산업보안을 위한 융합보안관제시스템에 관한 연구

하 옥 현*

요 약

현재 산업보안의 패러다임은 단순한 보안장비 설치에서 효율적인 운영·관리로 바뀌어 가고 있다. 물리적 보안시스템(출입통제시스템, 영상보안시스템 등)과 IT 통합보안관제시스템이 융합하면 기업의 위험관리 및 보안관리를 통하여 내부자의 정보유출을 획기적으로 예방, 차단하고, 사후 추적등을 가능케 해준다. 즉, 기존의 물리적 보안과 IT 보안인력의 추가적인 확충이 없어도 단시간 내에 체계적인 융합보안관리 프로세스 확립이 가능해져 전문 조직 체제를 상시 운영하는 효과를 기대할 수 있게 된다. 이제 개별 기술로 IT보안 및 물리보안 영역의 보안이벤트 수집 및 통합관리, 보안사고 발생시 사후 연계 추적 관리, 정보유출・보안위반 사항에 대한 패턴 정의 및 실시간 감시, 보안위반・정보유출 시도에 대한 신속한 판단 및 대응/조치, 단계적·체계적 보안정책 수립 및 융합보안의 통합보안관리체계 확립이 필요하다.

A Study on Conversion Security Control System for Industrial Security

Ok Hyun Ha*

ABSTRACT

Current paradigm of industrial security is changing into the effective operation and management from simple establishment of security equipments. If the physical security system(entry control system, video security system, etc.) and the IT integrated security control system are conversed, it makes us possible to prevent, disrupt and track afterwards the insider's information leakage through the risk and security management of enterprise. That is, Without the additional expansion of the existing physical security and IT security manpower, the establishment of systematic conversion security management process in a short time is possible and can be expected the effective operation of professional organization system at all times. Now it is needed to build up integrated security management system as an individual technique including the security event collection and integrated management, the post connected tracking management in the case of security accident, the pattern definition and real time observation of information leakage and security violation, the rapid judgement and response/measure to the attempt of information leakage and security violation, the establishment of security policy by stages and systematically and conversion security.

Key words : Industrial Security, Conversion Security

접수일 : 2009년 10월 5일; 채택일 : 2009년 12월 1일

* 호남대학교 경찰법행정학부

1. 서 론

지금까지 보안관제 시스템은 기존의 IT 보안 제품(IPS, Firewall, IDS 등)과 같은 단일 솔루션에 의한 방어 및 모니터링을 시작으로 위협관리시스템, 통합보안관제시스템등의 통합화 환경에 이르고 있다[1]. 하지만 기존 IT 보안 시스템은 기술유출 또는 산업보안에 관점에서는 비효율적인 구조를 가지고 있다. 기술 유출을 막기위해서는 내부 직원 또는 인적자원에 대한 감시나 모니터링이 필요한데, 이를 위해서는 사이버적 보안과 물리적 보안시스템(출입통제시스템, OA 시스템, 디지털영상보안시스템 등)의 융합의 필요성이 제기된다. 사이버적 보안과 물리적 보안에 관련된 이벤트를 정형화된 상관분석을 하게 되면 보다 적극적인 방어가 될 것이라고 판단되기 때문이다[2]. 기존에는 트래픽양과 보안이벤트를 여러가지 방법으로 상관분석하여 위험도를 자동화 했다면[3-5], 융합보안에서는 출입통제시스템에서의 각 사용자의 출입상황, 보안영역, 역할기반 등으로 이벤트를 나눌 수 있으며, OA 시스템에서도 복사매수, 시간 등으로 분석할 수 있을 것이다. 이러한 이벤트를 다양한 방법으로 상관분석하기 위해서는 자체 프로그래밍 언어로 보다 적극적인 분석이 필요하리라고 생각한다. 따라서 본 연구에서는 산업보안위험을 최소화하기 위한 노력의 일환으로 각각의 환경에서 이를 통합관리하여 관리 및 관제업무의 효율을 극대화할 수 있는 융합 보안관제가 가능한 통합보안관리 시스템의 개발을 모색하고자 한다.

2. 관련 연구

통합보안시 스템의 기술은 크게 특정화 되어 표준이라고 할 수 있는 사항은 없으나 다음과 같은 몇 가지 사안이 이슈가 되고 있다.

첫째, 표준 포맷이다. 서로 다른 이 기종의 에이전트(구축되어 있는 침입차단시스템·침입탐지시스템과 같은 보안 시스템이 향후 다른 회사의 제품으로 투입될 수 있는)를 추가로 구축할 수 있도록 표준화된 포맷(또는 API)이 필요하다. 이는 실제로 구축되어 있는 시스템에서 고객이 다른 회사의 제품을 추가로 투입할 수 있느냐 하는 문제로 확장성에 있어서 가장 중요한 문제가 된다. 또한 이러한 표준화된 포맷은 언급된 보안 시스템 간 여러 연동에 있어서 중요한 핵심이 된다.

둘째, 데이터 암호화 및 인증이다. 각 보안제품의 관리를 위해서는 제품 간 정보 교환이 필수인데 이 과정 중 발생할 수 있는 보안 로그의 변조를 예방하기 위해서는 데이터 암호화가 필요하다. 또한 허가되지 않은 에이전트에서 정보를 보낼 경우 통합보안 시스템이 오판할 수 있어 에이전트 인증이 필요하다. 현재 SNMP-trap이나 syslog를 이용하여 정보를 수집하는 경우 이러한 정보는 TCP/IP상에서 클리어 텍스트(clear text, 암호화 되어 있지 않은 상태)로서 이동하는데 스니핑(Sniffing, TCP/IP상에서 흘러 다니는 정보를 낚아 채 보는 것) 기법을 통하여 통합보안 시스템으로 전달되는 정보를 변조해 침입탐지 시스템(IDS)에서 탐지한 침입정보를 변경해 침입이 아닌 상황으로 보낸다면 정보를 수집·분석하는 통합보안 시스템의 입장에서는 수동적으로 들어오는 잘못된 정보를 분석하여 소비자로 하여금 오판을 내리게 할 문제점을 가지고 있다. 또한 공격자의 입장에서 인증 받지 않은 가짜 에이전트에서 실제 보안 사고가 발생한 것이 아닌 정상적인 상태로 데이터를 보내 준다면 통합보안 시스템에서는 올바르지 못한 상황을 설명할 수밖에 없기 때문에 인증과정 역시 반드시 필요로 한다.

따라서 보안로그 변조 방지 및 정확한 정보의 수집 및 분석을 위해 데이터 암호화 및 에이전트 인증이 통합보안 시스템의 주요 기술로 개발 되어야 할 것이다.

셋째, 이벤트 정보의 필터링이다. 침입차단시스

템이나 IDS 등 개별적인 보안제품의 경우 모든 공격에 대응 하도록 돼 있어 동일한 공격이라도 소비자에게 일일이 알려 주게 된다. 그러나 통합보안시스템의 입장에서는 여러 보안제품에서 일어나는 이벤트 정보에 대해서 전부 고객에게 보여 준다면 이러한 정보는 실시간 모니터링이라는 개념보다는 제품의 작동여부 밖에는 확인할 것이 없다. 따라서 실제 보안에 관련된 문제가 발생하게 되더라도 고객은 수많은 정보 중 어떤 것이 보안과 관련되어 있는지 파악하기 힘들어 지게 된다. 또한 이는 고객이 사용하고 있는 모니터링을 하기 위한 콘솔에 상당한 부하를 줄 수 있기 때문에 결국은 안정성에 문제를 야기 시킬 수도 있다.

넷째, 수집된 정보에 대한 내부적인 가공능력과 이에 대한 대응기술이다. 이것은 통합보안시스템의 가장 중요한 기능으로 통합보안 시스템이 단순한 정보의 수집 차원이 아닌 수집된 정보를 통해 소비자가 올바른 판단을 내릴 수 있도록 지원하는 개념이다. 다만 안타깝게도 현재 국내의 제품 중 이를 100% 완벽하게 지원하는 제품이 없는 실정이다.

다섯째, 정보처리 능력이다. 이는 장비의 사양에 따라 다를 수 있으나 네트워크 침입탐지 시스템이 처리할 수 있는 능력이 제품의 선정 기준중 하나인 것과 같이 이벤트의 처리 능력은 에이전트로부터 얼마나 많은 정보를 수집하여 얼마나 빠른 시간 내에 처리하느냐에 따라 통합보안시스템이 빠른 대응을 할 수 있는 기반을 이룬다.

기타 관리자의 권한 도용에 따른 문제점을 발생시키는 경우에 관리자 감사에 대한 문제점이나 보안제품의 가장 문제가 되는 리포팅, 관제 센터의 경우 담당자의 사건 처리에 대한 대응 확인 등 여러 가지 것이 있으나 현재 대부분 논의되어 있는 것은 위에서 언급한 바와 같이 에이전트의 추가에 따른 표준화 수용, 암호화 통신, 수집된 정보에 대한 가공 및 이에 대한 대응기술 등이 현재 중점화 되고 있는 기술들이다[6].

전체적으로 통합보안시스템의 기술이라는 것은 개별 보안제품이 표방하는 기술과는 개념적으로 다를 수밖에 없다. 따라서 통합보안 시스템자체는 어떠한 보안기능을 발휘하기 보다는 관리개념으로서의 인식 되어야하고 올바른 판단을 할 수 있도록 지원하는 기능 및 개별 보안제품의 자체적인 문제점을 보완해주는 기능으로 판단해야 할 것이다[7, 8].

3. 융합보안설계시스템

3.1 융합보안시스템 설계

융합보안시스템 설계를 위해 단계별로 구조를 살펴 보면, 첫째 출입통제, 생체보안, 스마트카드, OA보안의 물리보안영역에서의 보안정책위반 이벤트에 대한 수집 과정을 두고 각 보안영역별 핵심 이벤트의 분류 및 이를 통합 수용할 수 있는 이벤트 정규화에 대한 모듈이 (그림 1)과 같이 필요하다.

둘째 각 보안단말의 보안정책위반 이벤트 전송방법에 대한 연구 및 수집 모듈과 보안단말의 보안정책위반 이벤트의 직·간접 수집 인터페이스는 (그림 1)과 같이 위치 한다.

(그림 1) 물리적 보안영역의 통합보안관제 구조

세째 수집된 보안이벤트에 대한 정규화처리 엔

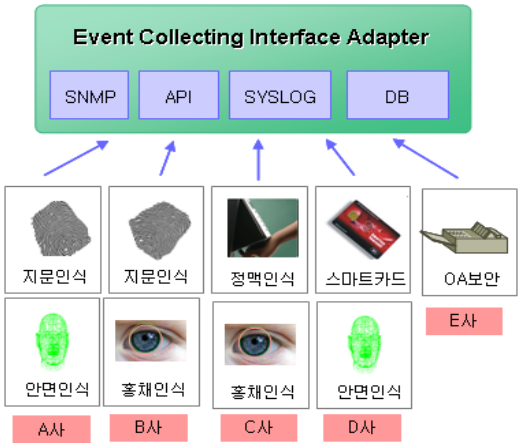
진을 통해 정규화 처리된 보안이벤트로부터 사용자 정의의 이벤트-이벤트간의 연계분석을 위한 융합보안 상관분석모듈로 보내지고, 상관분석모듈은 DB의존성이 없고, 분석의 실시간성을 제공한다.

네째 대용량 이벤트의 저장 및 검색에 최적화된 인덱싱 처리 및 대용량 이벤트로부터의 통계처리 성능저하를 방지하기 위한 실시간 통계처리 모듈로 처리된다.

3.2 보안이벤트로그 수집 및 이벤트로그 포맷 정규화처리부

3.2.1 보안이벤트 통합수집Adapter부(Event Collecting Interface Adapter)

다양한 종류의 보안단말(디지털도어락, 스마트카드, 지문인식, 안면인식, 홍채인식, OA사무기기보안 등)의 제조사 별 다양한 이벤트 전송프로토콜을 지원하여 실시간 또는 유사 실시간으로 원시형태의 보안이벤트 로그를 수집한다.



(그림 2) 이벤트 통합 수집 Adaptor 개념도

3.2.2 보안이벤트 정규화 처리부

제조사별 상이하고, 제품 버전별 상이한 보안이벤트의 표현 형식을 제품군별로 정의하고 보안이벤트를 상호 비교할 수 있도록 원시 이벤트의 형식을 정규화 처리한다.

동일한 내용의 이벤트이지만 제조사, 버전별 상이한 형태로 표현되는 정보를 하나의 공통된 형식으로 표현함으로써 이벤트와 이벤트 간의 연계 분석 및 상세 필터링 분석을 가능하게 함을 목적으로 한다

3.3 이벤트로그저장부 : 대용량 보안이벤트의 저장

통합관리되는 대량의 보안이벤트에 대한 장기간 저장 및 향후 추적 분석을 원활히 할 수 있도록 정규화(Normalization)된 이벤트로그를 데이터베이스에 저장함에 있어서, 로그의 특성(대용량, 데이터 내용의 변경 없음, 신속한 검색 지원)을 최대한 고려하여 최적의 데이터 인덱싱 메커니즘을 적용하여 데이터의 입출력을 신속히 처리한다.

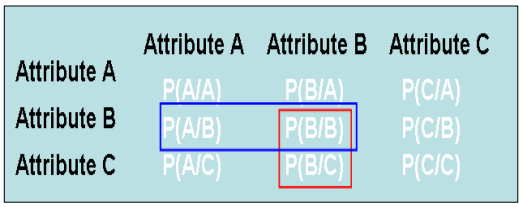
〈표 1〉 이벤트의 정규화 처리 예

제조사	원시 이벤트 로그	정규화 이벤트 로그
A사	2009-02-09 16 : 00, ID-09218, Access Deny, Password Failure, …	=> 20090209|1600|1|1| 날짜|시간|단말ID|인증여부|인증사유|.
B사	200902091600 access_failure id09218, access_denied, …	

3.4 보안이벤트 상관분석 모듈

수집된 개별 이벤트로 부터 다양한 방식의 보안 패턴분석 및 보안단말의 단위그룹 내의 이벤트의 Sequence 맵 또는 시간/공간/타입에 기반한 패턴의 일치를 바탕으로 정확한 이벤트 연계상황 결정 및 경보를 제공한다.

- 이벤트 처리과정을 용이하게 식별할 수 있는 보안 패턴 분석 및 이벤트의 상관분석 기능 제공
- 사용자 정의의 Attribute 조합을 통한 상관관계를 정의 할 수 있는 상관분석규칙 언어의 제공



(그림 3) 사용자 정의의 보안이벤트 상관분석

3.5 실시간 통계분석 모듈

통계추이분석 및 신속한 보고서 작성을 위해 백그라운드의 자동 분석을 통한 통계 데이터의 상시 업데이트로 사용자가 요구하는 데이터의 최단 시간 응답이 가능하며, 실시간, 일별, 주별, 월별 및 사용자가 정의한 기간에 대한 다양한 형식의 보고서 산출 및 이벤트별 Historical 데이터의 제공으로 이벤트 추이의 비교 분석을 통한 감시기능 제공한다.

3.6 사용자 운용 환경 제공

운영자 편의의 사용자 인터페이스를 위해 IT 보안 및 물리보안의 융합된 관제환경에서의 사용자 편의에 입각한 통합관제업무에 대한 연구 및 융합관제업무에 최적화된 사용자 환경 제공한다.

- 관제Dashboard를 통한 통합관제 화면 제공
- 장애 관리
- 시간별, 지역별, 조직별, 장비별 통계 자료 제공
- 이력 변경 정보 제공
- 텍스트, 차트, 그래프 형식의 다용한 보고서 출력 등

4. 결 론

산업보안을 위하여 현재 물리적인 보안 시스템, 사이버적인 보안 시스템은 각각 구축되어 있지만 최근 기술유출 트렌드는 융복합적인 기술 유출이 있다. 이에 각각의 시스템을 융합관제할수 있는 것이 필요하며, 이에 따른 핵심 기술은 상관관계 분석 기술이라고 할수 있다. 본 연구에서는 물리보안영역에서의 보안정책위반 이벤트에 대한 연구, 이벤트 정규화에 대한 연구, 각각의 시스템에서의 수집 인터페이스를 개발 하였다. 또한 정규화 엔진과, 상관분석엔진으로 실시간 융합보안관제를 가능하게 하였다.

그러나 상관관계방안을 효율적으로 사용하기 위해서는 체계적인 방안 마련이 필요하며, 따라서 향후 물리적인 보안 이벤트와 사이버적인 이벤트에 대한 각 상황별 표준방안을 마련하고, 위험에 오래되고 축적된 데이터와 경험이 필요하다.

참 고 문 헌

[1] 이동휘, 이동춘, 김귀남, “실시간 위협에서 Event 유형의 정형화설계 및 구현”, 정보보안논문지, 2006.

[2] 국가정보원, 국가사이버안전매뉴얼, 2008.

[3] C. Zou, L. Gao, W. Gong, and D. Towsley, “Monitoring and Early Warning for Internet Worms”, In Proceedings of the 10th ACM Conference on Computer and Communication Security, p. 10, 2003.

[4] J. B. D. Cabrera, L. Lewis, X. Qin, C. Gutierrez, W. Lee, and R. K. Mehra. “Proactive Intrusion Detection and SNMP based security management”, In proceedings of IFIP/IEEE Eighth International Symposium on Integrated Net Work Managemen, pp. 225-254, 2003.

[5] J. Zhai, J. Tian, R. Du, and J. Huang, “Network Intrusion Early Warning Model Based on D-S Evidence Theory”, In Proceedings of 2003 International Conference on Machine Learning and Cybernetics, Vol. 4, pp. 1972-

1977 2003.
[6] 이동휘, “소규모 네트워크의 통합보안관제를 위한 SnSA 설계 및 구현”, 정보보안논문지, 2004.
[7] J. Li, and C. Manikopoulos, Early statistical anomaly intrusion detection of DOS attacks using MIB traffic parameters, Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, pp. 53-59, 2003.
[8] 박재현, “통합보안관제시스템 고도화를 위한 위협관리시스템 구현방안에 관한 연구”, 충남대, 2006.

하 옥 현

1978년 성균관대학교 정치외교학과(정치학사)
1980년 서울대학교 행정대학원(행정학석사)
1998년 프랑스 사회과학대학원(EHESS) 박사과정(DEA 취득)
2005년 고려대학교 정보보호대학원(공학박사)
2008년~현재 호남대학교 경찰법행정학부 교수