전산망 보안관리 통합시스템에서의 피해 복구를 위한 에이전트 백업 매커니즘

송병욱°,박보석, 장희진, 김상욱
경북대학교 컴퓨터과학과
{bwsong, parkbs, janghj, swkim}@woorisol.knu.ac.kr

Agent Back-up Mechanism for Recovery under Integrated System for Computer Network Security

Byung-Wook Song°, Bo-Seok Park, Hee-Jin Jang, Sang-Wook Kim
Dept. of Computer Science, Kyungpook National University

요 약

인터넷에서의 보안 사고가 급증하게 되면서 여러 가지 보안 도구들이 소개되고 있으나, 보안상 완벽한 효과를 기대하기 어렵고 침입에 의한 자료 손실이 발생하였을 경우를 위한 대책은 전무한 상태이다. 본 논문은 보안관리 통합시스템의 에이전트들 간에 주기적인 백업을 수행하게 함으로써 침입자의 부정행위에 의한 자료 손실을 신뢰적으로 복구할 수 있는 메커니즘을 제시한다.

1. 서론

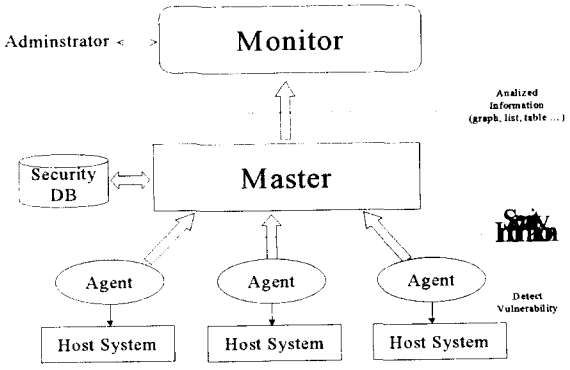
최근 인터넷의 사용이 보편화됨에 따라 부정행위에 위한 보안 사고가 급증하고 있다. 이에 따라 보안 강화를 위한 여러 가지 도구들이 소개되어 여러 가지 시스템에 적용되고 있으나, 기준으로 채택된 보안 사항들이 이미 공개되어 있고, 제품의 성능이나 기능이 빈약한 것이 많아 보안상의 완벽한 효과를 기대하기는 어렵다. 뿐만 아니라, 침입자의 부정행위에 의한 자료 손실에 대응하는 기술이 전무한 상태다. [1,3]

이에 본 논문은 전산망 보안관리 시스템에서의 효과적인 피해 복구를 위한 백업 메커니즘을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 전산망 보안관리 시스템의 구조와 마스터와 에이전트, 그리고 모니터의 역할을 설명하고, 3 장에서는 백업 메커니즘의 구조와 동작 규칙, 에이전트와 마스터의 관계와 역할에 대하여 알아본다. 그리고, 마지막으로 4 장에서 향후 연구과제를 제시하고 결론을 맺는다.

2. 전산망 보안관리 시스템

전산망 보안관리 통합시스템은 정보 시스템 침해방지 시스템에서 전산망 관리자에게 전산망 전체의 보안 사항들을 분석할 수 있도록 보안 정보를 나타내어 주는 시스템으로, 에이전트와 마스터로 구성된 클라이언트/서버 구조와 관리자를 위한 모니터 시스템으로 구성된다.



[그림 1] 전산망 보안관리 통합시스템

에이전트 시스템은 보안관리 마스터 시스템이 보안 정보를 수집, 분석하고자 하는 대상 시스템을 의미하며, 마스터 시스템에서 설정된 정책에 따라서 해당 시스템의 보안 정보를 수집, 분석하여 보안 관리 마스터 시스템에 보안 정보를 전송한다. 수집되는 항목은 시스템 정보, 사용자 정보, 그룹 정보, 파일 정보이다. 주요 기능으로는 마스터의 요청에 의한 점검 모듈의 활성, 실시간 정보를 마스터 시스템으로 콜백이 있다.

모니터 시스템은 에이전트로부터 보안정보를 전달 받아 이것을 분석하여 보안 상황 모니터 시스템으로 전송한다. 주요 기능으로는 수집 정보 저장 및 통계적 분석, 보안 정보 수집, 분석, 저장과 에이전트 시스템의 관리 등이 있다. 수집한 정기적인 보안 정보나 침입자 감시 시에 보내지는 메시지를 분석하고 통계적인 정보로 가공한다. 전산망 관리자가 발생하는 메시지를 분석하여 에이전트들에게 멀티케스팅한다.

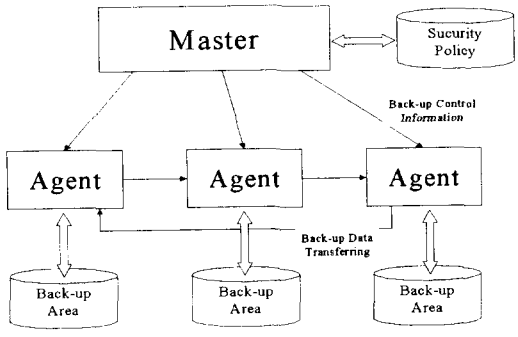
모니터 시스템은 분석, 정리된 시스템 및 네트워크 보안 정보와 취약성 정보들을 멀티미디어를 이용하여 프리젠테이션하는 역할을 수행한다. 그리고, 특정 보안 문제로 판단 시 경보 기능을 이용하여 전산망 관리자가 신속한 조치를 취하도록 한다. [1,2]

3. 에이전트 백업 메커니즘

에이전트 백업 메커니즘은 동일한 도메인에 포함되어 있는 에이전트들 사이에 서로의 백업 데이터를 확보해서 침입자의 부정행위에 의한 데이터 손실을 효과적으로 복구하기 위한 것이다.

3.1 구조

그림 2 와 같이 마스터에는 하나 이상의 에이전트가 연결되어 있는 트리 구조로 되어 있으며, 에이전트들은 원형 리스트 구조로 연결되어 서로 다음 에이전트에게 데이터를 백업하도록 되어 있다.



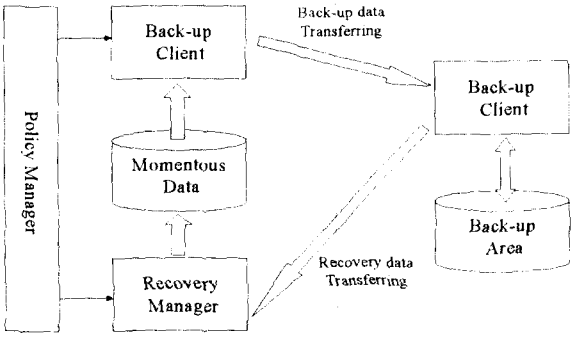
[그림 2] 에이전트 간의 연결 구조

에이전트가 추가되는 경우에는 마지막으로 추가된 에이전트의 백업을 받게 되고, 자신은 가장 처음 추가되었던 에이전트로 백업하게 된다. 이 때, 새로운 에이전트의 백업을 받게 되는 에이전트는 백업 영역을 초기화한다. 반대로, 에이전트가 제거되는 경우에는 자신에게 백업하고 있는 이전 에이전트가 자신이 백업했던 다음 에이전트에게 백업하도록 설정한다. 마찬가지로 이 때에도, 새로운 에이전트의 백업을 받게 되는 다음 에이전트의 백업 영역을 초기화한다.

3.2 동작 모델

그림 3 과 같이 에이전트 간의 백업은 백업 클라이언트와 백업 서버가 담당하게 된다. 백업 클라이언트는 보안 정책에 따라 주기적으로 백업 서버에 보호 자료를 전달한다. 그리고, 침입자의 부정행위에 의하여 보호 자료에 손실이 생겼을 경우, 리커버리 매니저는 백업 서버로부터 백업 자료를 받아서 호스트의 보호 자료를 복구하게 된다.

보호 자료는 마스터에 의하여 결정되는 일반 자료와 에이전트에 의하여 결정되는 특수 자료로 구성된다. 일반 자료는 동일한 도메인에 포함되어 있는 모든 에이전트가 공통적으로 보호해야 할 자료로, 호스트 시스템의 시스템 파일, 로그 파일, 사용자 정보 파일 등이 여기에 포함된다. 특수 자료는 에이전트에 따라 다르게 결정되는 자료로, 주로 개인 자료가 여기에 포함된다.



[그림 3] 백업 서버/클라이언트 구조

에이전트가 백업을 수행하기 전에는 반드시 침입 탐지 시스템의 의한 점검을 거쳐 보호 자료의 무결성을 검증받아야 한다. 만약, 침입자의 부정행위에 의하여 보호 자료의 무결성이 파괴되었다면 리커버리 매니저에 의하여 보호 자료는 가장 최근의 백업 자료로 복구됨으로써 다시 무결성을 확보하게 된다.

백업을 하는 주기는 보호 자료의 중요도와 크기에 따라 세가지 레벨로 구분된다. 첫번째 레벨은 중요도가 매우 높고 크기도 작은 보호 자료에 적용되는데, 에이전트의 작업을 실시간에 가깝게 백업한다. 두번째 레벨은 중요도와 크기에 있어 평이한 보호 자료에 적용되는데, 네트워크에 부담을 주지 않는 범위 내에서 이루어진다. 세번째 레벨은 크기가 매우 커 네트워크에 상당한 부담을 줄 것으로 예상되는 자료에 적용되는데, 주로 에이전트의 사용자가 가장 적은 시간대를 선택하여 하루에 한 번 정도 이루어진다. 백업 주기는 세가지 단계로 구분되긴 하지만, 각 단계별로 구체적인 시간 간격은 마스터의 보안 정책에 따라서 결정된다.

본 논문에서 제안한 백업 방식은 물리적으로 분리되어 있는 시스템 간에 이루어지기 때문에 필연적으로 네트워크를 사용하게 된다. 따라서, 보호 자료의 규모에 따라 네트워크의 부담이 커질 수 있고, 그에 따른 에이전트와 마스터 시스템의 성능을 저하시킬 수 도 있다. 이러한 문제를 해결하기 위하여, 에이전트는 백업을 하기 전에 보호 자료의 체크섬을 먼저 보내서 변경된 자료를 선별한 후, 갱신해야 할 보호 자료만을 백업한다.

마스터는 에이전트 간의 백업 관계, 보호 자료와 백업 주기 등을 결정하고, 자신이 관리하는 에이전트들 간의 백업 시간을 조정해서 원활한 백업이 이루어지도록 한다.

4. 결론 및 향후 연구

본 논문에서는 동일한 도메인에 포함되어 있는 에이전트들 간의 주기적인 백업을 통해 침입자의 부정행위에 의한 자료 손실을 효과적으로 복구할 수 있는 방법을 제안하였다.

향후 연구 과제로는 효율적인 자료 전송 프로토콜을 통한 네트워크의 부하를 줄이고, 에이전트들 간의 실시간 백업을 가능하게 하는 메커니즘의 개발이다.

5. 참고 문헌

[1] 김건우, 박보석, 장희진, 김상욱, "전산망 보안관리 통합시스템 개발에 대한 연구", 한국정보보호센터, p 25 - 31, 1998. 12.

[2] 김민수, 이형효, 김정순, 김인권, "멀티호스트 기반 침입탐지 시스템", 한국정보보호센터, p 15 - 18, 1998. 12.

[3] "유닉스 시스템 보안 취약성 분석 및 진단에 관한 연구", http://ncadl.nca.or.kr