일반화된 보안패치 분배 및 관리 시스템을 위한 프레임워크 설계

이상원°, 김윤주*, 손태식*, 문종섭*, 서정택**, 이은영**, 이도훈**
고려대학교 정보보호대학원*, 국가보안기술연구소**
{a770720°, zzuya99, 743zh2k, jsmoon}*@korea.ac.kr, {seojt, eylee, dohoon}** @etri.re.kr

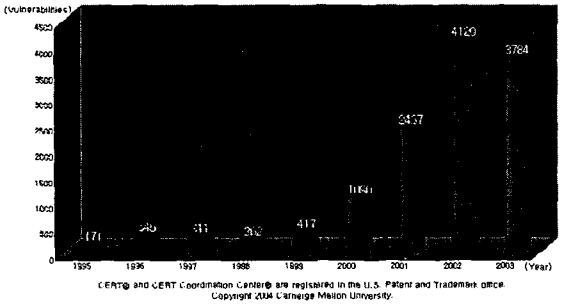
Design the Normalized Secure Patch Distribution & Management System

Sangwon Lee°, Yun-Ju Kim*, Tae-Shik Sohn*, Jong-Sub Moon*, Jung-Taek Seo**, Eun-Yong Lee**, Do-Hoon Lee**
Center for Information Security Technologies (CIST), Korea University*,
National Security Research Institute**

요 약

해마다 보고되는 보안 취약점은 크게 늘어나고 있으며, 이를 보완하기 위한 보안패치 역시 릴리즈 되는 시간 간격이 짧아지고 있는 실정이다. 따라서, 효과적인 보안패치 분배 작업이 이루어지기 위해서는 자동화된 보안패치 관리 시스템의 도입이 절실히 필요하다.

본 논문에서 이러한 필요성을 기반으로 한 지금까지의 보안패치 분배 및 관리 시스템에 대한 연구 내용들을 분석함으로써 보안패치 분배 및 관리 시스템이 갖추어야 할 요건들을 살펴보고, 이러한 문제점들을 해결하기 위한 프레임워크를 직접 설계함으로써 그 해결 방안을 제시하고자 한다.



(그림 1) 보안 취약점 보고현황 (1995-2003)

1. 서 론

2003년 1월 25일 발생한 SQL Slammer 웜은 전세계 컴퓨터 사용자들에게 보안에 대한 관심을 불러일으키는데 아주 중요한 역할을 했다. 그러나, 일반 사용자들이 이에 대한 대응책으로 선택한 것이 안티 바이러스 소프트웨워의 설치 수준에 머물러 있어서 또 다른 문제점으로 대두되고 있다. CERT에서는 "위험에 노출되었던 사용자들이 단지 안티 바이러스 소프트웨어를 설치하고 있는 것으로 모든 악의적인 코드의 공격으로부터 그들을 보호할 수 있다는 잘못된 생각을 인식한 국내 안티 바이러스 소프트웨워 제작 회사인 안철수 연구소는 "보안 취약점을 악용하는 웜/바이러스는 아무리 백신으로 진단하고 치료해도 취약점을 없애주는 보안패치 파일을 설치하지 않으면 다시 감염되기 때문에 패치 관리 시스템이 효과적인 대안" 이라고 강조하고, 자사 안티 바이러스 소프트웨워에 보안패치 관리 솔루션을 도입하여 보다 안정적인 통합 보안 솔루션을 만들려는 노력을 하고 있다고 밝히고 있다[2].

게다가 (그림 1)에서도 알 수 있듯이 해마다 보고되는 보안 취약점은 크게 늘어나고 있으며, 이를 보완하기 위한 보안패치 역시 릴리즈 되는 시간 간격이 짧아지고 있는 실정이다[1]. 따라서, 효과적인 보안패치 분배 작업이 이루어지기 위해서는 자동화된 보안패치 관리 시스템의 도입이 절실히 필요하다.

이러한 필요성을 기반으로 그동안 다양한 분야에 대해서 보안패치 분배 및 관리 시스템에 대한 연구 및 설계 개발 작업이 진행되어왔다. 이러한 과정에서 보안패치 분배 및 관리 시스템이 갖추어야 할 조건들을 보다 명확하게 정의하고, 그 각각에 대한 설계 및 개발 작업을 이끌어냄으로써 앞으로 보다 진보된 보안패치 분배 및 관리 시스템에 대한 연구 작업이 이루어질 수 있는 기반을 마련할 필요성이 대두되었다.

따라서, 본 논문에서는 지금까지 연구되어 온 보안패치 분배 및 관리 시스템에 대한 고찰을 통하여 보다 일반화된 보안패치 분배 및 관리 시스템의 프레임워크를 설계하고자 한다. 2장에서는 기존 보안패치 관리 프레임워크에 대한 고찰, 3장에서는 2장의 내용을 바탕으로 한 보안패치 분배 및 관리 시스템이 갖추어야할 요건, 4장에서는 이러한 요건들을 모두 만족시킬 수 있는 보안패치 분배 및 관리 시스템의 구성을 위한 프레임워크 설계 내용을 언급하고, 5장에서는 결론을 맺도록 구성되었다.

2. 기존의 보안패치 분배 시스템에 대한 고찰

2.1 멀티플랫폼 환경에서의 보안패치 분배를 위한 DB구축 및 검색 방법에 관한 연구 [7]

보안패치 분배 시스템에 대한 관심이 증가하여 많은 관련 제품들이 나오면서 이에 대한 선별 기준에서 충족시켜야만 하는 필수 조건으로서 이종 컴퓨팅 환경과 다중 플랫폼, 운영체제, 버전의 지원여부를 들고 있다. 이러한 요구조건들을 충족시킬 수 있도록 하기 위해서 멀티플랫폼 환경에서의 보안패치 분배를 위한 DB 구축 및 검색 방식을 제안하였다.

2.2 RMI와 SSL를 이용한 멀티플랫폼 환경에서의 안전한 보안패치 분배 시스템 설계 [8]

멀티플랫폼 환경을 지원하기 위해서 각각의 플랫폼별로 보안패치 분배 시스템을 설계 및 개발하는 것은 많은 부하가 걸리는 작업이며, 자칫 안정적이지 못한 시스템을 양산할 수 있다. 더군다나 보안패치 분배 시스템이 정상적으로 작동하지 않을 경우 해당 네트워크의 안정성에 큰 위협을 가할 수 있기 때문에, 보안패치 분배 시스템은 반드시 그 운영에 있어서 안정성을 보장할 수 있어야만 한다.

이러한 조건들을 모두 충족시키며 분산 컴퓨팅 기능을 제공할 수 있도록 하기 위해서, Java RMI 기술과 안전한 통신을 보장하기 위해서 SSL를 함께 도입한 보안패치 분배 시스템을 제안하였다.

2.3 확장성을 고려한 계층적 패치 분배 시스템 프레임워크 설계 [9]

최근 자동화된 패치 관리 시스템에 대한 연구가 많이 이루어지고 있지만, 패치 관리 대상이 되는 대규모 네트워크 그룹의 규모와 구조가 유동적임을 간과하고 있다.

여기서 제안하는 프레임워크로 패치 분배 서비스를 제공하는 것은 하나의 서버를 관리함으로서 여러 그룹을 동시에 제어할 수 있게 된다. 이것은 각각의 패치 서버들이 다양한 운영체제 벤더에 산재되어

있는 패치를 일일이 수집하고, 테스트, 배포, 적용, 확인하는 시간과 비용을 현격히 줄일 수 있고, 개인 프라이버시의 문제를 갖고 있는 그룹화를 사용하지 않고 서버의 부하를 줄일 수 있는 장점이 있다.

2.4 계층적 보안패치 분배 시스템의 안정성 확보를 위한 프레임워크 설계 및 구현 [10]

클라이언트 시스템에 보안패치를 설치해주는 과정에서의 안정성 확보를 위해서 보안패치간의 의존성 해결을 위한 방안을 모색, 개발하였다.

3. 보안패치 분배 및 관리 시스템이 갖추어야할 요건

① 보안성 : 이 요건은 단순히 보안패치 분배 및 관리 시스템만이 아니라 모든 것이 공개되어 있는 인터넷 환경에서 일정한 목적을 가지고서 중요한 일련의 작업들을 처리하는 과정에서는 가장 기본적으로 해결되어야 하는 문제이다. 이 요건을 무시하고 보안패치 분배 및 관리시스템의 동작 환경을 단순히 보안성이 확보된 폐쇄 네트워크 또는 특정 그룹내의 네트워크 환경으로 한정짓는 것은 현실적이고 근본적인 대처 방안이 절대로 될 수 없다.

② 안정성 : 보안패치 분배 및 관리 시스템과 같이 조직의 중요한 기능을 담당하고 있는 서버들의 경우, 안정성을 확보하는 것은 앞에서 살펴본 보안성과 함께 가장 기본적으로 확보해야만 하는 전제 조건이다. 보안패치 분배 및 관리 시스템이 정상적으로 동작하지 않을 경우, 해당 서버의 관리영역에 있는 많은 시스템들이 그들의 안정성에 큰 위협을 받을 수 있기 때문이다.

③ 의존성 : 보안패치의 경우 상호 의존성을 가지고 있는 보안패치들이 존재한다. 예를 들어서, 특정 보안패치의 경우 설치 이전에 반드시 설치되어 있어야 할 다른 보안패치를 요구하거나 특정 수준 이상의 보안패치 설치 현황을 요구할 수 있다. 따라서, 의존성을 무시하고 단순히 보안패치를 분배 및 설치하는 작업은 정상적으로 동작하고 있는 시스템에 심각한 오류를 발생시키며, 이것은 보안패치를 설치함으로써 취약점으로부터 벗어나 안정성을 확보하려는 본래 목적과는 상치되는 역효과를 불러올 수 있다.

④ 확장성(유동성) : 보안패치 분배 및 관리 시스템을 필요로 하는 곳은 개인보다는 일정 규모 이상의 중·대형 네트워크를 구축하고 있는 기업 또는 공공 기관과 같은 조직이라고 할 수 있다. 이러한 중·대형 네트워크 환경에서 하나의 서버가 모든 일을 처리하는 것은 서버의 과부하 발생 및 병목현상을 불러올 수 있기 때문에, 계층적으로 다단계 서버들을 배치시킴으로써 규모에 있어서의 확장성을 지원할 수 있어야만 한다. 또한, 그룹의 형태 및 구성원들이 자주 변화할 수 있는 실제 사회의 유동성에 적절히 대응할 수 있도록 하기 위해서라도 규모에 있어서의 확장성을 지원하는 것은 필수 요건이라고 할 수 있다.

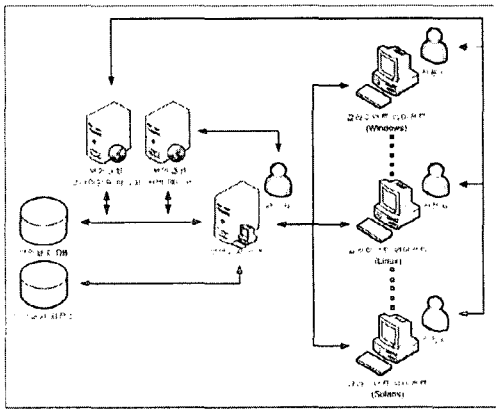
⑤ 범용성 : 보안패치 분배 및 관리 시스템이 관리하는 네트워크 환경에는 일반적으로 하나 이상의 상이한 운영체제를 가진 시스템들로 이루어져 있다. 이러한 환경에서 단순히 하나의 운영체제에 대한 보안패치 서비스를 제공하는 것은 의미가 없으며, 필수적으로 멀티플랫폼 환경을 지원할 수 있어야만 한다. 또한 네트워크 환경은 동적 IP, 사설 IP환경 등 매우 다양한 형태를 띠고 있기 때문에 보안패치 분배 및 관리 시스템이 범용성을 갖추기 위해서는 다양한 네트워크 환경을 지원할 필요가 있다.

⑥ 관리성 : 보안패치 분배 및 관리 시스템이 단순히 자동적으로 보안패치를 분배해주고 설치하는 단계까지 유도만 해주는 것은 각각의 개인에게 직접 운영체제 벤더로부터 보안패치를 설치할 것을 권고하고, 그러한 행동을 해주기를 바라기만 하는 수동적인 태도와 다를 바가 없다. 즉, 이러한 솔루션을 도입한다는 것 자체가 의미가 없는 것이다. 따라서, 보안패치 분배 및 관리 시스템은 중앙에서 보안패치 설치 현황을 한눈에 살펴볼 수 있으며, 필요한 경우 적절한 조치를 취할 수 있도록 지원해야만 한다.

⑦ 편리성 : 보안패치 분배 및 관리 시스템을 통한 일련의 작업들을 분명히 매우 중요한 작업이다. 그러나, 사용자의 특수한 사정으로 인하여 분배받은 즉시 보안패치를 설치할 수 없어서 일정한 시간만큼의 설치 기한 연장을 요구할 수 있으며, 일부 사용자들은 분배받은 보안패치를 설치할 때마다 승인을 받지 않고 백그라운드에서 자동으로 설치할 것을 요구할 수도 있다. 물론 특정 조직에서는 관리자의 설정에 따라서 보안패치들을 무조건 백그라운드에서 무인모드로 자동 설치할 수 있도록 정책 설정하기를 원할 수 있다. 이처럼 보안패치 분배 및 관리 시스템이 보다 효율적으로 동작할 수 있도록 조직의 안정성 정책에 크게 위반되지 않는 한 관리자 및 사용자들에게 다양한 편의 기능을 제공하는 것은 매우 바람직하다고 할 수 있다.

4. 보안패치 분배 및 관리 시스템의 구성

4.1 기본 구성



(그림 2) 보안패치 분배 및 관리 시스템 구성도

그림 2는 보안패치 분배 및 관리 시스템의 기본 구성도이다. 상술한 문제점들을 해결하기 위한 기술적 수단으로, 본 논문에서는 클라이언트와의 통신 작업을 통해서 클라이언트들에게 스캐닝 작업의 바탕이 되는 스캔 리스트 및 해당 클라이언트에게 필요한 보안패치 파일을 전송해주는 보안패치 서버[3,4], 스캔 리스트를 참조하여 클라이언트 시스템을 분석함으로써 설치할 필요가 있는 보안패치의 존재 여부를 확인하고 일련의 설치 작업을 수행하는 보안패치 클라이언트 에이전트[5,6,7,8], 클라이언트들의 보안패치 설치 현황들을 확인하고 관리할 수 있도록 인터페이스를 제공해주는 보안패치 서버 매니저[5,6,7,8], 사용자가 자신의 보안패치 설치 현황 등을 점검 및 확인하고 필요한 경우 요청할 수 있도록 인터페이스를 제공해주는 보안패치 클라이언트 매니저[5,6,7,8], 이 시스템의 주요 핵심 데이터가 되는 스캔 리스트 및 보안패치 파일을 보관하고 있는 보안패치 저장소, 보안패치 설치 현황을 관리할 수 있는 기반을 만들어주는 보안패치 DB[3.4]를 포함하여 구성되며, 일반적으로 클라이언트 에이전트가 서버에 접속하여 자신의 시스템에 맞는 스캔 리스트를 받아서 설치해야 할 보안패치 파일의 존재여부를 확인하여 그 결과에 따라서 적절한 행동을 취함으로써 보안패치 분배 서비스를 제공받을 수 있다.[3,4,5,6,7,8]

4.2 보안성 확보를 위한 설계 및 구성

① 서버와 클라이언트간의 모든 통신작업은 인증서를 기반으로 한 SSL방식을 사용한다. [5]

② 분배받은 보안패치 파일과 서버에 있는 원본 파일과의 진위여부를 판단하기 위해서 해쉬함수, CRC체크 등의 방식을 이용한다.

4.3 안정성 확보를 위한 설계 및 구성

① JVM의 관리를 받는 RMI를 이용함으로써 많은 사용자들에게 동시 서비스를 제공하기 위한 쓰레드 및 소켓 처리, 메모리를 비롯한 각종 자원의 할당 등의 작업을 안정화시킨다. [6]

② 보안패치 저장소에 보관되어 있는 스캔 리스트를 이용하여 클라이언트 에이전트에서 검색작업을 수행하도록 함으로써 서버에서 가장 부하가 큰 작업중의 하나인 보안패치 검색 작업을 서버에서 클라이언트로 이관시킨다.

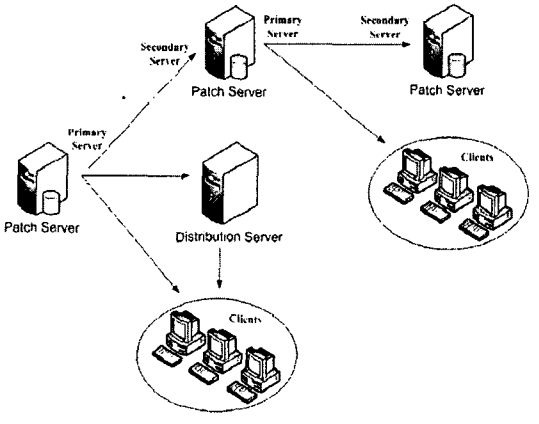
4.4 의존성 확보를 위한 설계 및 구성

① 의존성 해결을 위한 정보들을 담고 있는 스캔 리스트를 참고하여 클라이언트 에이전트에서 보안패치간의 상호 의존성 관계 (특정 dll 및 파일의 버전 정보, 레지스트리 정보, 파일의 존재성 여부 등)를 정확하게 판단할 수 있다.

4.5 확장성 확보를 위한 설계 및 구성

① 확장성을 지원하고 서버의 과부하를 방지하기 위한 목적으로 보안패치 서버는 크게 Primary Server, Secondary Server, 분배 서버로 다시 나눌 수 있다.

② 관리자가 직접 관리하는 일종의 상위레벨 그룹을 담당하는 보안패치 서버를 Primary Server라고 하며, 이러한 Primary Server로부터 관리를 받는 그룹의 보안패치 서버를 Secondary Server라고 한다. 일반적인 보안패치 서버로서의 역할은 서로 비슷하지만, Primary Server는 보안패치를 분배해주어야 하는 클라이언트로서 Secondary Server까지 포함한다는 점이 다르다. 이러한 구분은 확장성을 지원하기 위하여 그룹간의 통합만이 아니라, 초기에 보안패치 분배 및 관리 시스템을 구축하는 과정에서 서버의 과부하를 방지하기 위한 목적으로 구축할 때 역시 발생할 수 있다. 그림 3은 이러한 Primary Server와 Secondary Server가 여러 단계로 확장된 경우를 나타낸다. 그림에서도 알 수 있듯이, 하나의 보안패치 서버는 자신의 상위 서버에게는 Secondary Server이지만, 하위 서버들에게는 Primary Server가 된다. 분배서버는 Primary Server와 Secondary Server와는 다르게 자신이 관리하는 클라이언트들이 명확하게 정해져 있지 않고, 단순히 상위의 서버로부터 분배해주어야 하는 보안패치 파일과 함께 분배해주어야 하는 대상 클라이언트 목록을 함께 전달받아서 상위 서버가 해야하는 분배 작업을 함께 수행함으로써 상위 서버의 과부하 발생 및 병목 현상을 없애줄 수 있다.



(그림 3) 확장성을 위한 보안패치 분배 및 관리 시스템의 구성

4.6 범용성 확보를 위한 설계 및 구성

① 보안패치 분배 서비스를 받기 위해서는 가장 먼저 클라이언트 매니저에 접속하여 가입 후 에이전트를 다운로드 받아야만 한다. 이때 자신이 서비스를 받을 수 있는 서버 정보를 받게 되며, 따라서 모든 통신과정은 클라이언트에서 접속을 시작함으로써 이루어질 수 있다. 이와 같은 방식을 따를 경우, 동적 IP 및 사설 IP환경에서도 원활한 보안패치 분배 서비스를 제공받을 수 있게 된다.

4.7 관리성 확보를 위한 설계 및 구성

① 스캔 리스트를 기반으로 하여 클라이언트 에이전트는 중앙에서 관리를 수행하는데 기준이 되는 보안패치 설치 현황 정보를 생성하여 서버에게 넘겨준다.

② 이 정보를 바탕으로 서버에서는 각각의 사용자별 보안패치 설치 현황 확인, 각각의 보안패치에 대한 사용자별 설치 현황 확인, 특정 사용자에 대한 보안패치 설치 경고를 통한 강제 설치 기능 등을 수행할 수 있다.

4.8 편리성 확보를 위한 설계 및 구성

① 사용자의 작업을 방해하지 않도록 보안패치 설치 작업은 기본적으로 백그라운드 설치 기능을 제공하며, 관리 정책으로부터 크게 위반되지 않는 범위내에서 환경설정 UI를 이용하여 자신의 환경 설정을 파일로 보관하여 적절한 행동을 취할 수 있도록 지원한다.

5. 결론

지금까지 기존 연구를 분석한 결과들을 바탕으로 보안패치 분배 및 관리 시스템이 갖추어야 할 기본적인 요건들에 대해서 제안하고, 해당 요건들을 어떠한 방식으로 해결해 나갈 수 있는지 직접 설계함으로써 자세한 작업 과정을 살펴보았다. 이러한 설계내용을 바탕으로 그 구성의 세부 내용들에는 보안패치 분배 및 관리 시스템의 사용 현황에 따라서 보다 많은 관련된 기능들이 더욱 추가되거나, 기본적인 골격을 유지한 채로 변형도 가능할 것이다.

앞으로는 본 논문의 내용들을 기반으로 하여 직접 개발하는 과정이 뒤따라야 할 것이며, 또한 다양한 운영체제를 사용하는 시스템들이 함께 존재하는 것이 일반적인 네트워크 환경에서 의존성 해결 및 검색 작업이 이루어질 수 있도록 하기 위해서 운영체제 벤더간의 XML등을 이용한 표준 스캔 리스트를 만들 것을 제안한다. 이것은 앞으로 보다 범용적이고 안정적인 보안패치 분배 및 관리 시스템을 위해서라도 반드시 필요한 연구 작업이 될 것이다.

6. 참고문헌

[1] CERT Coordination Center, http://www.cert.org
[2] 안철수연구소, http://home.ahnlab.com/
[3] Sohn Tae-Shik, "Safe Patch Distribution Architecture in Intranet Environments", SAM, 2003
[4] Cheol-Won Lee, "A Secure Patch Distribution Architecture", ISDA 2003, Lecture Notes in Computer Science, Springer-Verlag, 2003
[5] Frier A., Karlton P. & Kocher P., The SSL Protocol Version 3.0, http://wp.netscape.com/eng/ssl3/draft302.txt
[6] Java RemoteMethodInvocation Specification, ftp://ftp.java.sun.com/docs/j2se1.4/rmi-spec-1.4.pdf, Sun Microsystems, Inc.
[7] 이상원, 김윤주, 손태식, 문종섭, 서정택, "멀티플랫폼 환경에서의 보안패치 분배를 위한 DB구축 및 검색 방법에 관한 연구", 한국정보과학회 춘계학술대회, 2004
[8] 이상원, 김윤주, 손태식, 문종섭, 서정택, 최대식, 박웅기, "RMI와 SSL를 이용한 멀티플랫폼 환경에서의 안전한 보안패치 분배 시스템 설계", 한국정보과학회 춘계학술대회, 2004
[9] 김윤주, 이상원, 손태식, 문종섭, 서정택, 윤주범, 박웅기, "확장성을 고려한 계층적 패치 분배 시스템 프레임워크 설계", 한국정보과학회 춘계학술대회, 2004
[10] 김윤주, 이상원, 손태식, 문종섭, 서정택, 최대식, 박웅기, "계층적 보안패치 분배 시스템의 안정성 확보를 위한 프레임워크 설계 및 구현", WISC 2004