이프사에서 보안을 위해 개발한 네트워크 레이어의 암호화 방식으로 TLS라는 이름으로 표준화되었고 Authentication, Encryption, Integrity를 보장한다. HTTPS, SSL 같은 암호화 기법의 경우 공격자가 정상적인 사용자인 것처럼 서비스를 요청한 후 응답메시지를 수집하여 메시지를 복호화할 경우 메시지 보호에 대한 보안 프로토콜 문제점이 라는한다. 메소드 암호화 기법[3]은 소스코드가 누출되더라도 사용자로부터 웹서비스를 보호하는 것으로 웹서버의 URL을 관리하는 URL LIST server를 추가하여 서비스 사용자가 정당한 절차로 접근했는지 확인하여 암호화 기법의 취약성을 극복하고 있고, 웹서버에 접속하는 사용자의 웹서비스 메소드 암호화를 통해 소스 코드가 누출되더라도 암호화되어진 값을 통해 사용자 요청에 대한 응답페이지를 작성하여 서버 측 메소드를 보호하게 된다.

웹 2.0에서 웹 서비스의 경우, 개인 정보가 저장되어 있는 클라이언트 웹 브라우저를 통해 웹의 보안 위협을 검사하는 방안으로 로컬 웹 프록시와 네트워크 필터링을 사용할 수 있다[2]. 로컬 웹 프록시는 클라이언트 보안 솔루션에서 주로 사용하는 것으로 클라이언트에 프록시를 설치하여 웹 서버와 클라이언트 사이에서 서버에서 전송된 데이터의 유해한 요소를 검사하는 방법이다. 브라우저가 쿠키를 저장하고 저장된 쿠키로 요청이 이루어져 개인화된 페이지까지 검사할 수 있지만 스크립트에 의해 동적으로 구성되는 웹 페이지를 미리 예측하기 어렵고 느리다는 단점이 있다. 네트워크 필터링의 대표적인 방법은 Socket Hooking 과 network filtering이 있는데 필터링하기 위해 검사할 네트워크 트래픽을 선택하고 HTTP State Inspection을 수행하고 HTML을 추출하여 HTML을 파싱한 후 각 요소를 검사하게 된다[2]. 필터링으로 웹 페이지의 유해성을 검사할 경우 웹 브라우저에서 하는 역할과 중복되어 속도가 느려질 수 있다. 웹 2.0 환경에서 속도 저하 없이 클라이언트 PC를 검사하는 방법으로 웹 브라우저에서 새로운 프로세스가 실행되는 시점에 검사하는 방법이 있다[2]. 실행하려는 프로세스나 바이너리 코드에 악성코드가 있는지 검사하고 실행하여 클라이언트 시스템의 속도 저하를 최소화할 수 있다.

동영상 UCC의 경우 사이트에 등록하기 전에 악성코드 점검 애플리케이션으로 악성 코드가 삽입되었는지 점검하여 사이트에 게시한다. 악성 URL이 삽입된 UCC를 찾기 위해 정보보호진흥원의 악성코드 은닉사이트 탐지시스템

(McFinder)을 사용하여 악성 URL 목록을 얻는다. 게시된 UCC의 동영상을 실행시켜 코드나 삽입된 URL을 추출한 후 악성 URL목록과 비교하여 악성 URL로 판명나면 해당 동영상을 차단하여 악성 UCC 동영상으로부터 피해를 줄일 수 있다.

5. 웹 2.0에서 개인 정보 보호 기술 현황

2008년 정보보호진흥원의 정보보호실태조사의 역기능 유형별 심각성 조사에서 개인정보/프라이버시침해가 96.5%로 가장 높고 스팸(95.8%), 해킹/바이러스(95%), 애드웨어/스파이웨어(92.2%), 불건전한 정보(90.7%), 피싱/파밍(88.9%) 순이었다. 정보보호실태조사를 통해 개인정보나 프라이버시침해 심각성을 인식할 수 있고 개인정보 침해에 대한 관심과 우려가 증가하고 있음을 알 수 있다.

개인 정보 보호 기술은 아직 초보 단계로 기존의 정보 보호 기술을 웹 2.0환경에서 개인 정보 보호 기술에 적용하여 클라이언트 기반의 개인 방화벽, 서버 기반의 방화벽 및 VPN, 클라이언트/서버 기반의 암호화 기반 기술 등을 사용할 수 있고 개인정보보호 기술로는 검색 기술, 개인정보 인증 기술, 홈페이지 개인 정보 노출 검색 및 차단기술, 홈페이지 변조를 통한 스파이웨어 삽입 탐지 기술 등이 진행되고 있다[6]. 웹 2.0을 추진하는 기업에서 기업 내에 저장된 개인 정보 유출을 방지하기 위한 솔루션[5]으로 통합PC 보안 솔루션, 보안 USB 솔루션, DRM 솔루션, DB 보안 솔루션, 네트워크 발신통제 솔루션, 프린트 보안 솔루션, 개인정보 검출/삭제/암호화 솔루션 등이 있다.

통합PC 보안은 내부 직원이 사용하는 PC 단말에 대한 보안 솔루션이다. 보안이 취약한 PC를 통해 기업 내 네트워크를 보호하기 위해 개개인의 PC에 대한 보안을 강화하여 내부 정보의 유출을 방지한다.

보안 USB 솔루션은 일반 USB 대신 보안 USB를 사용하여 사용자 식별 인증, 지정 데이터의 암호화/복호화, 저장된 자료의 복제 방지, 분실시 데이터 보호를 위한 삭제 규정에 따라 보안 USB를 통해서만 정보를 이동하고 정보의 유출을 방지하는 보안 방법이다.

DRM 솔루션은 문서를 암호화하여 보안 문서로 생성한 후 접근 제어, 권한 관리 및 사용 내역에 대한 로깅 기능을 갖는다. 문서가 처음 생성될 때부터 암호화되고 사용 중에도 암호화를 유지하여 문서가 유출되거나 복사되더라도 사용권한이 있는 경우에만 사용가능하도록 하여 정보 유출을 방지한다.

DB 보안은 DB에 저장된 데이터의 유출 방지를 위한 솔루션이다. 서버 관리자나 일반사용자의 DB 접근 권한의 오남용을 방지하고 DB 관리자의 ID나 암호의 도용을 막고 운영체제나 DBMS의 취약점을 노린 해킹도구, 바이러스 등으로부터 데이터 유출을 방지한다.

네트워크 발신통제 솔루션은 기업 내부의 정보가 네트워크를 통해 유출되는 것을 방지하기 위해 각종 인터넷 기기 사용을 감시하여 내부자에 의한 정보 유출을 방지하고 보안 업무를 유지한다.

프린트 보안 솔루션은 기업 내부의 출력시스템을 원격으로 통제하고 관리 감독하는 것으로 출력되는 모든 내용에 대해 로깅을 남기고 모든 출력 시스템을 중앙에서 통제하여 정보 유출을 방지한다.

개인정보 검출/삭제/암호화는 기업의 업무상 개개인의 PC에 흩어진 개인 정보 파일을 검출하여 중앙서버에서 통제하는 솔루션으로 개인정보 파일을 삭제하거나 암호화하여 개인 정보 유출을 방지한다.

기존 솔루션들의 경우 자신이 보안할 수 있는

5) 개인정보보호 솔루션은 "개인정보보호 기술의 현황 및 전망"[6]에서 발췌하여 정리한 것이다.

영역을 벗어나 우회경로를 통한 정보 유출이 가능하고 내용 검사를 기반으로 자료를 통제하지 않고 각종 매체를 차단하거나 문서의 암호화로 정보 유출을 막아 중요하지 않은 정보까지 자유롭게 활용하지 못하는 경우가 생길 수 있다.

웹 2.0 기업의 경우 지능화되고 고도화되는 사이버 테러로부터 정보자산을 보호하기 위해 전반적인 계획 없이 위에 열거한 각종 보안 솔루션을 낱개로 구입하는 것은 효율적인 방법이 아니다. 체계적이고 세부적인 통제 항목을 통해 전체적인 정보 보호 활동을 위한 전사적인 정보보호 정책[6][7]을 수립하고 기업의 정보 자산을 효율적으로 통제하고 운영하는 구조화된 보안 프레임워크가 필요하다.

6. 결 론

비즈니스 측면에서 웹 2.0은 새로운 사업 기회와 새 시장을 열어주고 있다. Open API와 공개된 자료를 활용하여 다양한 애플리케이션을 만들고 있지만 공유하고 개방된 정보자원에 대한 노출이 프라이버시나 개인정보를 침해하는 심각한 문제를 초래할 수 있다.

본 연구에서는 웹 2.0 환경에서 지능화되고 고도화되는 사이버 테러로부터 정보 자산을 보호하기 위해 정보보호 기술들과 보안 취약성을 분석하였다. 삽입 취약성으로는 RSS/Atom과 Xpath 및 SQL 질의 삽입(injection) 공격 등이 발생할 수 있고 Ajax기술에서 XSS의 스크립트 삽입과 관련된 취약성을 분석하였고 보안 취약성의 문제점을 해결하는 방안들을 제시하였다.

기업입장에서 사내 정보 유출을 방지하기 위해 개인정보보호를 위한 기술 현황들을 살펴보았다. 대부분의 기업의 경우 정보보호 시스템과 네트워크 보안에 주안점을 두고 해당 조직의 규제 방안을 모색하지 않고 있고 자율 규제 방안은 국가기관이나 정보보호 단체에서 권고안으로 제시한 내용만을 받아들이고 있다. 따라서 효과적인 개인정보보호를 위해 개별적인 솔루션을 구입하는 것보다 전체적인 보안 계획 하에 통합 관리할 수 있는 전사적인 보안 솔루션을 위한 프레임워크를 개발할 필요성이 제기된다.

개인 정보나 저작물들이 개인의 통제권을 벗어나 남용될 여지가 많아 이를 보호해줄 메커니즘이 필요하고 자신의 통제권을 강화할 수 있는 세심한 기술을 개발해야 한다. 정보보호와 개인 프라이버시를 보장할 수 있는 정책이나 제도를 수립하기 위한 개인의 태도나 성향에 대한 연구와 체계적이고 계획적인 정보보호 관련 연구의 활성화를 통해, 정보보호에 대한 사회적인 합의 수준을 파악할 수 있고, 그 성향을 토대로 보다 현실적이고 구체적인 국가 정보보호 정책을 수립하는데 기여할 수 있을 것이라 전망한다.

참고문헌

[1] 한정란,웹 2.0 서비스 모델의 특징 및 전망, 정보처리학회지 2007, 7월호.

[2] 이창우외 2인, 웹 2.0 환경에서의 보안 문제와 효율적인 웹 검사 방안, 정보보호학회지, 제18권 3호, 2008.

[3] 김진보, Ajax 통신에서 메소드 암호화를 통한 웹서비스 보안 모델 연구, 석사학위논문, 목포대학교, 2007.

[4] 양형초,RSS 및 Atom 피드 삽입 취약점을 이용하는 비정상행위 탐지, 석사학위논문, 전남대학교.

[5] 이나영, 웹 2.0에서 Xpath Injection의 취약성 분석에 대한 연구, 석사학위논문, 성균관대학교, 2007.

6) 전사적인 정보보호 정책은 정보보호 관련 공통 요소를 모두 포함하고 정보보호 정책을 수립하기 위해 현재 소유하고 있는 정보 자산을 확인하고 해당 정보자산에 대해 대내외적인 위협과 취약점을 인식하여 이를 보호하고 완화하기 위한 구체적인 방법론이다.

[6] 김상진, 개인정보보호 기술의 현황 및 전망, 정보과학회지, 2009. 12
[7] 박종락, 보안 위협요소 분석 및 정보보호 프레임워크 제시를 위한 연구, 아주대학교 석사학위논문, 2009
[8] http://www.owasp.org/images/0/0f/OWA SP__T10__-__2010__rc1.pdf

저자약력

한 정 란

이화여자대학교 전자계산학과 졸업
이화여자대학교 대학원 졸업(석사) 프로그래밍 언어론 전공
이화여자대학교 대학원 졸업(박사) 프로그래밍 언어론 전공
1999년~현재 협성대학교 경영정보학과 부교수
관심분야 : 전자상거래, e-CRM, XML, 웹서비스, 웹 2.0 등
이 메 일 : jlhan@uhs.ac.kr