침해사고 예방 프레임워크 개발

이은영°, 김도환, 김우년, 주미리, 박응기
국가보안기술연구소
{eylee°, dkim,mrjoo, wnkim, ekpark}@etri.re.kr

Development of a Framework for Preventing Computer Incidents

Eun Young Lee°,Do hwan Kim, Woonyon Kim,Mi-Ri Joo, EungKi Park
National Security Research and Institute

요 약

최근의 웜이나 바이러스로 인한 침해 사고는 다수의 불특정 시스템을 대상으로 삼는 특성을 지닌다. 대부분의 침해 사고의 처리는 감염된 시스템을 발견하여 처리하는 방식이나 이러한 방식으로는 급속도로 확산되는 침해사고를 미리 방지하기가 힘들다. 본 논문에서는 침해 사고의 효과적인 방지를 위한 새로운 프레임 워크를 제안하였다. 평소에 관리하고자 하는 서버들의 정보를 수집하고 관리함으로써 새로운 취약점이 발견되었을 때 또는 침해 사고가 발생하였을 때 취약할 가능성이 있는 서버들을 신속히 파악할 수 있으며, 이를 바탕으로 특정 취약점을 점검하는 도구를 생성하는 공통 프레임 워크를 통해 취약점을 점검하는 도구를 생성한다. 즉, 이를 이용해 취약할 가능성이 있는 서버들을 사전에 점검하는 것이다. 점검결과 감염된 시스템은 치료하고 취약하나 감염이 되지 않은 시스템은 취약점을 제거하여 침해사고에 미리 대응할 수 있다. 본 논문에서는 데이터베이스에 등록된 관리 대상이 되는 서버 목록에 대해 특정 공격 출현 시, 공격에 대한 취약점을 진단하여 공격에 빠르게 대처함을 목적으로 하는 시스템을 제안하고 이를 구현하였다.

1. 서 론

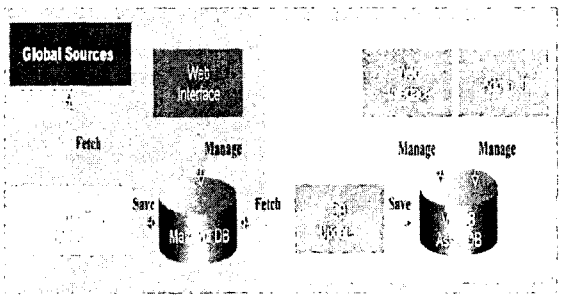
최근의 공격의 특징을 보면 불특정 다수의 시스템을 대상으로 하는 경우가 많다. 이들 인터넷 웜이나 바이러스는 확산 속도가 빨라 짧은 시간에 대다수의 시스템을 감염시킨다. 2002년도의 slammer worm 과 2003년도의 blaster worm의 예를 보면 발견 된지 1~2일 만에 전 세계로 확산되어 그 피해의 정도가 매우 컸음을 알 수 있다[1]. 이러한 사실은 침입에 대한 예방에는 소홀하였음을 말해 주고 있다. 특히 규모가 큰 회사와 연구소는 다수의 시스템을 보유하고 있기 때문에 침해사고가 발생하였을 때마다 모든 시스템을 일일이 점검하기가 어려우며, 점검하는데 많은 시간과 비용이 소요된다. 이러한 이유로 침해사고의 예방이 더욱 중요시 되고 있다. 침해사고의 확산 속도가 갈수록 빨라지고 있기 때문에 이를 진단하기 위한 취약점 진단도구의 제작 기간을 단축하는 것이 필요하며, 이를 이용하여 침해사고의 확산을 보다 효과적으로 예방할 수 있다.

본 논문에서는 침해사고가 발생하였을 때 대응 및 예방을 위한 프레임 워크를 제안[12]하고 이를 구현하였다. 평소에 주기적으로 시스템들의 정보를 수집함으로써 시스템 상황을 파악한다. 이러한 자료들은 새로운 취약점이 발표되거나, 침해사고가 발생 하였을 때는 시스템 취약여부를 결정하는 일차적 대상으로 사용된다. 침해 사고 발생시 일차적으로 감염 가능성이 존재하는 서버들을 대상으로 시스템 정보는 필수적이다. 이렇듯 진단 도구 생성에 필수적인 정보수집 과정, 프레임 형성과정 등에 관한 공통적인 프레임워크를 개발하여 진단 도구를 작성하는데 필요한 공통 Template을 제공함으로써 진단도구 제작 기간을 단축시킬 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 연구를 살펴보고 3장에서는 제안한 시스템을 소개하며 4장에서는 시스템의 설계와 구현을 다룬다. 마지막으로 5장에서 결론으로 끝을 맺는다.

II. 관련 연구

본 장에서는 시큐리티맵에서 개발한 실시간 취약점 관리시스템을 소개한다.[10] 실시간 취약점 관리 시스템은 크게 취약점 DB 관리와 자산 DB 관리로 나눌 수 있다. 취약점이 발견될 때마다[11] 이를 취약점 DB에 저장하여 관리하고 이와 함께 관리·보호해야할 시스템들의 자산 DB를 유지한다. 새로운 취약점이 발견되었을 때 이 취약점을 자산 DB와 비교를 하여 만약 관련된 자산이 있을 때에는 관리자에게 이를 알려 취약점에 대비를 하도록 한다. (그림1)은 실시간 취약점 관리시스템의 구조이다.

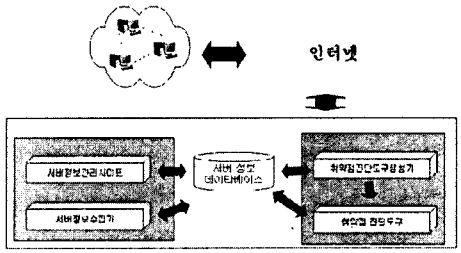


(그림 1) 실시간 취약점관리시스템 구조

Ⅲ. 제안한 프레임워크

제안한 프레임 워크는 크게 둘로 나누어 볼 수 있다. 하나는 평상시 관리해야할 서버들의 정보를 수집/분석하여 DB에 저장하는 Scanner Server시스템이다. 즉, 관리하고자 하는 시스템의 정보를 유지함으로써 침해 가능성이 있는 대상을 미리 파악하고 대처함으로써 공격을 미연에 대처할 수 있다. 다른 하나는 취약점 점검도구 생성 시스템이다. 이는 침해사고 발생시 취약점 진단 코드만을 삽입함으로써 취약점 점검도구를 생성해주는 시스템이다. 취약점 점검 코드의 삽입만으로 취약점 점검을 수행하는 도구를 자동으로 생성하는 프레임을 제공하는 것이다.

(그림2)는 제안한 프레임워크에 따른 시스템의 구성도이다.



(그림 2) 침해사고 예방 프레임워크 구성도

- 서버정보 데이터베이스
  서버정보 수집기에 의해 수집된 서버정보를 저장한다. 수집된 서버정보는 분석 및 1차 취약점 진단의 기본 데이터로 활용한다.

- 서버정보 수집기
  서버정보 관리사이트에 정해진 스케줄에 따라 특정 대역의 서버정보를 수집하며 지정된 규격으로 데이터베이스에 저장한다. 스캔을 통한 정보 수집은 네트워크 대역에 무리가 가지 않아야 한다. 한 단위 네트워크에 너무 많은 패킷이 전달되면 안 되므로 분산화된 스캔 과정이 필요하다. 즉, 각 서버들의 작동하는 네트워크의 부하를 줄이도록 분산화된 스캔을 수행하여야 한다.[2][3][4]

- 취약점 진단도구 생성기
  특정 취약점을 점검하는 코드만을 삽입한 후 컴파일하면 취약점 진단도구를 생성한다.

- 취약점 진단도구
  특정한 공격에 대해 취약점을 진단할 수 있는 도구로 데이터베이스 검색을 통한 1차 취약점 진단에서 검색된 서버를 대상으로 실질적인 취약점 진단을 수행 한다. [3][4]

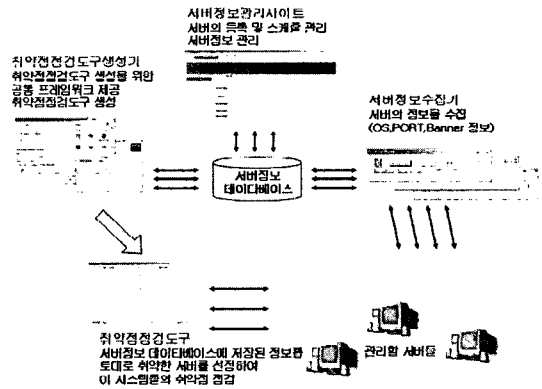
- 서버정보 관리사이트
  관리해야할 시스템을 등록하며 정보수집의 스케줄을 설정한다. 데이터베이스에 저장된 서버정보를 관리하며 정보에 대한 검색/수정/삭제 등이 가능하다. [3][4]

침해사고 예방 프레임워크는 다음과 같이 동작한다. 서버 현황 관리기를 통해 관리하고자 하는 네트워크 망내 시스템의 정보를 등록 하고 스캐닝 일정을 정한다. 서버 정보 수집기는 일정에 따라 시스템의 정보를 수집하고 이를 서버정보 데이터베이스에 저장하고 업데이트한다. 새로운 취약점이 발견되거나 침해 사고 발생하였을 때 취약점을 점검하는 코드를 취약점 진단도구 생성기에 삽입하여 취약점 점검도구를 생성한다. 생성된 취약점 점검도구는 감염이나 공격의 대상이 될 가능성이 있는 서버들을 대상으로 시스템을 점검한다. 마지막으로 점검결과에 따라 조치를 취하도록 서버관리자에게 통보한다.

침해사고 예방 프레임워크는 관리해야할 자산에 대한 현황을 미리 파악하고 있다. 따라서 새로운 취약점이 발견되었을 때 바로 침해 가능성이 있는 시스템을 파악할 수 있으며 즉시 조치가 가능하다. 또한 적절한 조치를 취하였는지를 점검할 수도 있다.

Ⅳ. 시스템 설계 및 구현

(그림3)은 본 논문에서 제안한 시스템의 전체 구현 모습이다.



(그림 3) 침해사고 대응 및 예방 프레임워크의 구현 모습

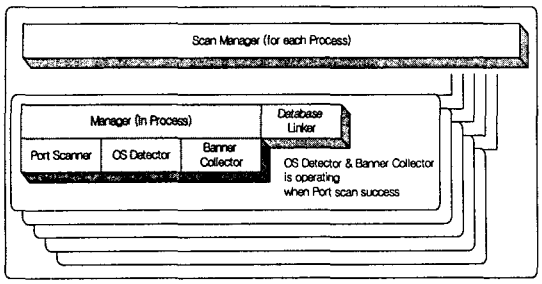
4.1. 서버 정보 데이터베이스

관리할 대상이 되는 서버에 대한 정보를 등록 및 관리하며, 서버정보 수집기를 통해 수집된 Port/OS/Banner 등의 관련정보를 저장한다. 데이터베이스는 기관 정보를 기준으로 기관 소속의 관리자, 서비스 제공업체, 기관이 소유하는 서버의 정보(IP 및 Port/Os/Service)를 저장한다. 이러한 정보는 관리사이트를 통해 기관, 관리자, 서비스 업체, 서버 정보를 입력/수정/삭제할 수 있으며, 수집된 정보를 토대로 각종 통계정보를 볼 수 있는 기반이 된다.

4.2 서버 정보 수집기(NscanRobot)

서버정보 수집기는 데이터베이스를 검색하여 해당되는 서버에 대해 Port Scan / OS Detection / Banner Collection 작업을 수행한다. 수집된 정보는 데이터베이스에 업데이트 된다. 서버정보 수집기는 하나의 Target 시스템에 대해 3개의 Module이 동작하며, 각각은 Port Scanner / OS Detector / Banner Collector이고, 이러한 동작은 하나의 Process로 구현된다. 또한, 정보 수집의 효율을 높이기 위해 동시에 여러 Process가 동작

하며 이에 대한 관리를 Scan Manager가 담당한다.[6][7][8][9]



(그림 15) 서버정보 수집기(NscanRobot)의 구조

4.3 취약점 진단 도구생성기

취약점 진단 도구 생성은 진단 코드 작성의 디버깅을 지원하기 위해 컴파일과 연계하였다. 취약점 진단도구 생성 Template은 특정 취약점 진단도구의 인터페이스 및 기능에 대한 부분을 미리 담고 있는 소스코드와 사용자가 Port/OS/Banner 등의 데이터베이스 검색 조건 및 취약점 점검 내용을 소스 수준에서 직접 입력할 수 있는 형태로 되어있다. 즉, Compile 전의 상태로 소스코드가 존재하며, 이 소스코드에 사용자가 직접 취약점 점검 코드를 추가하기 쉽게 하는 인터페이스를 갖는 어플리케이션 Template이다.

특정 취약점 진단도구 생성 Template은 MS의 Visual Studio 2003 version 7.1 상의 Template Project를 이용한다. 미리 제작된 특정 취약점 진단도구 Application의 VC Project 파일을 VC Template 형태로 전환하여 사용자가 직접 VC Project를 생성시에 제작된 Template을 선택하고, 기본 파라미터를 입력하면 직접 취약점 진단 코드만을 입력할 수 있는 형태로 Project가 생성된다.

4.4 취약점 진단 도구(VulChecker)

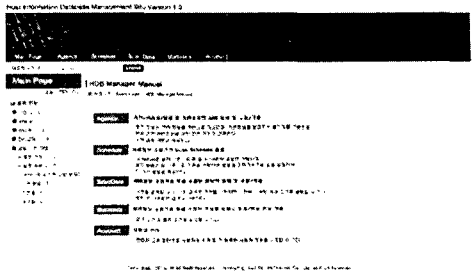
취약점 진단 도구 생성기에 의해 생성된다. 진단도구는 취약 Port 및 OS/Banner 정보를 이용하여 취약 가능한 서버의 IP 리스트를 얻는다. 얻어진 서버의 IP에 실제 진단코드를 수행함으로써 실제 취약한 시스템을 발견할 수 있다.

4.5 서버 정보 관리사이트(HDB SiteManager)

서버정보 데이터베이스를 관리하는 사이트이다. 저장된 정보에 대해 삽입/수정/삭제가 가능하다. 서버정보 수집기에 의해 수집된 정보를 볼 수 있는 웹 사이트이다. 본 관리사이트를 통해 관리대상 서버를 등록하며 정보수집 일정을 정한다.

관리사이트의 기능은 크게 다음과 같이 나눌 수 있다.

기능	상세설명
기관 정보 등록	기관소유의 서버등록 및 수정/삭제
Scan Schedule 설정	월 및 기관 단위의 Scan schedule 설정 - 날짜별 , 기관별 설정
수집된 서버정보 관리	수집된 서버정보의 열람 및 수정/삭제
통계기능	수집된 정보를 기반으로 하는 통계/현황 정보 산출



(그림 4) 서버정보 관리사이트 화면1

V. 결 론

현재 대부분의 침해 사고 대응은 침해사고가 발생한 이후 이를 처리하는데 초점을 두고 있다. 하지만 이러한 방식은 자동화, 분산화된 공격으로 인해 짧은 시간 안에 전 세계로 확산되는 침해사고에는 초기 대응이 어렵다. 제안된 시스템은 관리대상 서버들의 정보를 수집, 관리함으로써 평소에 이들 서버들의 현황을 파악하여 보안 지침을 제공할 수 있으며 새로운 취약점이 발견되거나 침해 사고가 발생하였을 때는 취약점에 대한 진단 도구를 빠르게 생성하여 시스템들을 점검함으로써 침해 사고에 대한 대응이 가능하게 한다. 하지만 서버의 스캔으로 인한 취약점 점검은 방화벽이나 스위치 등의 시스템에서 점검 패킷을 차단하는 경우에는 이용이 힘들다. 이러한 특징으로 본 시스템은 외부 시스템 점검보다는 기관의 내부 망에 존재하는 시스템을 관리하는 경우에 유용하다.

향후 연구과정으로는 제안된 시스템에 침해가 밝혀진 서버들을 복구하고 치료하는 대응 방법을 융합함으로써 예방과 대응이 가능한 침해사고 처리 방안의 연구가 필요하다.

참 고 문 헌

[1] 안철수연구소 homepage http://www.ahnlab.co.kr
[2] nmap homepage http://www.nmap.org
[3] nessus homepage http://www.nessus.org
[4] Security Administrator's integrated Network Tool http://www.wwdsi.com
[5] Internet Security Systems http://www.iis.net
[6] Metta Security Limited, *IP Network Scanning & REconnaissance, 2002*
[7] Fyodor, The Art of Port Scanning , http://www.phrack.com
[8] Joel Scambray, *Hacking Exposed 2nd*
[9] whitepaper by dethy@synnergy.net, Examing port scan methods - Analysing Audible Techniques
[10] 실시간 취약성 관리시스템. www.securitymap.com
[11] 취약점 DB 제공 HOMPAGE, http://www.cve.mitre.org/
[12] 이은영, 김도환, 박응기, 침해사고 대응 및 예방 프레임워크, *한국정보과학회*, 2003년 가을학술발표논문집, 30(2) pp. 730~732 2003