에이전트를 이용한 PC 보안 관제 시스템[1)]

김우년°, 노원섭, 이승우, 이종남, 강창구

니츠 정보보호연구소

PC Security Management Control System using Agent

Woo-nyon Kim, Won-seop Noh, Seung-woo Lee, Jong-nam Lee, Chang-goo Kang

Information Security Institute , NITZ

요 약

본 논문에서는 에이전트를 이용하여 개인용 컴퓨터의 보안성을 높이고, 중앙에서 PC 보안 정책을 조직 내에 일괄 적용하고 관리할 수 있는 PC 보안 관제 시스템의 개발에 대해서 설명한다. 에이전트는 각 PC에서 보안 정책을 적용하고 보안 로그를 수집하여 관제 시스템으로 전송하며, 관제 시스템은 이러한 정보를 기반으로 조직내의 PC 보안 정책을 일괄 적용할 수 있도록 지원한다. 에이전트를 이용한 PC 보안 관제 시스템은 에이전트에서 수집된 보안 로그를 이용하여 보안 정책을 조직에 알맞게 수립할 수 있으며, 수립된 조직의 정책이 조직내의 PC에 적용할 수 있고, 정책에 위배되는 사항을 실시간으로 확인할 수 있는 장점이 있다.

I. 서론

조직내에 있는 개인용 컴퓨터(PC)의 자료 유출을 방지하고 보안을 강화하기 위한 방법으로 개인용 컴퓨터 보안 시스템이 도입되었다[2]. 그러나 일반적인 사용자의 개인용 컴퓨터와 달리 조직내의 개인용 컴퓨터는 조직 내부의 보안 정책을 준수하고, 새로운 보안 정책을 수립할 수 있는 보안 로그 정보를 수집할 수 있도록 해야 한다[1]. 본 논문에서는 조직내의 개인용 컴퓨터의 보안성을 강화하고 조직내의 보안 정책 수립을 위한 보안 로그 데이터의 수집 및 분석, 조직내의 개인용 컴퓨터에서 조직의 정책을 적용할 수 있는 에이전트를 이용한 PC 보안 관제 시스템을 설명한다.

기존의 연구는 조직내의 다양한 보안 장비에 대한 로그 수집과 정책 수립을 지원하는 전사적 통합 보안 솔루션에 대한 연구가 많았다[3, 4, 5]. 본 논문에서는 조직내의 사람이 사용하는 PC 에 대한 보안 정책 및 보안 관리를 위한 영역을 중심으로 설명한다.

PC 보안 관제 시스템은 안전한 통신을 지원하고, PC의 다양한 이벤트를 수집/분석할 수 있어야하며, 조직의 보안 정책을 일괄 또는 특화되어 적용할 수 있어야 하며, 조직의 보안 정책이 유지되는지 확인할 수 있어야 한다. 또한, 정책이 위배되는 경우 이를 즉시 PC 보안 관제 서버에 통보하며, 보안사고 발생후 사후 처리를 위한 보안 로그 분석이 가능해야 한다. 본 논문에서는 이러한 사항들을 만족하기 위하여 에이전트 기술을 이용하여 보안 에이전트를 구성하였다. PC의 보안 에이전트는 PC 자체의 개별적인 보안을 처리하고, 보안 이벤트를 수집/분석하며, PC 보안 관제 서버의 정책이나 명령에 대응하도록 하였다. 또한 대규모 조직에 적용 가능하도록 복수 계층의 구조로 되어있다.

본 논문에서 제시하는 PC 보안 관제 시스템은 조직의 보안 정책을 일괄적으로 적용가능하고, 적용 상태를 확인할 수 있으며, 보안 에이전트에 의해 보안 정책 위배에 따른 정보를 실시간으로 PC 보안 관제 서버에 경보할 수 있는 장점이 있다.

2장에서는 PC 보안 관제 시스템의 동작 모델과 시스템 구조에 대해서 설명하고, 3장에서는 에이전트를 이용한 PC 보안 관제에 대해서 설명한다. 4장에서는 구현 결과에 대해서 설명하며 5장에는 결론이 있다.

II. PC 보안 관제 시스템 구조

본 논문에서 제안하는 시스템은 클라이언트/서버 구조를 가지며, 대규모 조직을 수용하기 위하여 복수 계층 구조를 가진다.

1. 동작 모델

PC 보안 관제 시스템의 동작 모델은 다음 그림과 같다.

1) 본 연구는 제2차 정보통신산업기술개발사업의 일환으로 연구되었음.

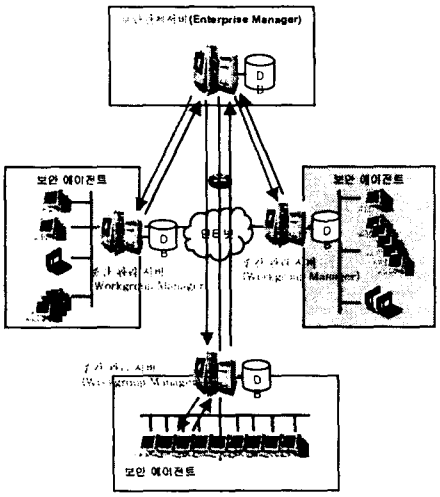

그림 1 동작모델

■ 보안관제(EM) 서버는 에이전트의 보안 정책을 설정하고 관리하며, 수집된 보안 로그를 분석하여 조직에 알맞은 보안 정책을 결정한다.

■ 중간관리(WM) 서버는 보안관제 서버의 역할을 분담하여 대규모 조직을 관리할 수 있도록 지원한다.

■ 보안 에이전트는 관제 서버에 의해 정해진 조직의 보안 정책을 적용하고, 보안 로그를 수집하여 보안 정책이 잘 적용될 수 있도록 한다.

2. 시스템 구조

에이전트를 이용한 PC 보안 관제 시스템의 구조는 그림 2와 같다.

보안관제 서버는 통신 처리부, 데이터베이스 처리부, 정책 관리, 로그 관리, WM 관리, 자산 관리, 에이전트 관리, 버전 관리, 통계/보고 모듈, 사용자 인터페이스 등의 모듈로 구성된다. 특히, 정책 관리와 로그 관리, 통계/보고 모듈은 조직내의 보아 정책을 생성하고 적용하는 중요한 모듈이다.

중간관리 서버는 대규모 네트워크 환경에서 보안관제 서버의 부하를 줄이는 역할을 수행하고, 관련 모듈은 보안 관제 서버와 같은 모듈로 구성된다.

보안 에이전트는 통신 처리부, 에이전트 처리부, 커널 처리부, 보안 처리부, 응용 처리부로 구성되며, 에이전트 처리부에서 필요한 보안 로그를 수집하고, 정책을 적용하는 역할을 수행한다.

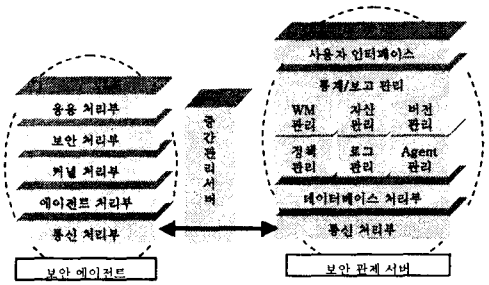

그림 2 시스템 구조

III. 에이전트를 이용한 PC 보안 관제

1. 보안 에이전트

보안 에이전트는 개별 PC에 설치되며, 개별적으로 PC에서 발생하는 보안 이벤트를 수집한다.

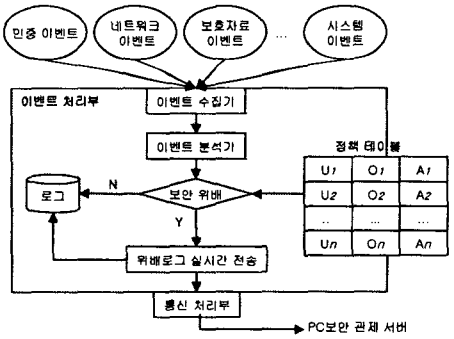

그림 3 보안 에이전트의 이벤트 처리

수집되는 보안 이벤트는 윈도우 로그온, 화면 보호기 인증 등의 인증과 관련된 이벤트, 네트워크와 관련된 이벤트, 보호된 자료에 대한 이벤트, 시스템 이벤트 등이 있다. 이벤트 수집에 의해서 수집된 보안 이벤트는 이벤트 분석기에 의해서 분석/분류되며, 설정된 보안 정책에 타당한지 검사한다. 설정된 보안 정책에 위배된 이벤트는 PC 보안 관제 서버로 즉시 전송하여 보안 위배가 발생하였음을 통보한다. 그림 3은 수집된 이벤트가 보안 에이전트에서 처리되는 과정을 설명한다.

보안 에이전트의 중요한 두 번째 역할은 PC 보안 관제 서버로부터 전송된 보안 정책을 PC에 적용하는 역할을 한다. 보안 에이전트의 정책 적용 규칙은 i) PC 보안 관제 서버에서 설정한 정책이 PC의 사용자가 설정한 정책보다 우선 적용되며, ii) PC 보안 관제 서버에서 정책을 명시적으로 해제하기 전까지는 지속적으로 적용되며, iii) 보안

정책이 위배된 이벤트는 로그를 남기고 실시간으로 보안 관제 서버에 통보한다.

2. PC 보안 관제

PC 보안 관제는 보안 에이전트에서 수집/분석된 로그를 에이전트로부터 수집하여 다양한 검색과 분석을 통해서 보안의 취약점이나 내부자 자료 유출과 같은 보안 사항을 검토할 수 있다. 또한, 보안사고가 발생한 후 수집된 보안 로그는 사고를 분석하기 위하여 이용 가능하다. PC 보안 관제는 관제 서버에서 보안 정책의 설정, 보안 로그 수집 등의 보안 명령을 내리면 명령을 암호화하여 중간관리 서버로 전송된다. 이때, 수신할 에이전트의 식별번호를 함께 전송하여 중간 관리 서버에서는 해당 보안 에이전트에 차례로 명령을 전달한다. 보안 에이전트는 수신한 명령을 복호하여 명령에 해당하는 작업을 수행하고 수행한 결과를 암호하여 중간관리 서버로 전송한다. 중간관리 서버는 수신된 결과를 수집하여 관제 서버로 전송하여 관리하게 된다. 이러한 과정을 통하여 조직 내부의 보안 정책이 올바르게 유지되고 있는지 확인하고, 새로운 보안 정책을 설정/유지할 수 있다. 실시간으로 전송된 보안 정책 위배 정보를 활용하여 각 에이전트에 알맞은 보안 정책을 새로이 설정할 수 있다.

IV. 구현

에이전트를 이용한 PC 보안 관제 시스템은 C++를 이용하여 개발되었으며, 데이터베이스는 MS SQL Server를 이용하였다. 네트워크는 윈도우 소켈을 이용했다.

그림 4는 보안관제 서버의 에이전트 정책을 설정하는 사용자 인터페이스이다. 특정 사용자에 또는 특정 부서에 대해서 필요한 정책을 설정할 수 있다. 또한 설정된 정책이 에이전트에 의한 적용 결과를 조회할 수 있다. 이러한 정책 조회는 특정 사용자 별로 검색 가능하다.

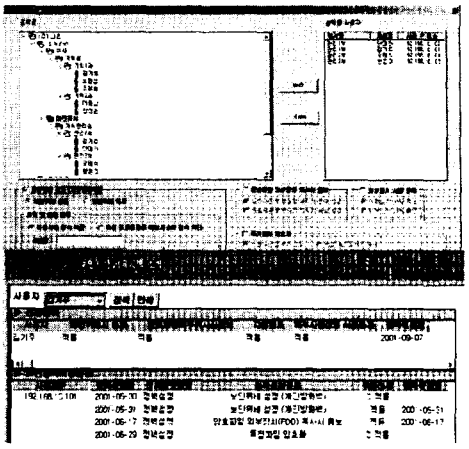

그림 4 보안 정책 설정 및 적용 결과 조회

그림 5는 설정된 보안 정책에 위배된 결과를 표시한다. 네트워크 접근 금지 설정이된 PC의 사용자가 특정 서버에 불법 접근한 경우 실시간 경고 메시지가 PC 보안 관제 서버로 전송되어 관리된다.

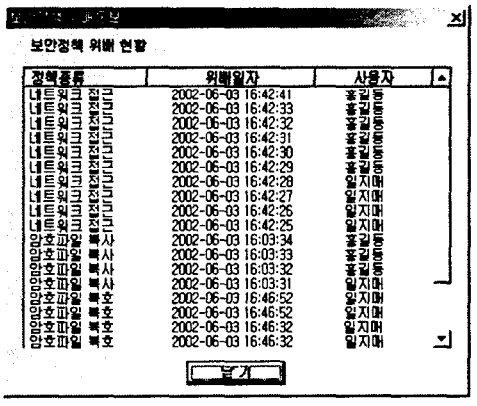

그림 5 보안 정책 위배 실시간 통보

그림 6은 보안 로그의 검색 결과 및 통계 결과이다. 로그의 검색은 특정 사용자별 검색을 지원하며, 통계는 그래프 형식으로 제공한다.

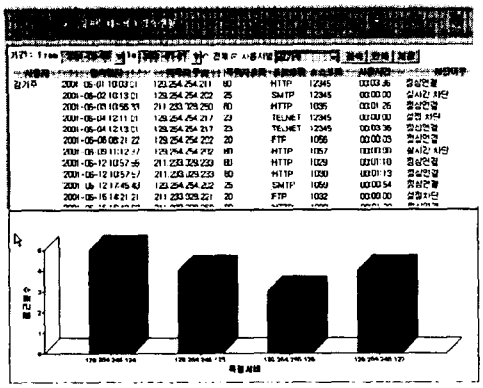

그림 6 로그 검색 및 통계

V. 결론

조직내의 보안 정책을 결정하고 보안 정책을 적용하기 위해서는, 조직 내부의 보안 로그를 수집/분석하여 조직내의 PC의 사용 유형을 분석해야하며, 이러한 분석을 통해서 유도된 보안 정책을 각 개인의 컴퓨터에 올바르게 적용을 해야한다. 본 논문에서는 대규모 조직내의 보안 정책을 설정하고, 적용하며 이를 통하여 조직내의 PC를 안전하게 관리/판제할 수 있는 PC 보안 관제 시스템에 대해서 설명했다.

에이전트를 이용한 PC 보안 관제 시스템은 조직의 보안 정책을 일괄 설정하고, 설정된 보안 정책을 개인용 컴퓨터에 실치된 보안 에이전트에 의해서 적용되도록 함으로써, 대규모 조직의 보안 정책을 설정/적용할 수 있도록 한다. 또한 보안 에이전트에 의해서 설정된 정책들이 감시되며, 위배된 사항에 대해서는 관제 서버로 즉시 통보되는 장점이 있다. 또한, 각 PC의 보안 로그를 수집해서 조직의 새로운 보안 정책에 반영될 수 있도록 정보를 제공한다.

앞으로의 연구는 각 개인 컴퓨터에 설치된 보안 에이전트가 다양한 이벤트를 수집/분석하여 사용자에게 특화된 보안 서비스를 제공하기 위한 연구를 수행해야 한다.

참고문헌

[1] 인젠, "ESM 현황과 발전방향," 제1회 사이버테리 정보전 컨퍼런스 2002, pp. 71-82, 2002년 3월.

[2] http://www.ahnlab.com/

[3] http://www.sccui.com/

[4] http://www.ffstek.com/

[5] http://www.haansecure.com/