멀티플랫폼을 지원하는 패치 자동관리시스템

서정택[O*] 윤주범* 최대식* 박응기* 서정우** 손태식** 문종섭**
*국가보안기술연구소, **고려대학교 정보보호대학원
{seojt[O], netair, dschoi, }@etri.re.kr, {korea002, 743zh2k, jsmoon}@korea.ac.kr

Patch Management System with Multiplatform Support

Jung-Taek Seo[O*] Dae-Sik Choi* Joo-Beom Yun* Eung-Gi Park* Jung-Woo Seo** Tae-Shik Sohn**
Jong-Sub Moon**
* NSRI(National Security Research Institute), **CIST, GSIS, Korea University

요 약

운영체제 시스템 및 관련 응용 프로그램들은 프로그램 개발 과정의 특성상 보안 취약성을 가지고 있다. 이와 같은 보안 취약성을 악용하는 침해사례가 최근 증가하고 있으며, 그 피해의 파급효과가 더욱 커지고 있다. 침해사고 예방의 기본적인 방법은 보안 취약성을 제거하는 패치의 실시간적인 설치이다. 그러나, 대부분 관리자의 관리가 미숙하여 각 사이트에 가서 패치를 다운받아 설치하는데 어려움을 느끼고 있다. 본 논문에서는 중앙의 패치관리서버가 Windows, UNIX, LINUX 벤더들로부터 패치를 다운받아 패치를 필요로 하는 시스템들을 선별하여 안전하게 패치를 자동분배하고, 설치하는 시스템을 제안한다. 멀티플랫폼을 지원하는 패치 자동관리시스템을 이용하여 그때그때 필요한 패치가 신속하게 설치됨으로써 시스템의 보안성을 높일 수 있다.

1. 서 론

일반적으로 모든 운영체제 시스템 및 관련 응용 프로그램들은 프로그램 개발 과정의 특성상 보안 취약성을 가지고 있기 마련이다. 이러한 보안 취약성을 악용하는 침해사례가 급증하고 있으며, 그 피해의 파급효과가 커지고 있다. 이러한 추세에서 패치에 대한 안전하고 신속한 분배 및 설치는 해당 시스템의 보안을 위한 가장 기본적이고 필수적인 요소로 강조되고 있다.

하지만 보안을 위해 시스템 관리자들이 주기적으로 패치를 다운받아 시스템에 설치하여야 하는데, 이 방법은 일일이 해당 사이트에 가서 패치를 다운받아야 하며, 관리자들의 처리를 필요로 한다. 또한, 패치의 분배 및 설치 과정에서 패치 정보의 누출이나 패치를 가장한 트로이목마와 같은 백도어의 설치 등과 같은 보안상의 문제점을 가져올 수 있다.

본 논문에서는 중앙의 패치관리 서버가 각 벤더들로부터 패치를 다운받아 DB에 저장하고, 프로파일 관리기법을 이용하여 해당 패치를 필요로 하는 시스템들을 선별하여 패치를 자동으로 분배하고, 설치하는 중앙 집중화된 보안관리 시스템을 제안한다.

2. 동향 분석

2.1 벤더별 패치 분배 기술동향

각 벤더들의 패치 분배과정에 있어서 능동적인 분배와 수동적인 분배로 나누어진다. 능동적인 분배는 벤더가 사용자에게 새로운 패치가 나왔음을 메일이나 다른 통신채널을 통하여 알려주어 사용자가 웹사이트나 FTP 사이트에 접속하여 패치를 다운받아 설치하는 것이다. 수동적인 분배는 사용자가 웹사이트나 FTP 사이트에 접속하여 새로운 패치가 있는지 확인하여 다운받아 설치하는 것이다.

운영체제 벤더들은 패치 분배 과정의 인증, 무결성 및 기밀성 보장하기 위하여 PGP(Pretty Good Privacy), HTTPs, SSH(Secure SHell) 기법을 사용하고 있다. 하지만 이 기법들을 이용하여 인증, 무결성, 기밀성을 동시에 다 만족시킬 수 없다.

2.2 Ecora Patch Manager

통합관리 솔루션 업체인 Ecora 시스템에서 패치 관리를 위해 만든 솔루션으로 중앙의 관리시스템이 각 클라이언트 시스템들에 대한 패치 관리를 수행한다. Ecora 시스템은 Windows를 기반으로 하고 있으며 패치 대상도 주로 Windows 제품군을 대상으로 하고 있다. Ecora의 Patch Manager는 다른 패치 관리시스템들과 같이 패치 DB를 따로 가지고 있지 않고, Ecora 사 측에서 자체적으로 제공해주고 있다. 즉, 시스템 관리자는 새로운 패치를 확인하기 위해 벤더 사이트에 접속하지 않고, Ecora에서 제공해 주는 패치만을 사용할 수 있다. / 또한, Ecora 시스템의 Free-Agent 기술은 관리자가 클라이언트 시스템에 Agent를 설치하지 않도록 하여 관리자의 편의를 제공하는 기술이다. 즉, Patch Manager 소프트웨어가 원격으로 에이전트 설치에 관련된 모든 작업을 수행한다.

Ecora 시스템에서도 관리자는 새로운 패치에 대해서 항상 민감하게 반응하여야 하고, 최신의 패치를 DB에 저장하고 있어야 한다.

Ecora 시스템은 중앙 집중화된 패치 관리를 효율적으로 수행하지만, 마이크로소프트 제품군에 치중된 패치를 관리하고 있다는 것이 단점이다. 리눅스와 솔라리스 등과 같은 다른 플랫폼에서의 패치를 제공하지 못하는 것이 단점이다.

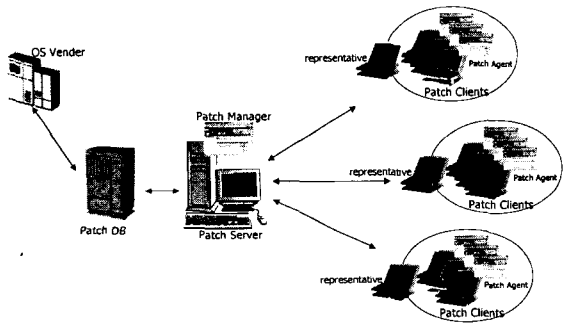
3. 멀티플랫폼을 지원하는 패치 자동관리 시스템

본 논문에서 제안하는 멀티플랫폼을 지원하는 패치 자동관리 시스템은 상이한 시스템들로 구성되어 있는 대규모 네트워크 환경에 적합한 패치 자동분배 및 설치 기능을 제공한다. 따라서, 상이한 시스템들로 구성되는 대규모 네트워크의 대상은 특정 조직이나 기관 등의 체계적인 시스템 관리가 가능한 네트워크 환경이어야 한다. 제안하는 시스템에서는 벤더가 제공하는 패치를 가져와 DB로 관리하며, 분배 솔루션에 의하여 분배 및 설치 과정이 수행된다. 또한, 멀티플랫폼으로 윈도우즈 계열의 Windows 2000과 Windows XP, 유닉스 계열의 Solaris, 리눅스 계열의 Redhat 시스템을 대상으로 한다.

3.1 멀티플랫폼을 지원하는 패치 자동관리 시스템 구성

멀티플랫폼을 지원하는 패치 자동관리 시스템의 구성은 패치 DB, 패치 관리 서버, 패치 매니저, 패치 클라이언트, 패치 에이전트로 구성된다.

- 패치 DB : 보안 도메인 내에 구성되어 있는 시스템에 해당하는 패치 파일 및 관련 정보와 패치 클라이언트 시스템의 패치 프로파일 및 사용자 정보를 저장한다. 이때 패치 DB에 저장되는 패치 파일은 패치 프레임워크에 알맞은 포맷으로 변환되어 저장된다.
- 패치 관리 서버 : 패치 클라이언트와의 분배 프로토콜을 통하여 패치 클라이언트에게 필요한 패치를 패치 DB로부터 가져와 분배 과정을 수행한다.
- 패치 매니저 : 패치 DB의 구성 정보에 대한 관리 및 패치 서버 관리를 수행하며, 웹기반의 UI를 이용하여 관리자에게 편의성을 제공한다.
- 패치 클라이언트 : 대상은 Windows 2000과 Windows XP, Solaris, Redhat 시스템이며 패치 서버에게 필요한 패치를 요구하는 등의 실제 패치 분배 및 설치 작업을 수행하기 위하여 패치 에이전트를 수행한다.
- 패치 에이전트 : 패치 클라이언트 측에 설치되어 대상 클라이언트의 패치 정보 관리를 수행하며, 웹기반의 UI를 통해 사용자에게 편의성을 제공한다.



[그림 1] 시스템 전체 구성도

멀티플랫폼을 지원하는 패치 자동관리 시스템은 클라이언트가 패치 관리서버에 신규 접속한 경우, 클라이언트가 패치를 요구하는 경우, 패치 관리 서버가 클라이언트에게 패치를 분배하는 경우, 클라이언트 시스템 설정이 변경된 경우의 총 4가지 경우에 분배 및 설치를 수행한다.

가. 클라이언트가 패치 관리 서버에 신규 접속한 경우
1. 패치 관리 서버의 웹브라우저에 신규 접속하여 에이전트 프로그램 다운로드 및 설치
2. 패치 관리 서버와 클라이언트 소켓접속을 통한 클라이언트 시스템 정보 조사
3. 패치 관리 서버와 클라이언트간의 상호 인증 수행 및 패치 설치정보 및 프로그램 정보 검색
4. 패치 관리 서버와 클라이언트간에 세션키 교환 및 클라이언트 프로파일 정보 생성
5. 클라이언트 시스템에 프로파일 정보 저장하고, 패치 관리 서버에 클라이언트 프로파일 정보 전송
6. 패치 관리 서버는 패치 DB안의 시스템 정보 및 프로파일 정보를 조사하여 갱신 또는 생성
7. 패치 관리 서버는 저장된 프로파일을 확인하여 패치 DB 안에 업데이트 할 패치가 존재하는지 조사
8. 업데이트가 필요한 패치를 패치 DB로부터 획득하여 클라이언트에 전송
9. 클라이언트는 패치를 다운로드 후 설치
10. 클라이언트 프로파일 정보 갱신 및 저장
11. 패치 관리 서버에 프로파일 정보 전송
12. 패치 관리 서버는 패치 DB의 프로파일 정보 갱신

나. 클라이언트가 패치 분배 및 설치를 요구하는 경우
1. 패치 검색을 위한 스케줄링 설정 및 수행
2. 스케줄링에 의해 패치 관리 서버에 접속
3. 패치 관리 서버와 클라이언트간의 상호 인증 수행
4. 패치 DB 안에 업데이트 할 패치가 존재하는지 조사
5. 클라이언트가 패치 관리 서버에 신규 접속한 경우의 7~12 와 동일

다. 패치 서버가 클라이언트에게 패치를 분배하는 경우
1. 벤더에서 제공한 새로운 패치를 패치 DB에 저장
2. 패치 DB에서 해당 패치가 필요한 클라이언트 시스템 정보 및 프로파일 정보 검색
3. 패치 관리 서버와 해당 클라이언트들간의 상호인증
4. 패치 DB 안에 업데이트 할 패치가 존재하는지 조사
5. 클라이언트가 패치 관리 서버에 신규 접속한 경우의 7~12 와 동일

라. 클라이언트 시스템 설정이 변경된 경우
1. 패치 관리 서버 웹브라우저에 신규 접속
2. 클라이언트 에이전트 프로그램 다운로드 및 설치
3. 클라이언트 시스템 정보조사 및 패치 설치 정보검색
4. 패치 관리 서버 접속 및 상호인증
5. 패치 관리 서버와 클라이언트간의 세션키 교환
6. 클라이언트에 프로파일 저장 및 패치 관리 서버에 전송
7. 패치 DB 내의 시스템 정보 및 프로파일 정보 조사 및 갱신
8. 클라이언트가 패치 관리 서버에 신규 접속한 경우의 7~12 와 동일

3.2 기능 설계

가. 인증 및 패치 파일에 대한 기밀성 및 무결성 제공

패치 관리 서버와 클라이언트 사이의 신뢰할 수 있는 통신 채널을 설정함과 동시에 세션키를 분배하기 위하여 사용된다. 이때, 인증서 기반의 Diffie-Hellman 키 설정 프로토콜을 사용하여 사용자 인증과 키 분배의 신뢰성을 확립한다. 패치 관리 서버에 등록된 클라이언트 시스템에서 패치를 요구할 경우에 사용자 인증을 수행한다. 이 경우 패치 관리 서버와 클라이언트 사이의 상호인증은 패치를 요구하는 클라이언트에서 생성된 랜덤넘버 값을 Diffie-Hellman 키 교환에 의하여 생성된 세션키로 암·복호화 함으로서 상호인증을 수행한다.

패치 파일에 대한 기밀성 제공은 사용자 인증과정에서 Diffie-Hellman 키 교환을 통해 분배된 128bit 세션키를 이용한 암·복호화를 통해 제공된다. 또한, 패치 파일에 대한 무결성 제공을 위해서 패치 파일이 패치 DB에 저장되는 과정에서 패치 파일에 대한 MD5 체크섬을 계산하여 이 값을 다시 패치 관리 서버가 서명하는 방법을 사용한다.

나. 클라이언트 그룹화

제안하는 패치 관리 시스템은 중앙의 패치 관리 서버가 여러 대의 클라이언트들에 대한 보안관리를 중앙집중화 방식으로 수행하는 것이다. 대규모 네트워크를 대상으로 하여 클라이언트의 개수가 증가하게 되면 중앙의 패치 관리 서버에 부하가 심해져 제 기능을 수행하지 못하는 상황이 발생할 수 있다. 또한, 벤더로부터 새로운 패치를 다운로드 해 오면 해당 운영체제와 버전을 사용하는 클라이언트들에 대해서만 선별하여 분배하고 설치할 필요가 있다. 이러한 문제점을 해결할 수 있는 방안은 클라이언트의 그룹화 기법이다.

우선 본 논문에서 제시하는 시스템은 Windows, UNIX, Linux 운영체제를 대상으로 함으로 이상의 세 가지 운영체제

별로 클라이언트를 그룹화 하여 관리할 수 있다. 새로운 패치가 나오면 해당하는 운영체제를 사용하는 클라이언트들에 대해서만 연결을 설정하고 패치를 분배 및 설치한다. 운영체제 외에도 IP 대역별, 시스템의 중요도 및 설치위치 등에 대한 그룹화도 가능하다.

다. 패치 프로파일

패치 자동 관리 시스템에서 클라이언트 시스템들을 관리하고, 패치 자동분배 및 설치에 사용되는 패치 프로파일을 정의한다. 보안패치 프로파일은 에이전트 설치 시 기본 설정을 제외한 모든 것이 자동 생성되며, 관리자가 사용자 인증 과정을 통하여 직접 수정 가능하다.

- 클라이언트 관리 프로파일

클라이언트 관리 사용자의 정보를 구성한다. 패치 관리 시스템에 접근시 사용되는 사용자 ID, 사용자정보(이름, 직위, e-mail, 연락처 등)를 포함한다.

- 클라이언트 환경 정보 프로파일

관리 대상 클라이언트들에 대한 정보를 구성한다. 관리 사용자 ID, 클라이언트 시스템 번호, 클라이언트 MAC 주소, 클라이언트 IP 주소, 클라이언트 운영체제 종류, 클라이언트 운영체제 버전, 최근 프로그램 설치 날짜 등의 정보를 포함한다.

- 클라이언트 패치 정보 프로파일

클라이언트에 설치되어 있는 패치들의 정보를 구성한다. 클라이언트에 설치된 패치 리스트, 패치 MD4SUM 값, 최근 패치 설치 날짜 등의 정보를 포함한다.

- 클라이언트 프로그램 정보 프로파일

클라이언트 시스템에 설치된 프로그램 정보를 구성한다. 클라이언트에 설치된 프로그램 리스트, 패치 MD5SUM 값, 최근 프로그램 패치 설치 날짜 등의 정보를 포함한다.

- 그룹 리스트 프로파일

패치를 효율적으로 분배하기 위하여 사용되는 그룹화에 사용되는 정보를 구성한다. 그룹 리스트, 그룹 구성원 IP 주소, 그룹 루트 클라이언트, 그룹명 등의 정보를 포함한다.

라. 패치 관리 DB

패치 관리 DB는 서버 DB와 패치 DB로 구성된다. 서버 DB는 클라이언트 관리 프로파일과 클라이언트 환경 정보 프로파일, 그룹 리스트 프로파일을 구성한다. 즉, 서버 DB는 Admin_Tabel, Client_User_Table, Client_Host_Table, Group_Table로 구성된다.

패치 DB는 클라이언트 패치 정보 프로파일과 클라이언트 프로그램 정보 프로파일로 구성된다. 즉, Window_Table, Solaris_Table, Linux_Table로 구성된다.

마. 패치 설치

각 에이전트는 패치 관리 서버로부터 패치 파일을 수신하여 128bit MD5SUM 값을 이용하여 무결성을 체크하고, 패치 파일에 대하여 각 운영체제 별로 설치를 수행한다.

- UNIX(Solaris) 패치 설치

패치 관리 서버로부터 수신한 zip 형태의 패치 파일을 unzip 명령을 이용하여 자동으로 압축을 풀고, patchadd 명령을 이용하여 패치를 설치한다.

- Linux(Redhat) 패치 설치

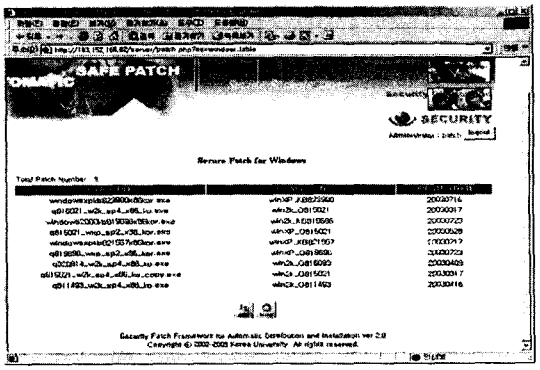
패치 관리 서버로부터 수신한 rpm 형태의 업데이트용 패키지를 rpm 명령을 이용하여 업데이트 시킨다.

- Windows 패치 설치

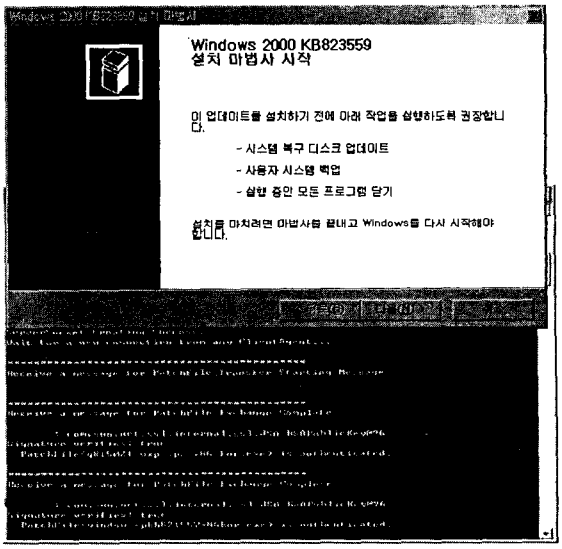
패치 관리 서버로부터 수신한 exe 형태의 패치 파일을 실행시켜서 패치를 설치한다.

3.3 구현 및 시험

기능 설계된 내용에 대한 구현을 통하여 다음과 같이 멀티플랫폼에 대한 패치 자동관리 시스템이 정상 작동함을 확인하였다.



[그림 2] 새로운 패치 등록



[그림 3] 클라이언트에서 체크섬 검사 후 설치

4. 결론 및 향후 연구 방향

본 논문에서는 멀티플랫폼을 지원하는 패치 자동관리 시스템을 제안하였다. 제안하는 시스템은 패치 분배시에 발생할 수 있는 보안 문제점을 해결하며, 대규모 네트워크 내의 클라이언트 시스템들에 대한 패치 관리를 자동으로 수행 가능하다. 클라이언트 시스템들에 대한 패치의 실시간적인 자동 설치를 통하여 시스템 보안을 향상시킬 수 있다.

향후에는 개발된 시스템에 대한 안정화 작업이 필요하다.

5. 참고문헌

[1] Sohn Tae-Shik, Moon Jong-Sub, Seo Jung-Taek, Im Eul-Kyu, Lee Cheol-Won, "Safe Patch Distribution Architecture in Intranet Environments", SAM, 2003

[2] Cheol-Won Lee, Eul Gyu Im, Jung-Taek Seo, Tae-Shik Sohn, Jong-Sub Moon, Dong-Kyu Kim, "A Secure Patch Distribution Architecture", ISDA 2003

[3] 손태식외 "안전한 패치 분배 구조 설계", 한국정보과학회 추계학술발표회, 2002. 10.

[4] 서정택외 "안전한 패치 자동분배 및 설치기법", the 13th JCCI, 2003