[5B-37]

멀티플랫폼 환경을 지원하는 계층적 패치관리시스템 연구

서정택, 박응기, 문종섭*
국가보안기술연구소, 고려대학교 정보보호대학원
{seojt, ekpark}@etri.re.kr, jsmoon@korea.ac.kr

A Study of Hierarchical Patch Management System Supporting Multi-Platform Environment

Jung-Taek Seo, Eung-Ki Park, and Jongsub Moon*
NSRI, *Korea University

요 약

운영체제 및 응용프로그램들은 프로그램 개발 과정의 특성상 보안 취약성을 가지고 있다. 최근 이러한 취약성을 악용하는 침해사례가 증가하고 있으며, 그 피해의 파급효과가 더욱 커지고 있다. 패치의 분배 및 설치는 취약성을 이용하는 침해사고를 예방하기 위한 가장 중요한 요소 중의 하나이다. 특정 기관이나 조직은 다양한 운영체제 및 응용프로그램을 사용하기 때문에 관리자가 매번 신속하게 모든 시스템들에 대하여 패치를 설치하기는 어려움이 있다. 본 논문에서는 중앙의 관리자가 패치관리서버를 이용하여 Windows, Linux, Solaris 클라이언트 시스템들에 대하여 안전하게 패치를 자동분배하고 설치하는 패치 자동관리시스템을 설계 및 구현하였다. 또한, 대규모 네트워크를 지원하기 위하여 확장성을 고려한 계층적인 패치 분배 구조로 설계 및 구현하였다.

1. 서론

일반적으로 모든 운영체제 및 응용 프로그램들은 프로그램 개발 과정의 특성상 보안 취약성을 가지고 있다. 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.[1].

하지만 시스템 관리자들이 패치 일일이 해당 사이트에 가서 패치를 다운받아야 부분과, 관리하고 있는 시스템이 이기종이고 그 수가 많은 경우에 효과적인 패치 관리에 어려움이 있다. 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 패치 서버 프로그램이 각 벤더들로부터 패치를 다운받아 DB에 저장하고, 프로파일 관리기법을 이용하여 해당 패치를 필요로 하는 클라이언트시스템들을 선별하여 패치를 자동으로 분배하고, 설치하는 중앙 집중화된 보안패치관리시스템을 설계 및 구현한다.. 또한, 대규모네트워크를 지원하기 위해서 확장성을 고려하여 계층적인 패치 분배 구조로 설계 및 구현하였다.

2. 동향분석

효과적인 패치관리시스템의 설계 및 구현을 위하여 국내외 상용화 제품 세부 기능을 분석하고, 운영체제 벤더별로 패치 분배기술을 분석하였다. 아래의 [표 1]은 국·내외 패치관리시스템의 세부 기능을 분석한 표이다. 세부 기능을 살펴보면, 우선 제품에 따라 에이전트에 기반 한 제품이 있고, 그렇지 않은 제품이 있다. [4][5][6][7][8].

[표 1] 국내외 상용화 제품 세부기능 분석표

	본 연구	Patch Link	BigFix	Shavlik	Gravity Strom	Inciter	TCO Stream
Agent Based	0	0	0	x	x	x	0
Hierarchical Distribution	0	x	x	x	x	x	x
Multi platform	0	0	0	x	x	x	x
Client scanning	0	0	0	x	x	x	0
Secure Transfer	0	0	0	x	x	x	x
Patch support for user *application*	0	0	0	0	0	0	0
Group	0	0	x	x	0	x	x
Patch file Encryption	0	0	0	0	0	x	0

에이전트에 기반 하지 않는 시스템의 경우 에이전트를 배포하지 않아도 되므로, 배포가 용이하지만, 반면에 대상 시스템의 정보를 얻기 위해서는 직접적으로 네트워크를 통해 분석을 해야 하므로, 네트워크 트래픽이 많이 발생하는 단점이 있다. 본 연구에서는 배포의 편리성 보다는 정보 수집 및 네트워크 부하를 고려하여 에이전트 기반의 패치관리시스템으로 설계 및 구현하였다.

국·내외 상용 제품의 경우 하나의 패치분배 서버가 다수의 클라이언트들에 대하여 패치를 분배하고 있다. 이는 대규모 네트워크에 대한 지원이 어려우며, 패치 분배 시 과부하가 발생할 수 있는 문제점을 가지고 있다. 따라서, 본 연구에서는 확장성을 고려한 계층적