패치 파일 무결성 검증에 관한 연구

안정민, 원유재*
충남대학교 컴퓨터공학과
e-mail:jm_an@cnu.ac.kr

A Study on Verification of Patch File Integrity

Jeongmin An, Yoojae Won*
Dept of Computer Science and Engineering,
Chung-Nam National University

요 약

패치 관리 시스템은 패치 서버에 속한 에이전트들의 보안 패치를 배포 및 관리하는 시스템이다. 에이전트에서의 보안사고로 인한 큰 피해를 막기 위해, 패치 관리 시스템은 패치 파일의 무결성 및 안정성을 고려해야 한다. 소프트웨어 벤더는 모든 패치 에이전트 환경에 대해 패치 호환성을 고려할 수 없기 때문에 충돌로 인한 패치 적용 실패 시 충돌 원인 분석이 필요하다. 기존의 패치 관리 시스템은 테스트 환경에서 수동으로 패치 파일에 대한 무결성을 검증하고 있다. 본 논문에서는 파일 변화 모니터링을 통해 패치 테스트 및 적용 과정을 자동화하고, 변경 파일 정보를 통해 호환성 충돌 문제에 대한 분석 시간을 단축하는 방법을 제시한다.

1. 서론

최근 소프트웨어 취약점을 이용한 공격 발생 수는 증가하고 있지만, 취약점에 대한 패치가 발표되어도 다수의 PC가 모든 패치를 적용하도록 하는 것에는 어려움이 있다. 이를 위해 기업에서는 소프트웨어 벤더로부터 패치 파일을 수집하여 에이전트의 패치를 관리해주는 패치 관리 시스템(Patch Management System, PMS)을 이용하고 있다[1].

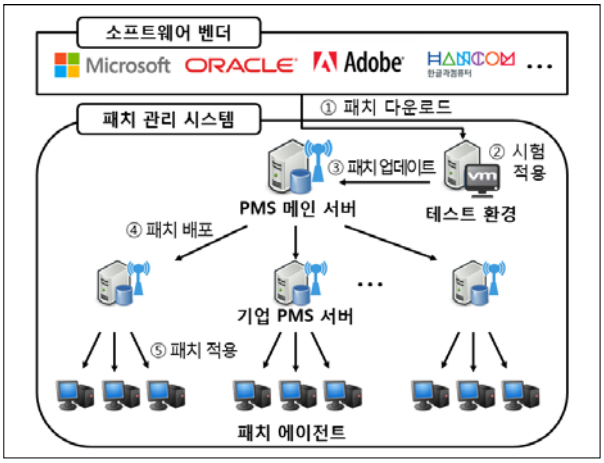
하지만, 패치 서버가 해킹되어 에이전트가 변조된 패치 파일을 내려받는 보안사고가 지속적으로 발생하고 있다. 2013년 3월 20일에는 방송·금융 6개사의 하드디스크가 파괴되는 등 전산망이 마비되는 사고가 발생하였다. 3·20 전산망 마비 사태는 바이러스에 감염된 PC를 통해 백신 서버에 원격 접속하여 백신 서버의 업데이트 파일에 바이러스를 삽입하였고, 변조된 파일을 내려받은 에이전트들은 바이러스에 감염되었다[2].

2016년 3월에는 인증서를 관리하는 에이전트 PC가 서버의 변조된 파일을 내려받아 악성코드에 감염되었다. 이로 인해 해당 에이전트 PC에서 관리하는 인증서들이 유출되었고, 유출된 인증서를 통해 서명된 데이터의 무결성을 위협하는 문제가 발생하였다.

본 논문에서는 이러한 문제를 해결하기 위해 기존에 패치 담당자가 수작업으로 무결성을 검증하는 테스트 과정을 자동화하고, 패치 에이전트에서 발생할 수 있는 호환성 충돌 문제의 원인 분석 시간을 단축할 수는 방법을 제안한다.

2. 기존 패치 관리 시스템

패치 관리 시스템은 서버-에이전트 구조에서 각 소프트웨어 벤더로부터 패치 파일을 수집하여 기업 내 패치 관리를 수행하는 시스템이다. 일반적인 패치 관리 시스템의 구성요소와 패치 수집부터 적용까지의 과정은 (그림 1)과 같다.



(그림 1) 패치 관리 시스템의 구성요소 및 패치 과정

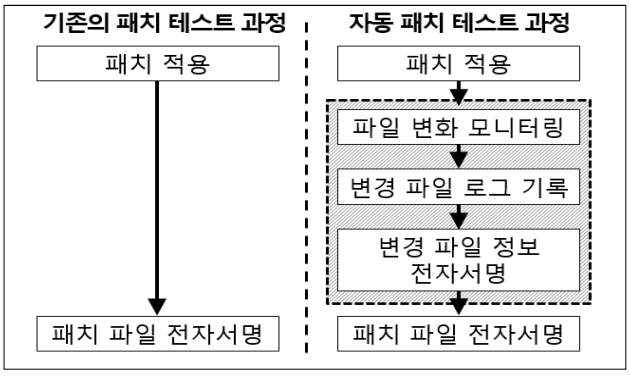
소프트웨어 벤더가 패치 파일을 배포하면 패치 관리 시스템은 패치 담당자에게 이메일 알림을 전송하고, 패치 파일을 수집한다[3]. 기업에서의 패치 적용 시, 에이전트에서의 보안사고를 방지하기 위해 파일의 무결성 검증을 수행해야 한다[4]. 패치 담당자는 패치 파일의 무결성 검증을 위해 신규 패치가 배포될 때마다 테스트 환경에서 패

* 교신저자

치 파일을 수동으로 적용하고, 패치가 정상적으로 종료되면 패치 파일에 전자서명하여 각 기업 PMS 서버에 배포한다. 하지만, 소프트웨어 벤더가 모든 기업 내 에이전트 환경의 패치 호환성을 고려하는 것은 어려움이 있다. 따라서 에이전트의 패치 호환성 충돌 시 문제를 해결하기 위한 분석 과정이 필요하다.

3. 변경 파일 정보를 이용한 무결성 자동 검증 방법

새로운 보안 패치가 공고되면 패치 관리 시스템은 패치 파일을 다운로드하여 테스트 환경의 PC에 설치한다. 테스트 환경의 PC는 패치 파일을 다운로드하는 경로를 지정하여 파일 생성 이벤트를 모니터링한다. 파일 생성 이벤트를 발생되면, 패치 적용 전 해당 패치와 관련된 소프트웨어 폴더의 파일 정보를 저장한다. 기존 파일 정보를 저장한 후, 패치를 적용하면서 파일 변화를 모니터링한다. 제안하는 패치 테스트 과정은 (그림 2) 와 같다.



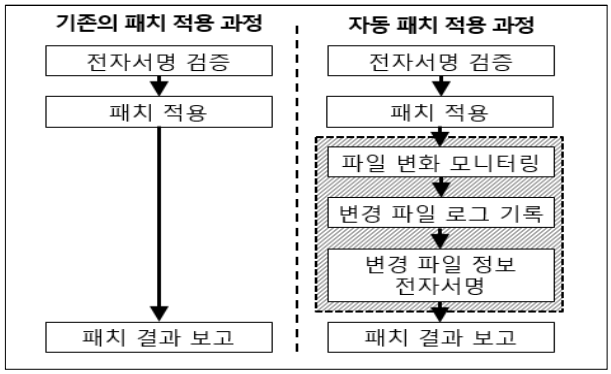
(그림 2) 테스트 환경에서의 자동 패치 테스트 과정

해당 패치가 적용되는 폴더의 파일 생성, 변경, 삭제 이벤트를 실시간 모니터링하여 변경 파일 정보를 순차적으로 기록한다. 정상적으로 패치가 적용되면 패치 파일에 전자서명하고, 모니터링을 통해 수집한 <표 1> 의 정보들에 PMS 메인 서버가 전자서명한다. 서명이 완료되면 서명된 패치 파일 및 변경 파일 정보를 각 기업의 PMS 서버로 전송한다.

<표 1> 테스트 환경에서의 수집하는 패치 관련 정보

수집 정보	설 명
패치 파일명	PMS 서버로부터 내려 받은 패치 파일에 대한 무결성 검증 정보로 이용
패치 파일 크기	
패치 파일 해시값	
변경된 파일명	패치 진행과정에서 호환성 충돌 발생으로 인해 패치가 중단된 경우, 충돌이 발생한 패치 시점을 패치 담당자에게 제공
변경된 파일 경로명	
변경된 파일 크기	
변경된 파일 해시값	

기업 PMS 서버는 서명된 패치 파일 및 정보들의 전자서명 유효성을 검사한다. 서명이 유효한 경우, 패치 파일과 관련 정보에 기업 PMS 서버가 재서명하여 에이전트에게 배포한다. 에이전트는 수신한 패치 파일과 패치 정보의 서명이 유효한 경우, (그림 3) 과 같이 패치를 적용한다.



(그림 3) 패치 에이전트에서의 패치 적용 과정

패치를 적용하면서, 파일 변화 모니터링을 통해 변경 파일 정보를 기록하고, 패치가 정상 종료되면 수신한 변경 파일 정보와 비교한다. 변경 파일 정보가 일치하는 경우, 기업 PMS 서버로 패치 적용 결과를 보고한다. 소프트웨어 호환성 충돌로 패치가 중단되는 경우, 에이전트의 변경 파일 정보와 기업 PMS 서버로부터 수신한 패치 파일 정보를 에이전트가 전자서명하여 기업 PMS 서버로 전송한다. 기업 PMS 서버는 충돌이 발생한 에이전트의 변경 파일 정보와 정상 패치 시 변경되는 파일 정보와 비교하여 호환성 충돌이 발생한 시점을 찾아낼 수 있다.

4. 결론

실제 기업 내 에이전트에서의 보안사고는 큰 피해를 초래하기 때문에 사전 예방과 신속한 대처가 중요하다. 본 논문에서 제안하는 무결성 검증 방법은 신규 패치 발표 시, 패치 담당자가 수동으로 테스트하는 과정을 자동화하여 효율적인 인력 분배를 가능하게 한다. 또한, 소프트웨어 벤더에서 고려하지 못한 기업 내 패치 에이전트 환경의 패치 호환성 충돌 발생 시, 충돌 시점을 제공하여 원인 분석에 시간을 단축할 수 있다. 패치 파일과 패치 정보를 함께 서명하고 제공하여 무결성 검증 절차를 강화하고, 호환성 충돌에 대한 문제 해결 시간을 단축하여 기존의 PMS보다 안정된 패치 관리를 기대할 수 있다.

감사의 글

본 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임.
(No.B0717-16-0099, IoT 보안 취약점 검색·공유 및 시험 기술 개발)

참고문헌

[1] Secunia, “Secunia Vulnerability Review 2015”, March, 2015
[2] KISA, “국내 주요 인터넷 사고 경험을 통해 본 침해사고 현황”, October, 2013
[3] Zhao, Duanyang, "The Research on a Patch Management System for Enterprise Vulnerability Update", ICIE'09. WASE International Conference on Vol. 2, p.250-253, 2009.
[4] NIST.SP.800-40r3 “Guide to Enterprise Patch Management Technologies”, July 2013