Pre-Forensic 정책을 도입한 통합보안관리시스템 연구

최대수*, 이용균*, 김성락**
*이글루시큐리티 인터넷보안연구소
**오산대학 컴퓨터정보계열
e-mail : dschoi@igloosec.com

A Study on Enterprise Security Management System with Pre-Forensic policy

Dae-Soo, Choi*, Yong-Kyun, Lee*, Sung-Rak, Kim**
*Internet Security Lab, IGLOO Security
**Dept. of Computer Information, Osan College

요 약

컴퓨터 포렌식절차에서 증거물 획득은 중요한 부분이다. 컴퓨터 포렌식의 여러 원칙 중 신속성의 원칙은 휘발성 정보의 획득유무와 관계가 있다. 기존 통합보안관리시스템(ESM: Enterprise Security Management) 은 보안이벤트중심으로 정보를 수집한다. 컴퓨터 포렌식에서 중요한 휘발성 시스템 포렌식 정보와 네트웍 포렌식 정보는 수집하지 않는다. 본 논문에서는 통합보안관리시스템에 Pre-Forensic 정책을 도입하여 기존 보안경보기능에 포렌식 데이터 수집 대응방안을 추가한 새로운 통합보안관리시스템 모델을 제안한다. 제안 시스템은 무결성이 보장되는 많은 증거를 수집할 수 있으며 향상된 컴퓨터 포렌식 증거물 획득 방법을 제시한다.

1. 서론

최근 해킹, 바이러스 등 사이버 공격과 망 사용자의 악의적 사용으로 인해 정보통신망의 마비 및 보안사고가 자주 발생되고 있다. 침입탐지시스템, 침입차단시스템, 침입방지시스템, 안티바이러스, 안티스팸, 등 다양한 보안제품을 도입했음에도 불구하고 보안사고에 대한 원인규명, 처리가 신속하게 이루어지지 못하며 처리비용은 증가되고 있다. 이러한 시대적요구로 인해 통합보안관리의 필요성이 증대되고 정부기관을 중심으로 통합보안관리시스템 도입이 활기를 띠고 있다[6]. 이와 함께 컴퓨터 관련 수사를 지원하며 법적 효력을 갖는 디지털 자료와 과학적이고 논리적인 절차와 방법을 연구하는 컴퓨터 포렌식 연구가 활발히 진행 중이다[1].

현재 통합보안관리시스템에서 수집하는 정보는 보안장비의 이벤트 중심이다. 즉, 보안사고발생시 빠른 시간내에 이루어져야 하고 컴퓨터 수사에 필수적인 휘발성 시스템 포렌식 정보와 네트웍 포렌식 정보들은 자동으로 수집하지 못하고 있다.

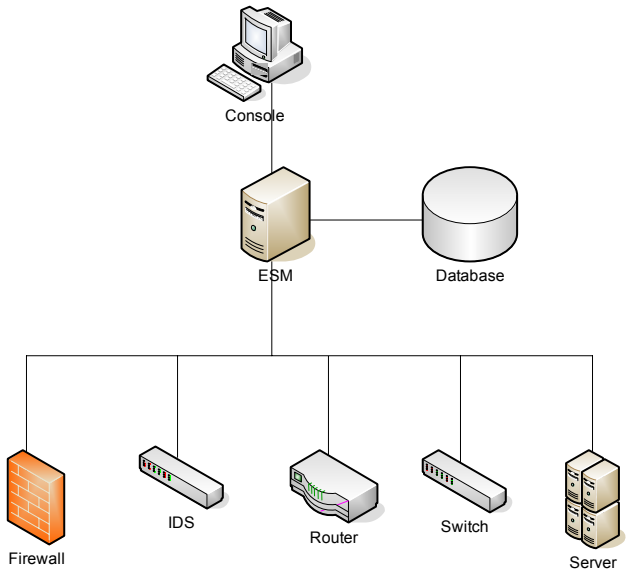
본 논문에서는 먼저 2 장에서 통합보안관리시스템의 개념과 구조 그리고 기능에 대해 살펴보고 3 장에서는 컴퓨터 포렌식에 대한 개념과 포렌식 절차, 네트웍 포렌식, 그리고 포렌식 연구동향을 살펴본다. 그리고 4 장에서는 Pre-Forensic 정책을 도입한 통합보안관리시스템을 제안한다. 마지막으로 5 장에서 결론 및 향후 연구방향에 대해 살펴본다.

2. 통합보안관리시스템

2.1 통합보안관리시스템 개요[6]

통합보안관리시스템의 정의는 전사적인 차원에서 일관된 정책을 가지고 보안시스템을 통합적으로 관제 및 운용, 관리함으로써, 보안관리 업무의 효율화와 보안성 향상을 극대화 시킬 목적으로 사용되는 통합보안관리 체계를 말한다[ ]. 또한 네트워크에 산재한 보안 시스템들을 통합 콘솔로 관리하고 유사한 보안 정책을 갖는 보안시스템 간에 정책을 통일시켜 전체적인 보안성을 향상 시키는 통합시스템이라고도 한다. 결과적으로 이기종 보안시스템의 효율적 운영(정책관리, 침해대응, 이벤트 통합관리/분석)등을 통한 사전적 사고예방을 목적으로 하며 넓게는 IT 자산 인프라에 대한 가용성, 무결성, 보안성을 보장하기 위한 위험관리 라고 볼 수 있다.

일반적으로 3-tier 형태로 구현되어 있으며, 단계별 관리에 의해 2-tier 나 4-tier 형태를 갖기도 한다. 구현 방법에 따라 구조만 다를 뿐 처리방법은 비슷하다. 3-tier 형태의 구조를 살펴보면 보안시스템들과 다양한 장비에서 이벤트를 실시간으로 수집해오는 에이전트, 중앙에서 통합적으로 에이전트의 이벤트를 받아서 DB 에 저장/분석 하는 매니저 그리고 사용자가 GUI 환경에서 보안정책을 설정하고 이벤트를 분석할 수 있는 콘솔 3 가지로 구성되며 다음그림과 같다.



[그림 1] 3-tier 통합보안관리시스템 구조

2.2 통합보안관리시스템 기능

현재 상용화되어 있는 통합보안관리 시스템들의 기능을 조사/정리해보면 다음 표와 같다.

[표 1] 통합보안관리시스템 기능명세

구분	기능설명
구성	Agent 의 Security Agent 와 Server Agent 구분/통합
	Manager 는 4-tier, 3-tier 형태로 구성
	Manager 시스템의 상용 DBMS 지원
관리 및 운영 방안	Console 의 Client/Server 형 또는 웹형태로 GUI 지원
	관리대상 시스템의 파일 무결성 점검 기능
	관리자별/운영자별 등급제한으로 인한 그룹관리 기능
	- 운용자 등급별 ESM 접속 사용 기능 제한
	- 동일한 이벤트에 대한 운용자별 선택적 모니터링
	ESM 사용자 접속 및 작업이력 관리 기능
	DB 로 저장되는 이벤트 보관주기 설정 및 자동 백업
	에이전트 기능 추가 또는 Upgrade 시 자동 Patch 기능
이벤트 수집	관리대상시스템과의 다양한 통합방법 (API, SNMP Trap, Syslog, Log File) 제공
	필요한 이벤트 만을 필터링 할 수 있도록 구현
통합 관제	Real-Time 모니터링 및 침입 분석 기능
	각 시스템별 이벤트의 하나의 창에서의 모니터링
	이기종 이벤트간 실시간으로 직관적인 방법 (Drag & Drop)으로 상호 연결 분석
	의심스러운 사용자, 서버에 대한 특별관리 (Black List DB)
	이기종 IDS 의 서로 다른 위험도 평가에 따른 정형화된 기준 제시
	Real-Time 알림/경보(Notice/Alert) 기능
	Sound, E-mail, SMS 등 다양한 방법으로 경보제공
	위험 등급관리에 의한 Threshold 지정 및 경보기능
상호 연계 분석	하나의 보안장비에서 발생하는 패턴의 이상징후 분석, 실시간 상호연관성 분석 기능
	탐지된 이상징후를 실시간으로 운용자에게 알릴 수 있는 Alert 기능 제공
	조합할 수 있는 Correlation-Rule 수의 무제한
	Correlation Rule 의 운용자에 의한 쉬운 추가 및 변경
	실시간 Correlation 으로 인한 성능저하 없음
리포팅	각 시스템별 통계보고서
	시스템 Resource 사용량 및 가동상태 통계보고서
	블랙리스트 대응보고서 등의 침해대응 운영보고서
	보고서의 사용자 정의 및 스케줄링에 의한 자동생성
기타	관리대상시스템에 Agent 가 탑재될 경우, 데이터 송수신의 암호화 및 비암호화 통신 지원

즉, 이벤트 수집과 분석에 주기능을 하고 있으며 휘발성 포렌식 정보 수집기능은 미약하고 수사에 큰 도움이 못된다.

3. 컴퓨터 포렌식

3.1 컴퓨터 포렌식 개요

컴퓨터 포렌식은 컴퓨터 관련 조사/수사를 지원하며, 디지털 자료가 법적 효력을 갖도록 하는 과학적/논리적 절차와 방법으로 사이버 경찰청과 같은 수사기관에서 사용하고 있다. 컴퓨터 포렌식의 범위는 스파이, 기술유출, 공갈, 사기, 위조, 해킹, 사이버 테러와 같은 컴퓨터 범죄수사에서 명예훼손, 업무상 과실/재해, 내부감사 같은 민사소송분재 분야 그리고 침해사고 예방 및 대응에 까지 넓은 범위를 가지고 있다. 컴퓨터 포렌식은 포렌식 기술을 이용하여 포렌식 절차대로 컴퓨터 범죄수사, 정보보호 침해사고 분석 및 대응, 컴퓨터 시스템, 네트워크의 데이터 분석한다 [1][2][3][4][5].

컴퓨터의 포렌식은 다음과 같은 절차로 수행된다.

a. 수사 준비단계 (Preparation) : 포렌식 툴 테스트, 장비확보, 협조체계확립

b. 증거물 획득단계 (Acquisition) : 현장분석, snap shot, Disk Imaging, 증거물인증

c. 증거물 보관 및 이송 단계 (Preservation) : Image 복사, 증거물, 포장 및 운반

d. 증거물 분석단계 (Examination & Analysis) : 자료복구/검색, TimeLine 분석, Signature 분석, 은닉자료 분석, Hash/Log 분석,

e. 보고서 작성단계 (Reporting) : 증거분석 결과, 증거담당자 목록, 전문가 소견

3.2 네트웍 포렌식[2]

지금까지의 컴퓨터 포렌식 연구는 포르노나 인터넷 사기등의 증거확보 및 분석을 위한 시스템 포렌식에 대한 연구만이 활발히 이루어졌고 최근들어 네트웍 포렌식에 대한 연구가 이루어지고 있다. 네트웍 포렌식은 침해사고 확인을 시발점으로 침해와 관련된 네

트웍 이벤트를 수집/분석/저장하는 일련의 과정이다.

네트웍 포렌식의 목적은 침해 당시의 상황재구성을 통해 증거자료에 대한 신뢰성을 제공하는데 있다. 네트웍 포렌식정보는 시스템 포렌식 정보처럼 사건에 대해 침입의 확실한 정보를 제공하지는 않지만 침입정보를 보충하고 정보에 대한 신뢰성을 제공한다.

기존의 네트웍 포렌식에 대한 분류는 중소형전산망에서 적합하지만 여러 정보보호장비로부터 수백만건의 로그정보들이 기록되는 통합보안관리시스템에서는 의미가 없다. 또한 여러 정보보호 장비들의 상호연관성 분석을 통한 침해정보 분석이 고려되지 않았다.

3.3 컴퓨터 포렌식 동향 및 요구사항

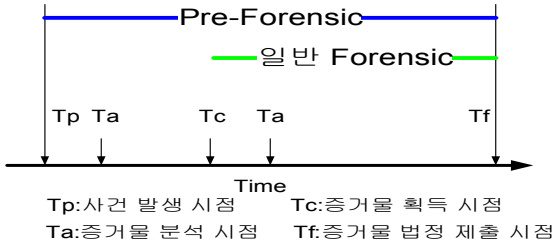
최근 포렌식에 대한 기술이 발전하고, 디지털 증거물이 법정에서 효력을 발휘하는 경우가 많아지면서 Anti-Forensic 개념이 등장하고 있다. 포렌식 기술에 대응하는 즉, 자신에게 불리하게 작용할 가능성이 있는 증거물을 차단하려는 일련의 활동을 Anti-Forensic 이라 한다. 주로 데이터 복구기법 회피, 증거자동삭제, 데이터 은닉등의 기법이 있다.

컴퓨터 포렌식의 여러 절차 중 디지털 증거물 획득 단계는 중요한 부분이다. 컴퓨터 포렌식 원칙 중 신속성의 원칙은 휘발성 정보의 획득유무와 관계가 있다. 시스템 포렌식의 경우 현장에 도착하여 시스템의 휘발성 정보 및 운용 상태를 수집한다. 하지만 가해자가 시스템의 증거를 소멸시켰을 경우 수사에 어려움을 초래할 수 있다. 그래서 신속한 사고 발생시 상황을 파악할 수 있는 시스템 포렌식 정보와 네트웍 포렌식 정보 획득은 중요하다. 하지만 아직 Ant-Foresic 기술에 대응할 수 있는 기술과 정책은 미흡한 실정이다. 본 논문에서는 증거차단의 우려가 높은 휘발성 정보의 신속한 획득방법에 관한 내용을 제시한다.

4. Pre-Forensic 정책을 도입한 통합보안관리시스템

4.1 Pre-Forensic 개념

침입탐지시스템, 침입차단시스템 등의 보안장비는 사고예방의 성격이 강하며 로그들의 무결성을 보장하기는 어렵다. 그러나 범죄수사 주체가 사건 발생 예상 지점에 포렌식 정책을 수립 및 구성할 수 있다면 사건 발생직후에 무결성이 보장되는 많은 증거를 얻을 수 있는데 이러한 방법을 Pre-Forensic 이라 한다. 이러한 Pre-Forensic 을 도입하면 사고 대응에 대한 신속성 뿐 아니라 증거물 확보의 무결성 정도에도 차이가 있다. [6]

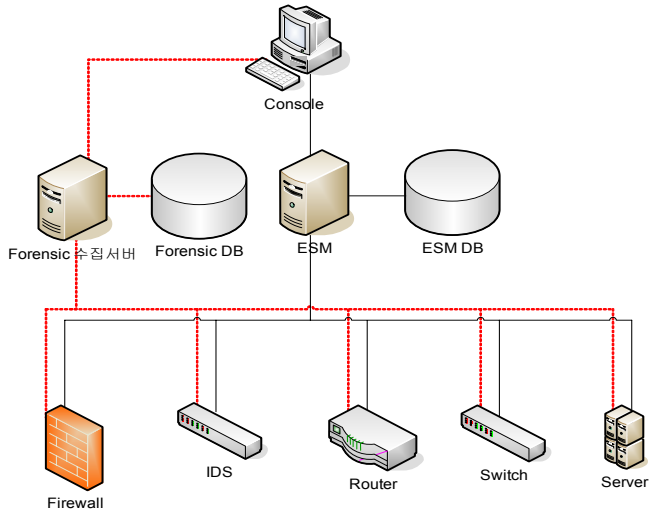


[그림 2] 증거물에 대한 무결성 보장범위

일반 Forensic 의 경우 Tc ~ Tf 는 무결성을 보장하고 Tp ~ Tc 는 무결성을 보장 못한다. 반면 Pre-Forensic 의 경우 Tc ~ Tf 는 무결성을 보장하고 Tp ~ Tc 는 조건부 무결성을 보장한다. 즉, Tp ~ Tc 는 즉각적으로 시스템에서 증거를 수집하게 되므로, 신속한 증거 수집을 보장할 수 있다.

4.2 제안 시스템 구조

본 논문에서 제안한 시스템은 통합보안관리시스템에 포렌식 수집서버과 데이터베이스를 추가하여 사고발생시 즉각적으로 시스템 포렌식 정보와 네트웍 포렌식 정보를 수집하는 구조이며 다음 그림과 같다.

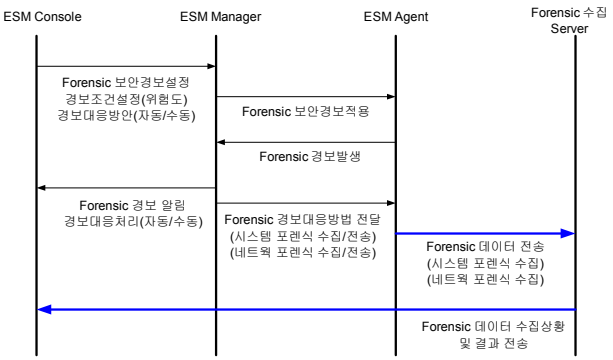


[그림 3] 제안 시스템 구조도

4.3 프로세스 흐름

기존 운영중인 통합보안관리시스템에 포렌식 수집 기능을 추가한 구조이며 콘솔에서 포렌식 보안경보를 설정한다. 위험도와 임계치 정보를 등록하고 경보발생시 대응방안을 설정한다. 대응방안은 수동 또는 자동으로 실행될 수 있으며, 대응방안은 휘발성이 강한 포렌식 데이터의 실시간 획득이 된다. 이러한 설정은 매니저를 거쳐 에이전트에 전달되고 에이전트는 포렌식 보안경보조건을 감시한다. 조건에 만족할 경우 포렌식 보안경보가 발생하고 매니저에게 전송된다, 수동 혹은 자동조건에 따라 매니저는 해당 포렌식 보안경보의 대응방안을 검색하고 처리한다. 이 시점에 포렌식 정보수집이 이루어지는데 단위 보안제품의 OS, 플랫폼에 따라 수집정보는 달라진다.

휘발성이 강한 시스템 포렌식의 경우 배치처리 형태로 실행된 다음 결과를 포렌식 수집서버에 실시간으로 전송한다. 네트웍 포렌식 정보도 사고발생 현시점의 정보를 획득하여 포렌식 수집서버에 실시간으로 전송한다. 또한 포렌식 경보가 발생한 네트웍에 트래픽분석서버(TAS:Traffic Analysis Server) 센서가 있는 경우, 상세한 트래픽 데이터 수집기능이 자동으로 시작된다. 그 결과도 마찬가지로 포렌식 수집서버로 전송된다.



[그림 4] 제안 시스템 프로세스 흐름도

4.3 수집 데이터 정의

유닉스 시스템의 경우 수집해야 할 휘발성 시스템 포렌식 정보는 다음과 같다[2].

1. 현재 시스템 시간/날짜
2. 시스템에 접속한 사용자 확인
3. 모든 파일의 접근시간과 수정, 생성시간 기록
4. arp 캐쉬목록과 라우터 목록
5. 열린포트 확인
6. 열린포트에 연결된 프로그램 목록
7. 실행되는 프로세스 확인
8. 현재, 그리고 최근 접속 목록
9. 실행한 작업내용기록
9. 시스템시간/날짜, 단계별 행동기록, 해쉬값 기록
10. 루트킷 탐지
11. 로그파일 수집
12. 중요 구성파일 획득
13. 불법적인 스니퍼 탐지
14. /proc 파일 시스템, 시스템 램 복사

그리고 단위제품마다 수집해야 할 네트웍 포렌식 정보는 다음과 같다.

[표 2] 네트웍 포렌식 정보

	시간/버전정보	설정/정책정보	로그정보
스위치	Time Version	Port Trunk Virtual Lan IP 정보	Local Log
라우터	Time Version	Routing ARP Netstat Interface	Local Log Netflow Log
침입차단 시스템	Time Version	탐지정책 통재정책	Local Log Filtering Log
가상사설망	Time Version	연결정책	Local Log Connection Log
침입탐지 시스템	Time Version	탐지정책	Detction Log
취약점	Time Version	취약점정보	
트래픽분석시스템	Time Version	수집정책	트래픽로그

4.4 정리

통합보안관리시스템에 Pre-Forensic 정책을 도입하고 기존 보안경보기능에 포렌식 데이터 수집 대응방안을 추가하여 설계하였다. 사고시점에서 Anti-Forensic 방법들에 의해 소멸될 수 있는 휘발성 정보들을 수집할 수 있다. 또한 트래픽 데이타의 경우 엄청나기 때문에 상세한 정보를 계속 수집할 수는 없다. 이러한 제약을 해결할 수 있는 방법은 사고시점부터 상세한 트래픽 데이타를 수집하는 것이다.

5. 결론 및 향후 연구 방향

통합보안관리시스템은 단위 보안제품들의 보안로그들을 중심으로 수집한다. 보안사고 발생시 신속하게 수집되어야 할 중요한 휘발성 정보들은 Anti-Forensic 기법들로 쉽게 소멸된다. 본 논문에서는 Pre-Forensic 정책을 통합보안관리시스템에 도입하여 휘발성이 강한 시스템 포렌식 정보와 네트웍 포렌식 정보의 수집 방안모델을 제시하였다. 또한 동일 네트웍에 트래픽수집서버가 있는 경우 상세트래픽수집 대응방안기능도 추가하였다. 이 시스템을 이용하면 컴퓨터 포렌식의 신속성의 원칙을 향상 시킬 수 있다.

향후 연구방향으로는 수집된 포렌식 데이터의 정확한 분석기법과 이기종간의 통합보안관리시스템 보안로그들과 포렌식 DB 에 저장된 휘발성 정보들간의 상호연관성분석 및 타임라인분석 방법 등이 연구되어야 할 것이다.

참고문헌

[1] 제 2 차 CONCERT 기술세미나, “컴퓨터 포렌식”, 한국 침해사고대응팀협의회, 2004

[2] 박종성, 최운호, 문종섭, 손태식. “자동화된 침해사고대응시스템에서의 네트웍 포렌식 정보에 대한 정의”, 정보보호학회, 2004

[3] Warren G. Kruse II, Jay G. Heiser, “Computer Forensics: Incident Response Essentials“, Addison Wesley, 2001

[4] Melisa LaBancz, “Network Forensics”, networksecurity.com IT Journalist, April 2002

[5] Vicka Corey, Charles Peterman. SybilShearin, Michael S.Greenberg, and James Van Bokkelen. “Network Forensics Analysis”, Sandstorm Enterprises, IEEE Internet Computing Magazine, November 2002

[6] http://www.igloosec.co.kr