주문형 보안 결함 탐지 서버 (Security On Demand) 프로토타입 개발

천왕성, 정종윤, 백석철.
한국통신 멀티미디어연구소 네트웍보안연구팀.
서울시 서초구 우면동 17 한국통신 연구개발본부 멀티미디어연구소
인터넷연구실 네트웍보안연구팀.

Developing the Prototype of Security-Hole Scanning Server on Demand (Security On Demand)

Wang-sung Chun, Jong-yun Jung, Seok-chul Baek.
Korea Telecom Multimedia Lab. Network Security Research Team.
Network Security Research Team, Internet Research Dep., Multimedia Lab,
Korea Telecom R&D Center, 17, Umyun dong, Seocho Gu, Seoul.

요약

최근에 시스템의 불법적인 침입, 정보 유출등의 보안 사고가 많아지면서 컴퓨터 보안을 위한 많은 방법들이 제시되고 있다. 그 중에서도 컴퓨터 시스템 자체에 존재하는 보안상의 결함을 막기 위한 노력들이 있어왔다. 그러나 시스템의 보안 결함은 기본적으로 운영체제나 어플리케이션 자체의 버그에 기인하므로 끊임없이 출현하는 실정이다. 따라서, 시스템 관리자가 이를 일일이 확인하여 보안 결함을 체크하고 대응하는 것은 상당히 힘든 일일 것이다. 본 논문에서는 HTTP 프로토콜을 이용하여 클라이언트 시스템의 보안 결함을 원격으로 점검해 주는 주문형 보안 결함 탐지 서버(Security On Demand)에 대해 설명한다. 주문형 보안 결함 탐지 서버(이하 SOD 서버)는 서버-클라이언트 모델로서 클라이언트가 원하면 보안 결함을 탐지하는 코드를 전송하여 클라이언트측에서 실행되도록 한다. 그러므로 SOD 서버 측에만 새로이 출현한 보안 결함 탐지코드를 추가하면 클라이언트는 최신의 보안 결함에 대한 점검이 가능하다. 또한 코드 자체가 클라이언트로 전송되어 수행되기 때문에 클라이언트측의 보안 결함 정보가 서버로 유출되지 않는 장점이 있다.

I. 서론

인터넷의 대중화와 정보에 대한 의존도 증가는 컴퓨터 시스템의 불법적인 침입을 통한 정보 유출, 시스템 파괴등의 범죄 증가를 초래했다. 이러한 해킹 범죄로부터 시스템을 보호하기 위해 방화벽, 패킷 암호화, 보안 결함 제거, 침입 감지 기술등 많은 노력들이 기울여져 왔다. 이 중 시스템의 보안상의 결

함을 제거하여 계정이 없는 외부 사용자의 침입 혹은 내부 사용자의 불법적인 권한 획득을 불가능하게 하는 보안 결함 제거는 시스템과 정보를 보호하는데 매우 중요하다.

그러나 시스템의 보안 결함은 끊임없이 발견되고, 또한 이를 막기위한 방법들이 제시되고 있기 때문에 시스템 보안 관리자는 발표되는 보안 결함 정보를 빨리 알아내 이에 대한 대처를 해야 한다. 그러나, 무수히 많은 보안 관련 단체와 정보 교류를 행한다는 것은 그 업무가 과다하여 실질적으로 불가능한 일이다.

최근들어 이러한 관리자의 편리를 위해 시스템의 보안 결함을 점검해주는 다양한 도구들이 개발되고 있다. 이러한 보안 결함 탐지 도구는 크게 자신의 시스템에 설치한 후 자신의 시스템의 이상이나 결함을 점검하는 방식과 외부에서 자신의 시스템의 이상이나 결함을 점검해 주는 방식으로 구분될 수 있다. 전자를 Local 형이라고 하고, 후자를 Remote 형이라고 할 때, 지금까지 개발된 보안 결함 탐지 도구들은 다음과 같이 특징지을 수 있다.

- Local 형
  1. 자체적인 DB 나 설정파일등을 가지고 있을 수 있기 때문에 보다 다양한 기능이 가능하며 또한, 자신의 시스템에 맞게 설정을 조정할 수 있다.
  2. 자신의 시스템에서 실행되므로 점검 결과등이 외부로 유출되지 않는다.
  3. 끊임없이 발견되는 보안 결함에 신속히 대응하기 어렵다.
  4. 소프트웨어를 설치, 관리해야하는 부담이 있다.
  5. 예) SHE, Cops, tiger, tripwire 등
- Remote 형
  1. 항상 최신의 보안 결함에 대한 점검이 가능하다.
  2. 사용자가 보안 결함 점검을 하는데 있어서 설치, 관리등의 부담이 적다.
  3. 네트웍을 통한 외부로부터의 점검이므로 여러가지 요인으로 인한 한계를 갖는다.
  4. 서버가 자신의 시스템을 점검한 결과를 알게 되므로 자신의 시스템의 보안 결함 정보가 유출될 위험이 있다.
  5. 예) Satan, iss 등

Local 형이나 Remote 형 모두 위와같이 각각의 장단점을 가지고 있다.

본 논문에서는 이러한 보안 결함 정보를 모아 시스템 관리자들이 쉽게 자신의 시스템의 보안 결함을 점검할 수 있도록 원격 보안 결함 서비스(Security On Demand : SOD)의 프로토타입을 소개한다. SOD 서버는 기본적으로 Remote 형이지만 코드가 전송되어 클라이언트의 시스템에서 실행되어 결과를 보여주기 때문에 클라이언트의 보안 결함 정보를 서버는 알 수 없다. 또한, 웹 서비스를 기반으로 하는 사용자 주문형 서비스이기 때문에 방화벽등의 장애를 받지 않는다.

SOD 에서는 사용자의 요구에 의해 보안 결함을 점검하는 Perl 코드가 HTTP 프로토콜을 통해 사용자의 시스템으로 전달되어 수행되고 보안 결함 점검 결과를 웹 브라우저를 통해 보여준다. 시스템 관리자만이 SOD 서비스를 이용할 수 있으며 점검 결과가 인터넷을 통해 전달되지 않기 때문에 보안상의 문제는 없으며, 웹 방식의 서비스를 제공하기 때문에 이용하기도 편리하다.

II. 본론

1. SOD 서비스의 개념 및 필요성

보안 결함은 주로 운영체제나 어플리케이션 자체의 버그나 결함에 근원한다. 운영체제나 어플리케이션은 계속해서 더욱 많은 기능을 가지고 새로이 배포되거나 revision 되고 있기 때문에 보안 결함도 꾸준히 발견될 수 밖에 없다. 실제로 Solaris, HP-Unix, Unicos, DEC, AIX 등 대부분의 유닉스 운영체제와 그에 따른 어플리케이션 패키지들은 버그나 결함이 발견될 때마다 그에 대한 패치를 배포하고 있는 실정이다. 이러한 버그나 결함은 대부분 보안상의 헛점에 관련된 것이 많아 시스템 관리자들은 이러한 배포 상황을 예의 주시하고 있다가 신속히 패치해야 한다. 더구나, 대부분의 해킹 사건들은 보안 결함이 발견된지 1~2 주일 안에 집중적으로 발생하는 경향이 있기 때문에, 운영체제 Vendor 들의 패치가 배포되기 전에 각종 보안 관련 인터넷 사이트로부터 정보를 구해 임시 대응책을 구해야 한다. 이러한 일들은 관리자가 수행하기에는 너무 많기 때문에, 이러한 일을 대신해 주는 서버가 필요하게 된다.

원격 보안 탐지 서비스인 Security On Demand(SOD) 서비스는 이러한 보안 결함 정보들을 모아 이를 원격 탐지해주는 서비스이다. 서버 관리자는 각종 보안 결함에 관한 정보를 모니터링하다가 새로운 보안 결함이 발견되면 즉시 이에 대한 탐지 코드 모듈을 만들어 항상 최신의 보안 결함 탐지 서비스가 되도록 유지한다. 반면에 서비스 가입자는 많은 보안 관련 사이트들을 방문할 필요 없이 SOD 서버에 접속하여 자신의 시스템의 보안 결함을 쉽게 점검할 수 있다. 특별한 클라이언트 프로그램은 필요하지 않고, 단순히 웹 브라우저와 Perl 만 설치되어 있으면 되고, 또한 시스템의 Root 권한을 가져야 한다.

2. SOD 서비스의 전체 구조 및 시나리오

SOD 서비스는 기본적으로 웹의 MINE type 어플리케이션 Helper 를 이용한 클라이언트/서버 모델이다. 즉, 서버가 클라이언트의 요구에 따라 클라이언트의 웹브라우저에 보안 결함 점검 코드를 보내주면, 웹브라우저가 Perl 을 구동하여 서버로 받은 보안 결함 점검 코드를 실행하게 된다.

SOD 서비스의 전체 구조는 그림 1 과 같이 클라이언트측에는 웹브라우저와 Perl 이 설치되어있고 서버측은 클라이언트의 HTTP Request 를 처리할 수 있는 웹서버 밑에 클라이언트의 요청에 따라 클라이언트의 보안 결함을 점검할 코드를 생성하는 부분으로 구성되어 있다. 이러한 구조하에 그림 2 와 같은 시나리오로 클라이언트에게 보안 결함 점검 코드가 전송되어 클라이언트측에서 실행되고 결과를 보여준다.

SOD 서비스의 시나리오는 다음과 같다.

a) 클라이언트측의 웹 브라우저에서 SOD 서버의 웹 서버에게 index.html (SOD 홈페이지)을 요구한다.

b) SOD 서버의 웹 서버는 index.html 을 웹 브라우저에게 보내준다.

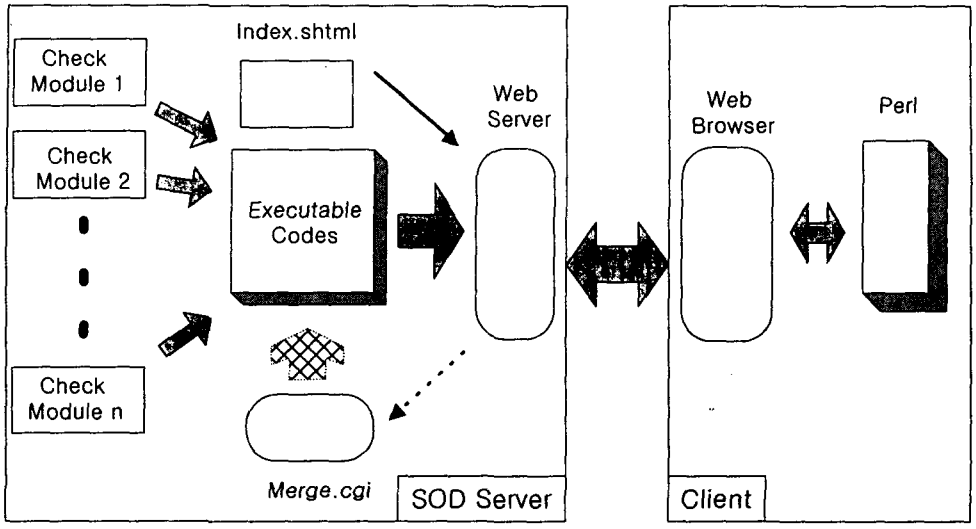

그림 1. SOD 서비스 전체 개념도

c) 클라이언트에서 원하는 보안 결함 점검 사항을 SOD 서버에게 보낸다.
d) 웹 서버는 클라이언트로부터의 주문사항을 인수로 하여 Merge.cgi 프로그램을 수행시킨다.
e) Merge.cgi 는 보안 결함 탐지 모듈중에서 클라이언트가 원하는 모듈을 모아 하나의 실행 가능한 Perl 코드를 생성한다.
f) 웹서버는 Merge.cgi 가 생성한 Perl 코드를 클라이언트측의 웹 브라우저에게 보낸다.
g) 웹 브라우저는 SOD 서버로부터 받은 Perl 코드를 클라이언트에 설치되어 있는 Perl 을 이용하여 실행시킨다.
h) Perl 코드가 모두 수행되면 결과를 HTML 문서로 작성하여 웹 브라우저를 통해 보여준다.

3. SOD 서비스의 설계 및 구현

3.1 웹 서버

웹 서버는 보안 기능이 좋은 Apache 1.1.1 을 이용하여 구성하였다. 여기에 사용자 인증 기능을 강화하고 클라이언트와 서버간의 패킷을 암호화하기 위해 SSLeay 를 기반으로 한 Apache-SSL 을 보안 결함 탐지 코드를 전송하고, 사용자 ID 와 패스워드등을 주고 받는데 이용하였다.

Apache-SSL 을 이용함으로써, 웹서버의 기본 인증 기능과 SSL 프로토콜의 인증서 확인 기능의 이중 인증 과정을 거쳐 보안 결함 탐지 코드의 오용을 막도록 노력하였다. 인증서는 한국통신 인증서 발급 서버(KTCAS)로 부터 발급 받은 인증서를 확인하도록 하였다. [6],[7]

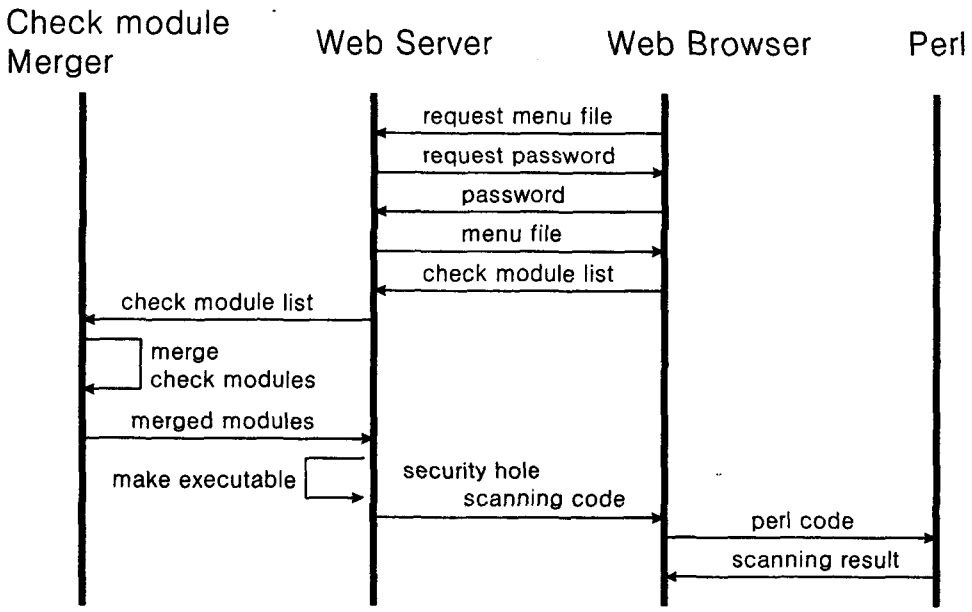

그림 2. SOD 서비스 시나리오

따라서, SOD 서비스를 받기 위해서는 한국통신 인증서 발급 서버(KTCAS)로부터 인증서를 우선 발급받아야 하고, SOD 서비스에 가입하여 User ID 와 패스워드를 발급받아야 한다.

3.2 사용자 정보 관리

SOD 서비스의 사용자 정보 관리를 위해 MySQL 을 이용하였다. 사용자 정보에는 일반적인 사항외에도 다음과 같은 정보가 포함된다.

- **User ID, Password, IP address** : 보안 결함 탐지 코드의 불법적인 악용을 막기위한 인증절차를 위한 정보.
- **Netscape Path, Perl Path, OS** : 보안 결함 탐지 코드가 클라이언트의 시스템에서 실행되도록 하기위해 필요한 정보.
- 각 보안 결함 탐지 모듈별 최근 탐지일 : 각 사용자가 언제 어떤 모듈에 대해 보안 결함을 실시하였는가에 대한 자료로서 사용자에게 아직 점검하지 않았거나 새로 갱신된 모듈만을 전송 받아 점검하도록 권장하기 위한 자료이다. 이는 코드 전송량을 최소화해 불필요한 트래픽을 줄이기 위함이다.

3.3 index.shtml

사용자에게 보안 결함 탐지 모듈의 메뉴를 제시하고 점검하도록 선택한 항목을 merge.cgi 에

게 인수로 넘겨주는 파일이다. 여기서 제시하는 12 개의 보안 결함 탐지 모듈은 4 절에서 자세히 설명한다.

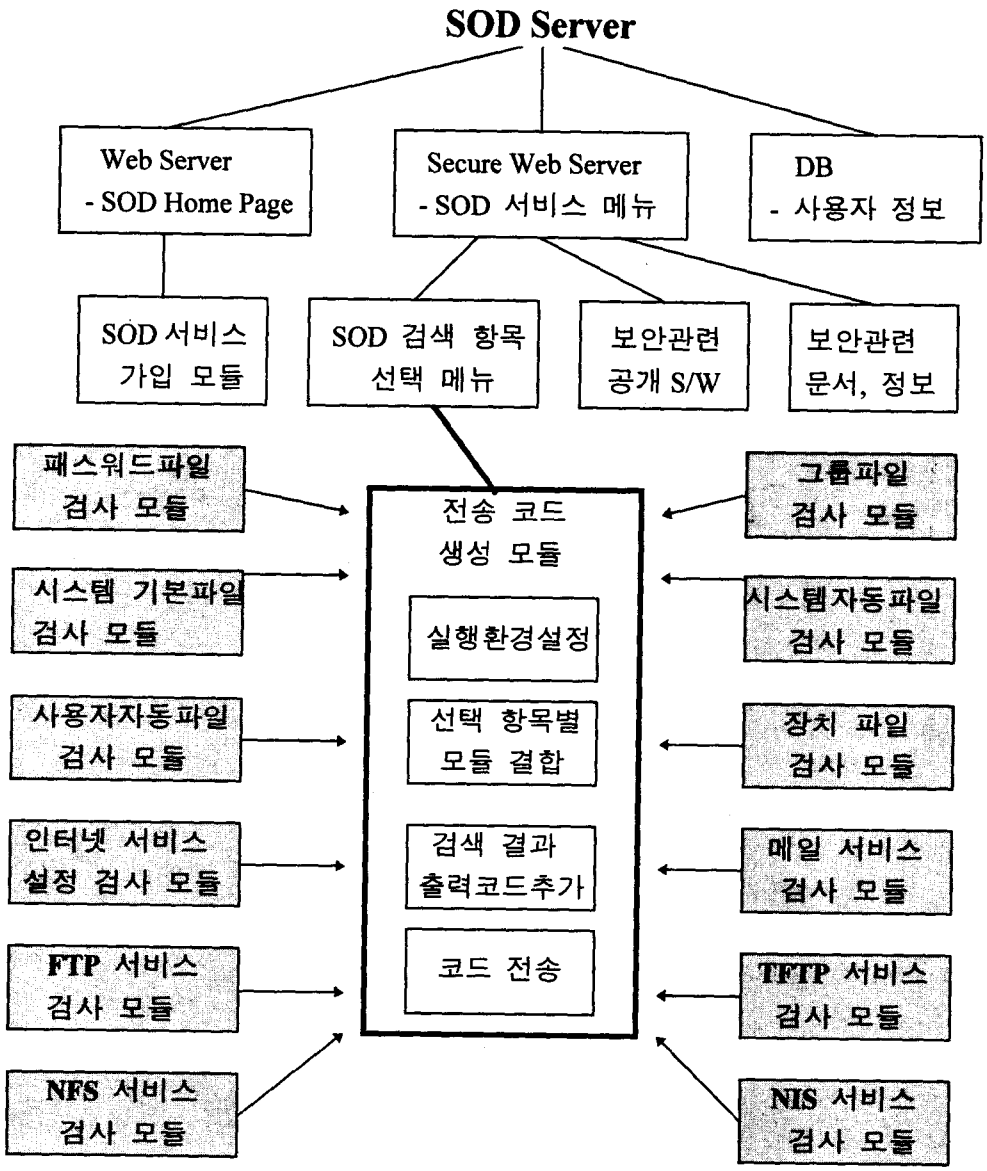

그림 3. SOD 서버 구성도

3.4 전송 코드 생성 모듈 (merge.cgi)

전송 코드 생성 모듈은 그림 3 과 같이 선택 메뉴로부터 받은 선택된 보안 결함 탐지 항목에 해당하는 모듈들을 합치고 클라이언트의 시스템 정보등을 이용하여 클라이언트의 시스템에서

실행될 수 있는 코드를 생성하는 모듈이다. 우선 Netscape, Perl 등의 경로와 OS 버젼등을 설정하고 선택된 모듈들을 합친 후 보안 결함 점검 결과를 출력하는 모듈을 추가하여 웹서버를 통해 클라이언트에게 전송한다.

3.5 클라이언트

클라이언트측에서는 Perl 과 웹 브라우저 이외의 특별한 소프트웨어는 필요로 하지 않는다. 단지, 웹 브라우저에서 MINE type 'application/x-perl' 의 Helper 로서 자신의 시스템의 Perl 실행 파일의 경로를 지정해 주는 것으로 족하다. 그리고 Perl 은 버젼 5.003 이상을 권장한다.

4. SOD 서버의 보안 결함 탐지 모듈

II-1 절에서 언급한 바와 같이 보안 결함은 계속해서 발견될 뿐만 아니라, 그 종류 또한 다양하다. 따라서 SOD 서비스에서는 여러가지 다양한 보안 결함을 체계적으로 분류하여 적절한 수준으로 모듈화하였다. 다음은 프로토타입 단계의 SOD 에서 제공하는 보안 결함 탐지 모듈이다.

- 패스워드 파일 검사 : /etc/passwd 파일의 비정상적인 설정 상태등을 점검한다.
- 그룹 파일 검사 : /etc/group 파일의 비정상적인 설정 상태등을 점검한다.
- 시스템 기본 실행 파일 검사 : 운영체제에서 기본적으로 제공해주는 실행 파일들 중 해킹의 가능성이나 사례가 있는 파일들의 보안 상태등을 점검해 준다.
- 시스템 자동 수행 파일 검사 : 시스템이 부팅될 때 자동적으로 실행되는 파일등은 관리자의 주의가 소홀하기 쉽다. 이러한 파일들의 설정 상태등을 점검한다.
- 사용자 자동 수행 파일 검사 : 사용자가 로긴할 때 자동적으로 실행되는 파일들은 사용자의 주의가 소홀하기 쉽다. 이러한 파일들의 설정 상태등을 점검한다.
- 시스템 장치 파일 검사 : 시스템마다 다양한 주변장치를 가지고 있다. 이러한 주변장치들은 파일처럼 관리되고 있는데 이 파일들에 대한 보안상의 점검을 수행한다.
- 네트웍 서비스 설정 파일 검사 : 대부분의 네트웍 서비스는 inetd 을 통해서 제공된다. inetd 의 설정파일에 존재하는 보안 결함등을 점검한다.
- 메일 서비스 검사 : 메일 서비스는 거의 모든 시스템이 제공하면서도 꾸준히 보안 결함이 발견되어 왔다. 이 검사는 메일 서비스에 관한 모든 보안 결함을 점검한다.
- FTP 서비스 검사 : 대부분의 시스템이 제공하는 FTP 와 익명 FTP 의 설정 상태등을 점검한다.
- TFTP 서비스 검사 : 하나의 호스트에 여러개의 X-터미널을 연결할 때, 혹은 디스크가 없는 호스트를 위해 제공하는 서비스로 보안상의 결함이 매우 많다. 이 서비스의 설정상태를 점검한다.
- NFS 서비스 검사 : 디스크를 다른 시스템에서 공유하도록 하는 서비스로 보안상의 결함이 많이 존재한다. 이에 대한 점검을 실시한다.
- NIS 서비스 검사 : 패스워드등 사용자 정보등을 NIS 클라이언트에게 제공해주는 서비스로

보안상의 결함이 많이 존재한다. 이에 대한 점검을 실시한다.

이외에도 많은 보안 결함이 있지만 이에 대한 탐지 기능을 추후 추가할 예정이다. 이러한 추가될 보안 결함 탐지 기능은 위의 모듈에 추가될 수도 있고, 또한 새로운 모듈로서 추가될 수도 있다. 이에 대한 선택은 SOD 서버 관리자가 코드의 분량, 보안 결함의 성격등을 고려하여 결정한다.

5. SOD 서비스의 특징

SOD 서비스는 시스템 관리자가 주의를 기울이기 힘든 보안 결함 정보를 한데 모아 원격으로 결함을 탐지하여 주므로 시스템 관리가 훨씬 쉬워질 뿐만 아니라 시스템의 보안 결함도 거의 제거 할 수 있다. 이밖에도 다음과 같은 특징을 들 수 있다.

- 고객 주문형 검색 항목

  이미 검색한 항목에 대한 불필요한 검색을 막아 네트웍 트래픽과 검색 시간을 줄이기 위해 보안 결함의 성격에 따라 그림 2 SOD 서버 구성도 에 표시된 12 개 항목으로 분류하여 선택적인 결함 검색 요청(일명, 주문형 결함 검색)이 가능하다.

- 내부 + 네트웍 보안 결함 탐지 기능

  한편, SATAN, ISS 와 이를 바탕으로 한 다른 원격 보안 결함 서버들은 외부에서 포트 검사 등을 이용하여 타겟 시스템의 보안 결함을 조사하기 때문에 네트웍 관련된 보안 결함 만을 탐지할 수 있다. 그러나 SOD서버는 보안 결함 탐지 모듈을 직접 클라이언트 시스템 내부로 전송시킨 후, 타겟 시스템 내부에서 작동시키기 때문에 네트웍 보안 결함 뿐만이 아니라 내부 보안 결함도 탐지할 수 있는 장점을 갖고 있다.

- 시스템의 보안 결함 유출 방지 및 실시간 보안 결함 보고

  SATAN, ISS 와 이를 바탕으로 한 다른 원격 보안 결함 서버들은 외부에서 포트 검사 등을 이용하여 타겟 시스템의 보안 결함을 조사한 후, 이를 다시 전자 메일로 타겟 시스템에 보내는 방식을 취하고 있다. 그러므로 이러한 방식에는 결정적으로 다음 세 가지 보안상 문제가 있다. 첫번째 문제는 고객의 시스템에 있는 보안 결함이 원격 보안 결함 탐지 서비스를 제공해주는 기관이나 업자에게 모두 공개된다는 사실이다. 그러므로 이러한 정보가 악용될 수 있는 소지를 남기게 된다. 두번째 문제는 실시간으로 보안 결함을 보고 받을 수 없다는 점이 있어 신속한 보안 결함에 대한 대책을 마련하기 힘들다. 끝으로 이러한 고객의 보안 정보가 전자 메일로 갈 경우 패킷 스니퍼링 등에 의하여 해킹될 수 있는 보안상의 문제점이 있다. 그러므로 이를 극복하기 위해서 PGP 등을 사용하는 번거로움이 발생한다. 반면에 본 SOD 서비스는 고객의 시스템의 보안 결함이 실시간으로 고객 시스템의 웹 부라우저에 표시되기만 하지 서버 쪽으로는 어떠한 보안 결함 정보도 보내지지 않게 되어 있어 훨씬 안전한 서비스라고 할 수 있다.

- SOD 서버와 클라이언트 간의 통신 방식

  SOD 서버는 SSL 이 장착된 Secure Web Server 를 사용한다. 그러므로 클라이언트 시스템이 웹 부라우저를 이용하여 SOD서버에 연결을 할 때, SSL 프로토콜을 이용하게 된다. 때문에 보안 결함

탐지 프로그램 전송 시, 혹 발생할지 모르는 검색 코드 유출을 방지할 수 있다.

- CA 서버가 발급하는 인증서를 이용한 최신의 인증 방식

기본 웹 서버 패스워드 인증 방식 이외에 한국통신에서 자체 개발한 CA 서버가 발급한 인증서를 통한 웹 브라우저의 인증을 추가하여 불법적인 SOD 서비스 이용을 방지할 수 있다. 또한, 불법 SOD 서버의 출현을 원천 봉쇄하기 위하여 SOD 서버도 웹 부라우저에 인증서를 발급한 CA 서버로부터 인증서를 발급 받는다.

- 새로운 보안 결함 검색 모듈의 신속한 제공

SOD 서버의 핵심 기능이라고 할 수 있는 최신의 보안 결함 검사 모듈을 서비스하기 위하여 SOD 서버 관리자는 단지 새로운 검색 모듈만 SOD 서버에 지속적으로 추가 하기만 하면 된다. 이러한 점은 기존의 보안 결함 탐지 도구의 사후 서비스(after service)에 비하여 훨씬 개선된 방법이라고 할 수 있다. 그리고 SOD 서버는 각 클라이언트 시스템이 SOD 서버를 이용한 정보들을 지속적으로 관리하여 아직 검색하지 않았거나 새로이 검색해야 할 필요가 있는 항목들을 기존의 모듈과 차별화되도록 표시하여 사용자가 쉽게 아직 수행시키지 모듈들을 쉽게 이용할 수 있게 했다.

- 방화벽이 보안 결함 탐지 서비스의 장애가 되지 않는다.

기존의 ISS, SATAN 및 이를 응용한 기존의 원격 보안 결함 탐지 서버들은 외부에서 포트 검사 등을 이용하여 검사를 받고자 하는 타겟 시스템들의 네트웍 보안 결함을 탐지하기 때문에 방화벽 안에서 보호 받고 있는 시스템들에 대해서는 서비스를 제공할 수 없다. 그러나 SOD 서비스는 보통의 웹 서버 포트인 80 번을 이용하고 있기 때문에 SOD 서버로부터 보안 결함 검사 모듈이 방화벽을 통과하여 검사 받고자 하는 클라이언트 시스템의 웹 부라우저로 전송되는데 방화벽이 방해 요소가 될 수 없다. 왜냐하면 대부분의 방화벽들은 내부 망에 있는 시스템들이 웹 부라우저로 인터넷 상에 있는 정보들을 검색하는 것을 기본적으로 허용하기 때문이다. 그러므로 다수의 방화벽을 설치한 큰 규모의 망이나 KORNET 과 같은 ISP 들이 단 하나의 SOD 서버를 설치하여 새로운 보안 결함 탐지 서비스를 제공하는 것을 가능케 한다.

- 추가의 클라이언트 프로그램이 필요하지 않는다.

추가의 클라이언트 프로그램을 설치할 필요없이 흔히 사용되는 Perl 과 웹브라우저만을 이용하므로 웹브라우저를 이용하여 간단히 SOD 서버에 접속하는 것만으로 자신의 시스템의 보안 결함을 점검할 수 있다.

- 사용자 인터페이스가 뛰어나다

이미 대중화된 웹브라우저를 사용함으로써 사용법을 익히기가 쉽기 때문에 특별한 교육 없이 사용하기 쉽다. 더구나, 사용자 정보를 관리하여 사용자 각각의 결함 탐지 선택 메뉴를 제공하여 최대한의 편의를 도모하였다.

- 기타 보안 관련 정보 제공 기능

앞서 열거한 SOD 서버의 기능들 이외에 신속하고 종합적인 보안 정보 서비스를 위해 SOD 서버 메일링-리스트, 각종 보안 관련 웹 사이트, 인터넷에 공개된 보안 도구 및 그 밖의 보안 관련 정보들을 제공한다.

III. 결론 및 향후 연구 방향

SOD 서비스는 시스템 보안 결함을 원격으로 점검해주는 서비스로 사용하기도 편리하고 확장성도 용이하며, 점검받는 시스템의 보안 결함 정보 자체에 대한 보안성도 뛰어나다. 기본적으로 웹 서버를 이용한 클라이언트/서버 모델을 취하고 있으며 Perl 을 이용하여 보안 결함 탐지 코드를 구현하였다.

현재 프로토타입인 SOD 서비스가 상품화 하기 위해서는 다음과 같은 연구가 필요하다.

- 지속적인 보안 결함 정보 검색을 위한 전략 수립
- 현재까지 발견된 모든 보안 결함에 대한 탐지 모듈 구현
- 다양한 운영체제 지원
- 보다 고도화된 탐지 모듈 생성 알고리즘 개발
- 코드의 분량을 최소화하여 전송속도 단축
- 일정규모 이상의 가입자 관리를 위한 가입자 정보 관리 데이타베이스 구축
- 여러 클라이언트의 동시 접속시 서버의 안정성 검증
- 가입자 등록 정보 보호를 위한 HTTPS 프로토콜로의 구현
- 특정 웹브라우저에 의존하지 않는 Perl 코드 생성
- 보다 세련된 홈페이지 작성

이외에도 SOD 서비스를 포함 각종 보안 관련 문서나 도구 제공, 보안 관련 상담, 다른 보안 정보 사이트나 메일링 리스트와의 링크등을 포함하여 보안 전문 종합 서비스로 발전시킬 수 있을 것이다.

<참 고 문 헌>

1. Eric Herrmann, *CGI Programming with Perl 5*, Sams.net, 1996.
2. Larry Wall and Ransal L. Schwartz , *Programming Perl,* O' Reilly & Associates, Inc., 1991.
3. 천왕성, *"통합 보안 결함 탐지 도구 개발 : Security Hole Examiner"* , Proceeding of COMSW' 97, 1997.
4. "Security Administrator Tool for Analyzing Networks(SATAN)" , Cert Advisory, April, 1995.
5. Daniel Farmer, "The COPS Security Checker System" , Purdue University Technical Report CSD-TR-993, September, 1991
6. 김영길, 박정식, 백석철, "SSL 프로토콜을 적용한 WWW 환경의 정보보호 방법 연구" , COMSW' 97, July, 1997.
7. 김영길, 박정식," Apache-SSL 을 이용한 보안 기능이 강화된 HTTP 서버 구축 방법" , 한국통신학회 1997 년 하계종합학술발표회 논문집, 1997.