멀티플랫폼 환경에서의 보안패치 분배를 위한 DB구축 및 검색 방법에 관한 연구

이상원[O] *, 김윤주*, 문종섭*, 서정택**
고려대학교 정보보호대학원*, 국가보안기술연구소**
{a770720[O], zzuya99, jsmoon}*@korea.ac.kr, {seojt}**@etri.re.kr

A Study on the DB Construction and the Searching for distributing the Multi-Platform Based Automatic Distribution Method of Security Patches

Sang-Won Lee[O*], Yun-Ju Kim*, Jong-Sub Moon*, Jung-Taek Seo**
Center for Information Security Technologies (CIST), Korea University*,
National Security Research Institute**

요 약

패치 분배는 시스템의 보안과 네트워크를 구성하는 여러 시스템들에 설치된 소프트웨워의 취약성을 보완하기 위한 가장 중요한 요소 중의 하나이다.[4] 최근 다수의 보안패치 분배 시스템이 나타나면서 이들에 대한 선별 기준에서 충족시켜야만 하는 필수 조건으로서 이종 컴퓨팅 환경과 다중 플랫폼, 운영체제, 버전의 지원여부가 중요하게 여겨지고 있다.[5,6] 본 논문에서는 이러한 필수 조건들을 충족시킬 수 있는 보안패치 분배 시스템을 설계 및 구현하는데 필요한 보안패치 DB 구축 및 검색 방법을 연구, 제시하고자 한다.

1. 서 론

최근 새로운 취약점들을 보완하기 위한 패치들이 많이 나오고 있기 때문에 단순히 수동적인 방법으로는 대규모 네트워크를 구축하고 있는 기업체를 비롯한 관공서, 대학 등에서는 시스템의 결함들을 제대로 제거할 수 없다. 따라서, 이러한 과정들을 보다 체계적인 방법으로 자동화 시켜놓은 보안패치 분배 시스템이 필요하다.[1,2,3]

이러한 필요성에 의해서 많은 보안패치 분배 시스템이 개발되고 있는 실정이지만 멀티플랫폼 환경을 지원하고 있는 시스템은 거의 전무한 실정이다. 그러나, 실제로 보안패치 분배 및 설치의 대상이 되는 네트워크는 상이한 여러 시스템들로 구성되어 있기 때문에 보안패치 분배 시스템은 필수적으로 멀티플랫폼 환경을 지원할 수 있어야만 한다.

본 논문에서는 이러한 멀티플랫폼 환경(Windows, Solaris, Linux)에서의 보안패치 분배 시스템을 설계하는데 필요한 DB 구축 및 검색에 관한 방안을 제안하고 해당 시스템을 구현하고자 한다.

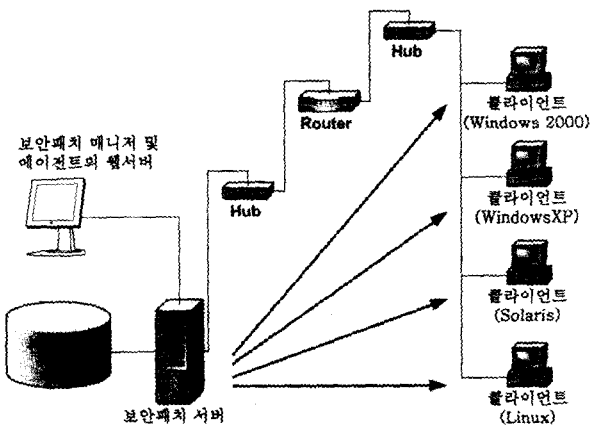

그림 1 보안패치 분배 시스템 전체 구조

2. 보안패치 분배 시스템 구조

2.1 전체 시스템 구조[3,4]

① 보안패치 매니저 : 보안패치 분배서버, 보안패치 DB 그리고 보안패치 프로파일에 대한 관리 기능을 수행하며 웹 기반의 사용자 인터페이스를 제공
② 보안패치 분배 서버 : 클라이언트와 보안패치 프로파일에 기반한 분배 메커니즘을 사용하여 실제 패치 분배 과정을 수행
③ 보안패치 DB : 보안 도메인 내에 구성되어 있는 클라이언트에 필요한 보안패치 파일 및 관련 정보를 저장하여 보안패치 분배 과정에서 보안패치 분배 서버의 요청에 의해서 보안패치를 제공
④ 보안패치 에이전트 : 보안패치 클라이언트와 보안패치 프로파일 정보에 대한 관리 기능을 수행하며 보안패치 에이전트는 웹 기반의 사용자 인터페이스를 제공
⑤ 보안패치 클라이언트 : 패치 분배 서버와 보안패치 프로파일에 기반한 분배 메커니즘을 사용하여 실제 보안패치 분배 과정을 수행

2.2 프로파일 구조

- 프로파일의 구조는 표1과 같다.[4]

표 2 프로파일 구조

프로파일 필드명	필드 설명
system_name	해당 시스템의 이름
user_id	사용자의 ID
os_type	운영체제의 종류
os_version	운영체제 버전 정보
ip_addr	IP 주소
mac_addr	MAC 주소
patch_number	현재 설치된 patch 의 개수
patch_list	설치된 패치 목록의 정보

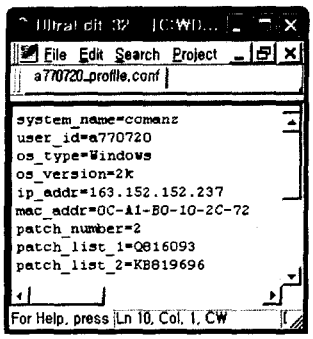

그림 2
Windows 프로파일 예제

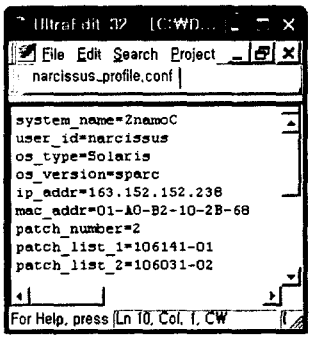

그림 3
Solaris 프로파일 예제

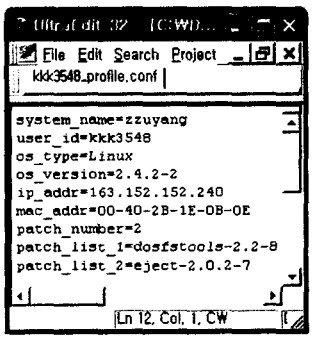

그림 4
Linux 프로파일 예제

표 3 보안패치DB 구조

보안패치DB 필드명	필드 설명
patch_target	보안패치 대상 파일 이름/버전
patch_path	보안패치 파일의 경로
patch_checksum	보안패치 체크섬 서명값
patch_update_date	마지막 업데이트 날짜

3. 보안패치 DB 구축 및 검색

3.1 보안패치DB 구조 : 보안패치DB 구조는 표2와 같다.

3.2 보안패치DB 필드 작성법

3.2.1 Windows 시스템 보안패치 필드 작성법

- patch_target 필드의 경우
  ① windows 시스템을 위한 보안패치임을 알 수 있도록 제일 앞에 "win"이라는 키워드를 넣는다.
  ② 해당 보안패치 파일이 적용될 수 있는 운영체제 버전 정보를 두 글자로 축약하여 넣는다.

표 4 보안패치 적용 대상 운영체제 버전 정보 삽입 방법

적용 대상 운영체제 버전	보안패치DB 키워드
Microsoft Windows 95	95
Microsoft Windows 98	98
Microsoft Windows Me	Me
Microsoft Windows 2000	2k
Microsoft Windows XP	XP

  ③ 필드를 파싱하기 쉽도록 "_"를 삽입한다.
  ④ 보안패치 정보를 삽입한다.

- 나머지 필드의 경우 : 특이 사항 없음

3.2.2 Solaris 시스템 보안패치 필드 작성법

- patch_target 필드의 경우
  ① Solaris 시스템을 위한 보안패치임을 알 수 있도록 제일 앞에 "Solaris"라는 키워드를 넣는다.
  ② 해당 보안패치 파일이 적용될 수 있는 벤더 정보를 넣는다. (SPARC 또는 Intel)
  ③ 해당 보안패치 파일이 적용될 수 있는 운영체제 버전 정보를 넣는다.
  ④ 필드를 파싱하기 쉽도록 "_"를 삽입한다.
  ⑤ 보안패치 정보를 삽입한다.

- 나머지 필드의 경우 : 특이 사항 없음

3.2.3 Linux 시스템 보안패치 필드 작성법

- patch_target 필드의 경우
  ① Linux 시스템을 위한 보안패치임을 알 수 있도록 제일 앞에 "Linux"라는 키워드를 넣는다.
  ② 해당 보안패치 파일이 적용될 수 있는 운영체제 버전 정보를 넣는다.
  ③ 필드를 파싱하기 쉽도록 "_"를 삽입한다.
  ④ 보안패치 정보를 삽입한다.

- 나머지 필드의 경우 : 특이 사항 없음

win2k_KB150383	/windows/KB150383.exe	cd5a36c6343cd3176	20040111
win9598_Q019327	/windows/Q019327.exe	6f3be31a237845972	20040123
win98ME_Q049375	/windows/Q049375.exe	be28309976a9b1807	20040217
win2kXP_Q112252	/windows/Q112252.exe	e4995ac4b722f3e532	20040228
SolarisSparc8_111517-01	/solaris/111517-01.zip	dd5c4c32b6d66070c	20040118
SolarisSparc8_125384-03	/solaris/125384-03.zip	405f16f3be31a23784	20040129
SolarisSparc8_101432-02	/solaris/101432-02.zip	b722f3e53566e4dcd	20040220
Linux2.4.2-2_apache-1.3.2-1.i386	/linux/apache-1.3.2-1.i386.rpm	31a2378459729f1b5	20040117
Linux2.4.2-2_dosfstools-2.2-8.i386	/linux/dosfstools-2.2-8.i386.rpm	6e4dcd1b07692e499	20040121
Linux2.4.2-2_glib-1.2.9-1.i386	/linux/glib-1.2.9-1.i386.rpm	2b6d66070c0cfbd47	20040203

그림 5 보안패치DB 필드 작성 예제

4. 보안패치 DB 검색

4.1 보안패치DB 검색 모듈 세부 흐름도

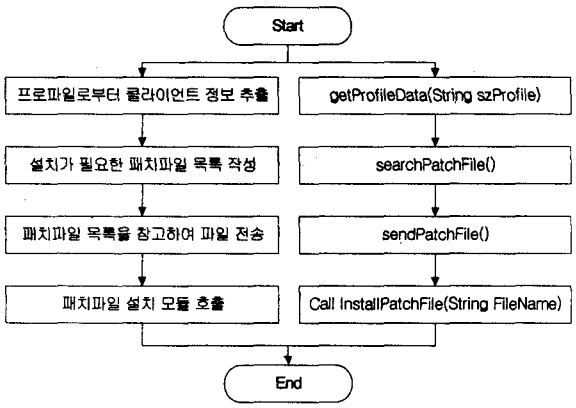

그림 6 세부 모듈 흐름도

4.2 설치해야 할 보안패치 파일 목록 작성 방법

① 설치해야하는 패치 파일 목록을 작성하기 위해서는 다음과 같은 정보가 필요하다.

- 운영체제의 종류 : Windows, Linux, Solaris
- 운영체제의 버전 : 95, 98, 2k (2000), XP, etc.
- 이미 설치된 패치 파일의 목록 : 클라이언트에서 생성한 프로파일로부터 정보를 가져온다.

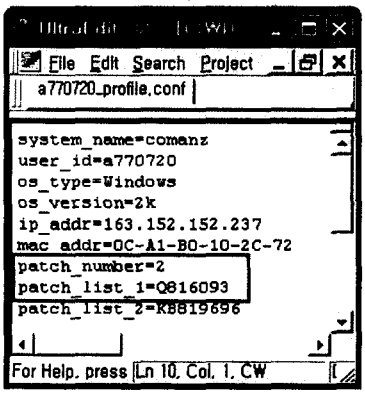

그림 7 설치된 패치 파일 목록

② 위의 정보를 바탕으로 다음과 같은 SQL쿼리문을 생성하여 DB 서버에 요청한다.

표 5 Windows 시스템에서의 SQL 쿼리문 예제

```
SELECT *
FROM patchDB_table
WHERE patch_target like "win%₩"
AND patch_target like "%XP%"
AND patch_target not like "%patch_list_[i]%"
```

- 검색 조건으로는 자신의 운영체제에 맞는 패치파일 목록으로 검색 범위를 줄이기 위해서 자신의 운영체제 버전 정보가 들어가고 (이 경우 'XP'), 마지막으로 자신이 설치한 패치파일은 설치할 필요가 없으므로 설치대상 목록에서 제거하기 위해서 not like 방식을 이용해서 프로파일에서 얻어낸 패치 파일 목록들을 대입한다.

③ 위의 SQL쿼리문 실행으로 얻어낸 보안패치 목록들의 index를 반환하여 해당 보안패치 파일들을 다운로드 받을 수 있도록 지원한다.

5. 결론

최근 보안패치 분배 시스템에 대한 관심이 증가하면서 많은 제품들이 우후죽순으로 나오고 있기 때문에 이를 활용하려는 기관 또는 업체들을 위해서 여러가지 보안패치 분배 시스템에 대한 선별 기준들이 나오고 있다.[5,6]

이러한 선별 기준에서 충족시켜야만 하는 필수 조건으로서 이종 컴퓨팅 환경과 다중 플랫폼, 운영체제, 버전의 지원여부를 들고 있다. 이것은 실제로 다양한 플랫폼을 사용하고 있는 클라이언트들이 모여서 하나의 네트워크 환경을 구축하고 있기 때문에 보안패치 분배 시스템이 반드시 갖추어야만 하는 필수조건일 수밖에 없다.

본 논문에서는 이러한 요구조건들을 충족시킬 수 있도록 하기 위해서 멀티플랫폼 환경에서의 보안패치 분배를 위한 DB 구축 및 검색 방식을 제안하였다.

추후에는 운영체제만을 대상으로 한 보안패치 분배 시스템이 아니라, 보안에 위협이 될 수 있는 다양한 응용 프로그램들에 대해서도 보안패치 파일 분배를 지원할 수 있도록 하기 위한 DB 구축 및 검색 방법에 관한 연구가 필요하다.

6. 참고문헌

[1] Sohn Tae-Shik, "Safe Patch Distribution Architecture in Intranet Environments", SAM, 2003

[2] Cheol-Won Lee, "A Secure Patch Distribution Architecture", ISDA 2003, Lecture Notes in Computer Science, Springer-Verlag, 2003

[3] LLNL, "Secure Software Distribution Architecture : SafePatch", Lawrence Livermore National Laboratory, May, 1999

[4] Tae-Shik Sohn, Jung-Woo Seo, Jong-Sub Moon, Jung-Taek Seo, Eul-Gyo Im, Cheol-won Lee, "Design and Implementation of a Secure Software Architecture for Security Patch Distribution", 한국정보보호학회, 2003

[5] Brad Carpenter , "Patch management: Find the weakest link", http://zdnet.com.com/2100-1107_2-5152602.html

[6] Network Computing, "패치 관리 툴 제품별 평가", NETWORK TIMES, 2003년 01월호